



UNITED STATES
NUCLEAR REGULATORY COMMISSION
ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
WASHINGTON, DC 20555 - 0001

August 22, 2007

MEMORANDUM TO: ACRS Members

FROM: Charles G. Hammer, Senior Staff Engineer */RA/*
Technical Support Branch, ACRS

SUBJECT: TRANSMITTAL OF REVIEW MATERIALS FOR DIGITAL
INSTRUMENTATION AND CONTROL SUBCOMMITTEE MEETING

The Digital Instrumentation and Control (I&C) Subcommittee will meet on September 13, 2007 to discuss digital I&C system issues.

To prepare for this meeting, the following information is attached:

1. A description of NRC Steering Committee activities for digital I&C
2. The current Digital I&C Project Plan
3. The current Interim Staff Guidance (ISG) for the major digital I&C issues

The proposed schedule and status report will be issued at a later date.

If you have any questions, please contact me at (301) 415-7363 (cgh@nrc.gov) or Girija Shukla at (301) 415-8439 (gss@nrc.gov).

cc w/o Attachments: F. Gillespie
S. Duraiswamy
C. Santos



Protecting People and the Environment

About NRC

Digital Instrumentation and Controls

Overview

• Nuclear Reactors

Key Issues

• Nuclear Materials

• Radioactive Waste

Steering Committee

• Nuclear Security

• Public Meetings

• Meetings & Involvement

Related Information

Frequently Asked Questions

Reports and Correspondence

Regulations and Guidance

Technical References

Regulatory References

Other Correspondence

Contact Us About Digital I&C

[Home](#) > [About NRC](#) > [How We Regulate](#) > [Research Activities](#) > [Digital I&C](#) > [Key Issues](#)

Key Issues

Digital instrumentation and controls (I&C) raise issues that were not relevant to analog systems. Examples of such issues include the following.

A common-cause failure attributable to software errors was not possible with analog systems. This potential weakness may require a consideration of diversity and defense in depth in the application of digital I&C systems.

Digital system network architectures also raise issues such as interchannel communication, communication between nonsafety and safety systems, and cyber security that must be reviewed closely to ensure that public safety is preserved.

Highly integrated control room designs with safety and nonsafety displays and controls will be the norm for new reactor designs. Quality assurance during all phases of software development, control, and validation and verification is critical to minimize the possibility of common-cause failures.

Qualification and dedication of commercial off-the-shelf equipment in safety-related applications are other important aspects of the implementation of digital I&C systems.

Key issues include those discussed in this section.

- [Diversity and Defense in Depth](#)
- [Highly Integrated Control Rooms—Digital Communication Systems](#)
- [Highly Integrated Control Rooms—Human Factors](#)
- [Cyber Security](#)
- [Risk-Informed Regulation of Digital I&C](#)

[Privacy Policy](#) | [Site Disclaimer](#)

Wednesday, July 11, 2007



About NRC

Digital Instrumentation and Controls

Overview

History of Digital I&C

Key Issues

NRC Activities

Summary

Public Meetings

Steering Committee

Design and Review

Program Activities

Related Information

Frequently Asked Questions

Reports and Correspondence

Regulations and Guidance

Technical References

Regulatory References

Other Correspondence

Contact Us About Digital I&C

[Home](#) > [About NRC](#) > [How We Regulate](#) > [Research Activities](#) > [Digital I&C](#) > [Steering Committee](#)

Steering Committee

In January 2007, the NRC formed a digital instrumentation and controls (I&C) steering committee to provide management focus on the NRC regulatory activities in progress across several offices, to interface with the industry on key issues, and to facilitate consistent approaches to resolving technical and regulatory challenges. The members of the steering committee include management representatives from the various NRC offices that have regulatory responsibilities related to digital I&C.

The primary responsibilities of the steering committee are to interface with industry representatives on plans for resolution of digital I&C issues, to oversee and facilitate resolution of technical and regulatory issues related to the deployment of digital I&C, and to ensure effective interoffice coordination on digital I&C issues. In addition, the steering committee interfaces with senior NRC managers, as needed, to facilitate its oversight function.

The steering committee is fulfilling this responsibility in an advisory capacity to the Directors of the Office of Nuclear Reactor Regulation (NRR), the Office of New Reactors (NRO), the Office of Nuclear Material Safety and Safeguards (NMSS), and the Office of Nuclear Regulatory Research (RES) in support of the line managers who are responsible and accountable for the implementation of the digital I&C guidance deployment.

Details of the steering committee charter are outlined in the memorandum from Mr. Luis A. Reyes, Executive Director for Operations.

The steering committee has formed the following six task working groups (TWGs) that focus on key areas of concern:

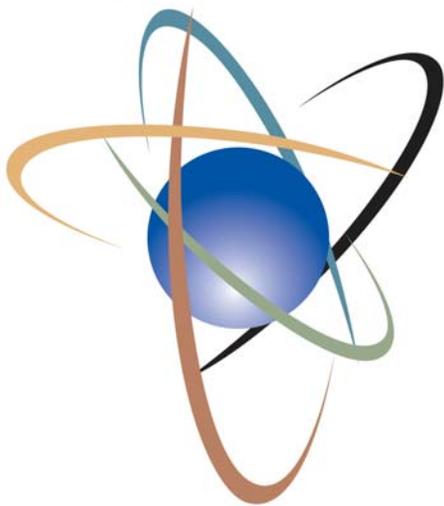
- Cyber Security
- Diversity and Defense-in-Depth
- Risk-Informed Digital I&C
- Highly-Integrated Control Room - Communications
- Highly-Integrated Control Room - Human Factors
- Licensing Process Issues

The TWGs consist of various staff members of NRR, NRO, RES, NSIR, and NMSS. Each TWG is responsible for developing a specific project plan to address the key area of concern. Essentially the plans are to identify and resolve technical issues that will result in more efficient licensing of digital I&C systems for new reactor applications and for retrofits at operating reactors/facilities. The [Digital I&C Project Plan](#) defines the problem statements, identifies deliverables, and establishes milestones to resolve the issues. In May 2007, the Steering Committee appointed Ms. Belkys Sosa as Director for the digital I&C TWGs. Ms. Sosa will coordinate the activities of six Task Working Groups that support the Steering Committee.

Since the formation of the digital I&C Steering Committee, the committee and its various TWGs have conducted numerous public meetings. The public meetings have been successful in engaging the industry in establishing the [Digital I&C Project Plan](#) that addresses specific digital I&C issues. The [Project Plan](#) is a living document and continued interaction between TWGs and their industry counterparts will be beneficial for complete resolution of the issues. The digital I&C Steering Committee and TWGs will continue to meet with the industry to achieve the objectives of the [Project Plan](#). These meeting announcements and summaries can be viewed at the [Digital I&C Public Meetings](#) webpage.



[Privacy Policy](#) | [Site Disclaimer](#)
Wednesday, July 18, 2007



U.S. NRC

UNITED STATES NUCLEAR REGULATORY COMMISSION

Protecting People and the Environment

**Thursday,
July 12, 2007**

PROJECT PLAN

Digital Instrumentation and Control

*Approved by the Digital I&C
Steering Committee*

Revision: 7/12/2007

DIGITAL I&C PROJECT PLAN

PURPOSE:

The purpose of the Digital Instrumentation and Controls (I&C) Project Plan is to identify the objectives and the scope of the project including the short-term and long-term deliverables. The Project Plan defines the roles and responsibilities of the digital I&C Steering Committee and the Task Working Groups (TWGs). It describes the process to develop Interim Staff Guidance (ISG) for the review of digital I&C technology for new reactors, operating reactors, and fuel cycle facilities. The digital I&C project plan accounts for issues related to the review of the anticipated licensing actions including digital upgrades at operating reactors and fuel cycle facilities, new reactor Combined License (COL) and Design Certification applications, and new fuel facilities.

OBJECTIVES:

The specific short-term objective of this plan is to identify digital I&C technical and regulatory issues for which ISG can be developed in time to support the review of the anticipated licensing actions. The long-term objectives of this plan are to continue stakeholder interactions to refine and enhance digital I&C regulatory guidance or identify consensus standards that could be endorsed as regulatory guidance. The deliverables associated with the long-term objectives are to develop recommendations that will be used to update the Standard Review Plan (SRP) and Branch Technical Positions (BTPs), and other regulatory documents, e.g., NUREGs or Regulatory Guides (RGs), and revise regulations, as appropriate, through established agency processes.

BACKGROUND:

The basis for the project plan is derived from the November 8, 2006, Commission meeting, the December 6, 2006, Staff Requirements Memorandum (SRM) (ADAMS Accession No. ML0640033), and the January 12, 2007, memorandum from the Executive Director for Operations (EDO) that chartered the Digital I&C Steering Committee (ML063390606). The plan was updated to reflect the Commission's directive following the June 7, 2007, meeting with the Advisory Committee on Reactor Safeguards (ACRS) and the associated SRM M070607, dated June 22, 2007, that directed the staff to include in the Digital I&C Project Plan activities to support development of the final regulatory guidance on diversity and defense-in-depth.

DIGITAL I&C STEERING COMMITTEE:

The Digital I&C Steering Committee provides oversight and guidance on key digital I&C technical and regulatory issues, and interfaces with industry on those issues. The primary responsibilities of the Steering Committee are (1) to interface with industry representatives on plans for resolution of digital I&C issues, (2) to oversee and facilitate resolution of technical and regulatory issues related to the deployment of digital I&C, and

(3) to ensure effective inter-office coordination on digital I&C issues. The Steering Committee will monitor the NRC line organizations' progress on Digital I&C Project Plan implementation and review specific goals and deliverables. The Steering Committee will approve the initial Digital I&C Project Plan and subsequent revisions to the plan. The Steering Committee will approve Interim Staff Guidance generated by the Task Working Groups.

TASK WORKING GROUPS:

The digital I&C Task Working Groups (TWGs) were established to include technical staff from appropriate NRC offices to focus on six key areas. The TWGs interactions with industry counterparts were designed to facilitate discussion of technical and regulatory issues and the development of recommendations to effectively address digital I&C concerns for each TWG area. The NRC representatives in each TWG are responsible for the development of their individual TWG project plans and the execution of those plans. The TWGs coordinate actions between groups to ensure consistency and alignment.

INDUSTRY CONTACTS:

The TWGs interface with industry-identified contacts in each of the key areas. The industry contacts will interact as necessary with reactor vendors, licensees, applicants, and other industry stakeholders to obtain design information that may be needed to support the work of the TWGs.

The industry contacts have provided input to the problem statements, deliverables, and milestones related to individual TWG project plan objectives. The industry contacts have provide input on the schedules for completing the deliverables. Some industry contacts have indicated that they will provide technical papers to the TWGs to address specific issues. The TWGs have considered industry's input in the development of the project plan.

NRC LINE ORGANIZATIONS:

The NRC line organizations will schedule and perform tasks identified in the individual TWG project plans. The line organizations will interface with the TWGs and report to the Steering Committee on progress, status, problems, and timeliness for preparing short-term deliverables such as Interim Staff Guidance and the long-term deliverables such as recommendations to revise regulatory guidance, and recommendations for revision to industry standards, as necessary.

INDIVIDUAL TWG PROJECT PLANS:

The TWGs have developed an individual TWG project plan for each of the 6 key areas:

- TWG #1: Cyber Security
- TWG #2: Diversity and Defense-in-Depth
- TWG #3: Risk-Informing Digital I&C
- TWG #4: Highly-Integrated Control Room–Communications
- TWG #5: Highly-Integrated Control Room–Human Factors
- TWG #6: Licensing Process

MILESTONES AND DELIVERABLES:

The project plan identifies the major milestones and planned deliverable dates for the TWG activities. The short-term deliverable dates are driven by the need to have ISG in place to review anticipated licensing actions for operating reactors, new reactors, and fuel cycle facilities. The TWG interactions with industry provide the necessary vehicle for updating the short-term and long-term deliverable dates based on identified industry needs for the development of design and procurement specification new plant simulators and for the design and implementation of digital retrofits at existing plants.

UPDATE PROCESS:

The Steering Committee will approve the initial Digital I&C Project Plan and subsequent revisions to the Digital I&C Project Plan.

The project plan represents a significant effort across multiple program offices and requires commitment of time from key managers and technical staff. The availability of resources, the need for contract effort, and the schedule for deliverables will be updated on a continual basis through insights from an enterprise project management tool. As resource, workload, and availability information increase in resolution, so will the forecasted dates identified for the long-term activities in this plan. Where "To Be Determined (TBD)" is indicated in this plan, specific dates are being developed. As the TWGs project efforts proceed, and industry planning data increases in resolution, deliverable dates will be identified for long-term activities that reflect best-estimates from planning-tool insights. The best-estimates will consider information on resource impacts, current schedules and budgets.

APPENDICES:

1. Project Plan - TWG # 1 Cyber Security
2. Project Plan - TWG # 2 Diversity and Defense-In-Depth
3. Project Plan - TWG # 3 Risk-Informing Digital I&C
4. Project Plan - TWG # 4 Highly Integrated Control Room - Communications
5. Project Plan - TWG # 5 Highly Integrated Control Room - Human Factors
6. Project Plan - TWG # 6 Licensing Process Issues

TWG #1: CYBER SECURITY

1. BACKGROUND:

In December 2005 the NRC Office of Nuclear Security and Incident Response (NSIR) endorsed Nuclear Energy Institute (NEI) guidance document NEI 04-04, "Cyber Security Programs for Power Reactors," Revision 1, dated November 18, 2005, as an acceptable method for establishing and maintaining a cyber security program at nuclear power plants. In January 2006, the NRC published Revision 2 to Regulatory Guide (RG) 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," as "acceptable for complying with the Commission's regulations for promoting high functional reliability, design quality, and cyber security for the use of digital computers in safety systems of nuclear power plants."

In October 2006, NRC, NEI, and industry representatives met and discussed, among other things, how to resolve differences between the various regulatory guidance documents pertaining to cyber security of power reactors. The primary objective of this effort will be to provide a coherent set of guidance for future Combined License (COL) applications, or existing licensees who may be developing plant-specific Digital Instrumentation and Control (DI&C) system upgrades. A specific problem statement (see Section 3) was developed based on the October 2006 meeting and subsequent input from industry for consideration by the Cyber Security Task Working Group (TWG#1).

2. SCOPE:

TWG #1 will be focusing its efforts in addressing inconsistencies within existing NRC and industry cyber security guidance documents. Specifically, the working group will be evaluating the differences between Regulatory Guide 1.152, and NEI 04-04. Chapter 7 of the SRP (e.g., SRP Appendix 7.1-D) will be reviewed to assure consistent cyber security guidance. The resulting deliverable will be used to modify these documents to build a coherent set of guidance. These documents will potentially be consolidated to provide consistent guidance based on existing requirements.

The development of guidance documents in support of the final cyber security rule, 10CFR73.55(m), is beyond the scope of this working group. The evaluation of specific cyber security technologies, such as firewalls and intrusion detection systems (IDS), is also not within the scope of this task.

3. PROBLEM STATEMENT:

Problem 1 Cyber Security Requirements for Safety Systems: Regulatory Positions 2.1 - 2.9 of RG 1.152 and NEI 04-04 provide conflicting guidance for implementing cyber security requirements for safety systems at nuclear power plants.

4. DELIVERABLES:

1. Cyber Security Requirements for Safety Systems: Develop Interim Staff Guidance to document the regulatory and design guidance developed by the Cyber Security TWG #1 relative to cyber security for digital systems used at nuclear power plants. Fuel cycle facilities may also use this guidance, as appropriate.

5. Milestones, Assignments, and Deliverables:

TWG#1: CYBER SECURITY					
Milestones, Assignments and Deliverables	Deliverable	Due date	Fcst/Actual	Lead	Support
NEAR-TERM					
Problem 1: Cyber Security Requirements for Safety Systems					
Complete gap analysis of RG1.152R2 and NEI 04-04	✓	Apr 30	A	NRC	NEI
Industry to provide changes to NEI 04-04 to address issues identified in the gap analysis	✓	Jul 19	F	NEI	n/a
Issue draft Interim Staff Guidance	✓	Jul 20	F	NRC	n/a
Discuss draft Interim Staff Guidance in public meeting		Aug 14	F	NRC	NEI
Receive comments		Aug 22	F	NRC	n/a
Issue Interim Staff Guidance	✓	Sep 28	F	NRC	n/a
LONG-TERM					
Problem 1: Cyber Security Requirements for Safety Systems					
Review Industry developed consensus standard that addresses acceptable cyber security practices		TBD		NRC	n/a
Recommend revisions to RG 1.152 and SRP	✓	TBD		NRC	n/a
Complete rulemaking on 10CFR73.55(m)	✓	TBD		NRC	n/a
ACRS Interaction (as needed)		TBD		NRC	n/a
CRGR Interaction (as needed)		TBD		NRC	n/a
Issue draft regulatory guidance related to proposed rule 10CFR73.55(m), including endorsement of industry standard(s)	✓	TBD		NRC	n/a

TWG#1: CYBER SECURITY					
Milestones, Assignments and Deliverables	Deliverable	Due date	Fcst/Actual	Lead	Support
Issue revised RG	✓	TBD		NRC*	n/a
Issue revised SRP	✓	TBD		NRC*	n/a

* Issuance of revisions to RGs and SRP will be conducted through established agency process.

TWG # 2: DIVERSITY AND DEFENSE-IN-DEPTH

1. BACKGROUND:

NRC regulations require licensees to incorporate diversity and defense-in-depth into a nuclear facility's overall safety strategy to ensure that abnormal operating occurrences and design basis events do not adversely affect public health and safety. The responsibility for incorporating appropriate diverse systems and defense-in-depth approaches into safety system designs lies with the licensee. The responsibility for independently evaluating the design lies with the NRC.

Historically, safety system designers have relied on three strategies for addressing potential common cause failures (CCFs): functional defense-in-depth, functional diversity, and system diversity. These approaches have worked well in analog protection systems because CCFs were assumed to be caused by slow processes such as corrosion and equipment wearing out, which could be identified by an operator in sufficient time to prevent multiple failures. This assumption, while shown to be valid for analog safety systems, does not fully address the potential for CCFs in software-based safety systems.

Implicit in the development of digital safety systems is the need to eliminate or mitigate the effects of potential CCFs during the safety system development process. However, the ability to identify CCF vulnerabilities during the system development phase has become especially problematic as the complexity of safety systems has increased. Consequently, the NRC published requirements and guidance for identifying and mitigating CCFs by analyzing safety system designs to ensure an acceptable level of diversity and defense-in-depth was present.

Guidance for performing diversity and defense-in-depth analyses of systems to identify appropriate diversity and defense-in-depth in nuclear power plant instrumentation and control system designs is provided in NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems" (ML9501180332), as well as Branch Technical Position (BTP) 7-19, "Guidance on Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems" [Chapter 7, "Instrumentation and Controls," of NUREG-0800, "Standard Review Plan for Review of Safety Analysis Reports for Nuclear Power Plants"]. This guidance was developed for nuclear power plant safety systems; however, the diversity attributes and associated criteria identified in the guidance are applicable for other nuclear facilities as well. The intention of this guidance is to provide the licensee and the staff a means for assessing whether additional diversity is required in a digital safety system on the basis of the safety system and nuclear power plant design features. The industry indicated that guidance to address the problem statements identified below is needed to provide additional details for clarification and to reduce potential regulatory uncertainty.

The NRC staff is also working closely with the industry to improve the current guidance as appropriate, and the Diversity and Defense-in-Depth Task Working Group (TWG#2) will develop guidelines and recommendations for confirming that sufficient diversity and defense-in-depth has been incorporated into a digital safety system design.

In addition, the NRC staff has been interacting with the Advisory Committee on Reactor Safeguards (ACRS) on this subject. Recently, ACRS made recommendations regarding diversity and defense-in-depth following its meeting with the staff on Digital I&C. The digital I&C project plan has been updated to include two action items: (1) Develop an inventory and classification (e.g., by function or other characteristics) of the various types of digital hardware and software systems that are being used and are likely to be used in nuclear power plants, and (2) Evaluate the operating experience with digital systems in the nuclear and other industries to obtain insights regarding potential failure modes. Insights developed from these actions are expected to be useful as the staff develops and refines regulatory guidance for diversity and defense-in-depth.

2. SCOPE:

The following areas and associated activities will be addressed by TWG #2:

- a. Describe existing regulatory requirements and regulatory guidance associated with diversity and defense-in-depth requirements, without consideration of specific nuclear facility designs (e.g., existing nuclear power plant designs and new nuclear power plant designs). This description will define the recommended boundaries for the ultimate products of TWG #2.
- b. Identify acceptable diversity and defense-in-depth strategies for implementing digital safety functions and systems. The strategies will be based upon existing guidance and the approaches taken by other countries, industries, and agencies; and upon recommendations from the scientific community and academia.
- c. Determine the criteria supporting operator actions in lieu of automated system responses to design basis and other accidents. For example, when operator responses to instrumentation indications could be credited for mitigating certain types of design basis accidents.
- d. Identify consensus standards that could be endorsed as regulatory guidance. For example, ANSI/ANS Std 58.8-1994 © (2001), "Time Response Design Criteria for Safety-Related Operator Actions," may provide acceptable guidance for crediting operator actions as part of a diversity strategy for certain classes of design basis events.
- e. Develop one or more Interim Staff Guidance (ISG) documents to document, by inclusion or reference, the guidance developed or identified by this TWG. The ISG will include references to suitable standards and other guidance that can be used to develop and license safety system diversity and defense-in-depth features.

- f. Recommend ISG to be incorporated into NRC Standard Review Plans and other regulatory guidance.
- g. Address the action items stemming from the Commission meeting with the ACRS.

3. PROBLEM STATEMENT:

Nuclear industry and NRC guidance does not explicitly identify what constitutes acceptable diversity and defense-in-depth in nuclear facility safety system designs. The following issues should be addressed to resolve this issue.

- Problem 1 Adequate Diversity: Additional clarity is desired on what constitutes adequate diversity and defense-in-depth. Determine: 1) How much diversity and defense-in-depth is enough; 2) If there are precedents for good engineering practice; 3) If sets of diversity attributes and criteria can provide adequate diversity; 4) How much credit can be taken for designed-in robustness in determining the required amount of diversity; and 5) Identify consensus standards that could be endorsed, if available.
- Problem 2 Manual Operator Actions: Clarification is desired on the use of operator action as a defensive measure and corresponding acceptable operator action times.
- Problem 3 BTP-19 Position 4 Challenges: Current guidance policy addresses system-level actuation in BTP-19, Position 4. Industry has proposed that further clarification is needed relative to when and if credit can be taken for component-level versus system-level actuation of equipment. Clarification is needed on the rationale for when and why BTP-19, Position 4 would not be applicable.
- Problem 4 Effects of Common-Cause Failure: BTP-19 guidance recommends consideration of CCFs that "disable a safety function." However, additional clarity is desired regarding the effects that should be considered (e.g., fails to actuate and/or spurious actuation).
- Problem 5 Common-Cause Failure Applicability: Clarification is desired on identification of design attributes that are sufficient to eliminate consideration of CCFs (e.g., degree of simplicity).
- Problem 6 Echelons of Defense: As described in NUREG-0737 Supplement 1, "Clarification of TMI Action Plan Requirements," the following plant safety functions must be controlled to mitigate plant accidents:
- 1. Reactivity control
 - 2. Reactor core cooling and heat removal from the primary system

3. Reactor coolant system integrity
4. Radioactivity control
5. Containment conditions

BTP-19 guidance references the following echelons of defense described in NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems" for maintaining the above safety functions within safe margins for nuclear power plants:

1. Control systems
2. Reactor Trip System (RTS)
3. Engineered Safety Features Actuation System (ESFAS)
4. Monitoring and indications

Additional clarification is desired regarding how the echelons of defense for maintaining the above safety functions should factor into diversity and defense-in-depth analyses. A particular concern is that the current BTP-19 guidance does not consider plant design characteristics and operating procedures that affect how diversity and defense-in-depth are actually used to maintain the safety functions.

Problem 7 Single Failure: Additional clarification is needed regarding the acceptance criteria for addressing CCFs versus the acceptance criteria for addressing single failures in safety system designs.

4. DELIVERABLES:

The Diversity and Defense-in-Depth TWG #2 will develop near-term ISGs for the problem statements by September 30, 2007, as necessary. Additional guidance may be developed as part of the long-term activities, as necessary. TWG #2 will recommend the ISGs to be incorporated into the SRP and other regulatory documents, e.g., NUREG or Regulatory Guides, in the longer term, as needed. TWG #2 will address the following issues and propose the following specific products:

1. Adequate Diversity: ISG will be developed by September 30, 2007. Additional ISG will be developed regarding adequate diversity that considers engineering approaches and acceptance criteria that have been developed in other countries, industries, and agencies. Additionally, academia and scientific organization recommendations for implementing appropriate diversity and defense-in-depth strategies will be considered in developing the guidance.
2. Manual Operator Actions: ISG will be developed that describes the conditions under which operator actions can be credited as a diverse method for initiating safety functions. Development of this guidance will be coordinated with the efforts of the Highly Integrated Control Room - Human Factors TWG #5.

3. BTP-19, Position 4 Challenges: ISG will be developed that describes the conditions under which credit can be taken for component-level versus system-level actuation of equipment. This guidance will address upgrades for currently operating nuclear plants and fuel cycle facilities, as well as new plant designs. Changes to BTP-19 may be recommended to make the guidance generically applicable to all plant designs.
4. Effects of Common-Cause Failure (CCF): BTP-19 guidance recommends consideration of CCFs that "disable a safety function." ISG will be developed to guide the process for evaluating potential CCF analyses and for specifying the failure states that should be integrated into safety system design basis analyses (e.g., fails to actuate and/or spurious actuation).
5. Common-Cause Failure Applicability: ISG will be developed for digital system design attributes that are sufficient to eliminate consideration of CCFs. These attributes will include recommended diversity strategies and acceptance criteria for attributes such as degree of simplicity, complexity, and robustness.
6. Echelons of Defense: ISG will be developed to describe appropriate levels of defense-in-depth in safety system designs.
7. Single Failure: ISG will be developed that addresses the conditions under which software failures are to be considered CCFs or single failures in plant design basis analyses.

5. MILESTONES, ASSIGNMENTS, AND DELIVERABLES:

TWG #2: DIVERSITY AND DEFENSE-IN-DEPTH					
Milestones, Assignments and Deliverables Diversity and Defense-in-Depth	Deliverable	Due Date	Fcst/Actual	Lead	Support
NEAR-TERM					
Problem 1: Adequate Diversity					
Develop draft Interim Staff Guidance		Jun 21	A	NRC	N/A
Issue draft Interim Staff Guidance	✓	Jun 22	A	NRC	n/a
Discuss draft Interim Staff Guidance in public meeting		Jun 22	A	NRC	NEI
Receive comments		July 6	A	NRC	n/a
Issue Interim Staff Guidance	✓	Sep 28	F	NRC	n/a
Problem 2: Manual Operator Action					
Develop draft Interim Staff Guidance		Jun 14	A	NRC	NEI
Issue draft Interim Staff Guidance	✓	Jun 22	A	NRC	n/a
Discuss draft Interim Staff Guidance in public meeting		Jun 22	A	NRC	NEI
Receive comments		Jul 6	A	NRC	n/a
Industry to provide white paper		Jul	F	NEI	n/a
Issue Interim Staff Guidance	✓	Sep 28	F	NRC	n/a
Problem 3: BTP-19, Position 4 Challenges Problem 4: Effects of Common-Cause Failure Problem 5: Common-Cause Failure Applicability Problem 6: Echelons of Defense Problem 7: Single Failure					
Industry to provide white paper on Effects of Common-Cause Failure	✓	Jul 20	F	NEI	n/a

TWG #2: DIVERSITY AND DEFENSE-IN-DEPTH					
Milestones, Assignments and Deliverables Diversity and Defense-in-Depth	Deliverable	Due Date	Fcst/Actual	Lead	Support
Develop draft Interim Staff Guidance		Aug 6	F	NRC	NEI
Issue draft Interim Staff Guidance	✓	Aug 10	F	NRC	n/a
Discuss draft Interim Staff Guidance in public meeting		Aug 14	F	NRC	NEI
Receive comments		Aug 22	F	NRC	n/a
Industry to provide white paper on Common-Cause Failure Applicability	✓	Aug 31	F	NEI	n/a
Issue Interim Staff Guidance	✓	Sep 28	F	NRC	n/a
Inventory and Classification of Digital Systems					
Develop draft assessment results	✓	Sep 28	F	NRC	n/a
Provide assessment results with appropriate recommendations on staff guidance	✓	Dec 31	F	NRC	n/a
Evaluation of Digital Systems Operating Experience Insights					
Develop draft assessment results	✓	Sep 28	F	NRC	n/a
Provide assessment results with appropriate recommendations on staff guidance	✓	Dec 31	F	NRC	n/a

TWG #2: DIVERSITY AND DEFENSE-IN-DEPTH					
Milestones, Assignments and Deliverables Diversity and Defense-in-Depth	Deliverable	Due Date	Fcst/Actual	Lead	Support
LONG-TERM					
Problem 1: Adequate Diversity					
Develop revised draft Interim Staff Guidance		Oct 1	F	NRC	N/A
Issue draft Interim Staff Guidance	✓	Oct	F	NRC	n/a
Discuss draft Interim Staff Guidance in public meeting		Oct	F	NRC	NEI
Receive comments		Nov	F	NRC	n/a
Issue Interim Staff Guidance	✓	Dec	F	NRC	n/a
Common Long-Term Actions for All Problem Statements					
Work with other organizations to incorporate diversity and defense-in-depth standards into consensus standards, as appropriate		TBD	F	NRC	n/a
Recommend revisions to SRP, BTP, and other regulatory documents, e.g., NUREG or Regulatory Guides, as appropriate.	✓	TBD	F	NRC	n/a
ACRS interaction (as needed)		TBD	F	NRC	n/a
CRGR interaction (as needed)		TBD	F	NRC	n/a
Issue revised RG	✓	TBD	F	NRC*	n/a
Issue revised SRP	✓	TBD	F	NRC*	n/a

* Issuance of revisions to RGs and SRP will be conducted through established agency process.

TWG #3: RISK-INFORMING DIGITAL I&C

1. BACKGROUND:

The Risk-Informing Digital Instrumentation and Control (RIDIC) Task Working Group (TWG #3) will address issues related to the risk assessment of digital systems with particular emphasis on risk-informing digital system reviews for operating plants, new reactors and fuel cycle facilities. The TWG efforts will be consistent with the NRC's policy statement on probabilistic risk assessment (PRA), which states, in part, the NRC supports the use of PRA in regulatory matters "to the extent supported by the state-of-the-art in PRA methods and data and in a manner that complements the NRC's deterministic approach and supports the NRC's traditional defense-in-depth philosophy."

Although digital I&C systems are intended to be at least as reliable as the analog systems they replace, digital systems have unique failure modes. Of significant concern are digital I&C system common cause failures that can propagate to multiple safety channels and divisions thereby defeating the defense-in-depth and diversity that was considered adequate for an analog I&C system. Since digital systems play an increasingly important role in nuclear facility control and safety systems, the need for risk assessment methods for digital I&C systems is evident.

The current methodology for evaluating a digital I&C system in either an operating plant or new reactor involves a broad range of deterministic guidance for the development, testing, implementation, and maintenance of digital systems to manage digital system failures. This guidance is "process based" in that the regulatory guidance is designed to provide software and hardware of "high quality" with adequate diversity (of various types) such that the potential for failure, including common cause, is minimized. Specific guidance is provided to assess defense-in-depth and diversity by identifying potential vulnerabilities to digital system common cause failures that could disable a safety function. Where potential vulnerabilities are identified, diverse means are put in place to perform either that safety function or a different safety function. However, these reviews typically involve significant staff effort in the determination of adequate defense-in-depth and diversity when using current staff guidance.

To address this, TWG #3 task will evaluate the feasibility of risk-informing the digital system evaluations with the intent of improving the effectiveness and efficiency of the digital system review process while adhering to the five key principles of risk-informed decision-making including adequate defense-in-depth and diversity when implementing a digital I&C system either as a retrofit or new reactor installation.

2. SCOPE:

One of the key concerns with the current state-of-the-art in digital system modeling is it does not yet support risk-informed decision-making for digital systems, particularly with respect to software reliability quantification. Therefore, adequate digital system risk and reliability methods are needed to support the integration of digital systems into a risk evaluation method. After this risk method is developed, the NRC must also develop additional staff policy or guidance to support risk-informing digital system reviews.

As part of risk-informing the current regulatory process for the review of digital systems, there is a need to develop NRC guidelines to establish quality and completeness of digital system risk and reliability modeling in current generation plant PRAs and PRAs being developed to support Part 52 Design Certifications (DC) and Combined Licensee (COL) applications. These PRAs need to be completed in the near-term. Although current guidance (i.e., Regulatory Guide 1.200) provides attributes associated with PRA quality, there is limited guidance available as to the completeness of digital I&C system modeling, the level of detail needed in digital I&C system modeling, and the uncertainties associated with digital system modeling. Guidance as to what risk metrics are appropriate for evaluating digital I&C systems in operating reactors and DC and COL PRAs also may be needed. Additionally, in the near-term, guidance on how risk-insights could be used to support digital I&C systems reviews in the evaluation of key digital system issues, such as diversity and defense-in-depth and inter-channel communications is needed.

The NRC is actively working to develop tools and methods to perform risk assessments of nuclear power plant digital systems. NRC is investigating both traditional fault tree/event tree methods and dynamic methods that may be used to support risk-informed digital system reviews. The NRC staff recognizes the industry's interest in risk-informing digital system reviews, and seeks to leverage insights and approaches developed by industry in the staff resolution process. However, the NRC also recognizes the challenges in integrating digital systems into PRAs and the practicality of using a PRA to assess digital systems. Therefore, guidance on how to risk-inform digital system applications and associated performance based acceptance guidelines to support licensing of operating reactor upgrades, new reactors, and fuel cycle facilities is also needed.

TWG #3 recommendations are not expected to involve changes to NRC policy or rulemaking. However, recommendations proposed may impact the regulatory burden for both NRC staff and industry. When developing recommendations, these burdens will be considered in conjunction with the potential benefit.

Therefore, the following will be addressed by the TWG #3:

- a. The use and application of risk-insights in the evaluation of digital I&C systems for both operating and new reactors.

- b. Tools and methodologies to enable improved risk assessments of digital I&C systems in nuclear power plants.
- c. Regulatory guidance to enable the use of risk-informed decision-making in the evaluation of digital I&C systems for operating and new reactors.

The following define the limitations of the scope of TWG #3:

- a. Work products will be consistent with the five key principles of risk-informed decision-making
- b. Work products will be consistent with the Commission direction outlined in Staff Requirements Memorandum (SRM) to SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light Water Reactors (ALWR) Designs".
- c. Security issues (i.e, cyber security) are not within the scope of TWG #3.

3. PROBLEM STATEMENT:

The NRC and nuclear power industry share the goal of risk-informing the decision-making in licensing reviews of digital systems for current and future reactors and fuel facilities. However, currently there is no detailed guidance on what would constitute adequate digital system modeling in probabilistic risk assessments (PRAs), including: modeling of digital system common-cause failures (including software), level of modeling detail, failure data, adequacy of modeling methods, uncertainties and interfacing digital system models with the rest of the PRA. There is also no detailed guidance on integrating risk insights into digital system reviews or risk-informing digital system reviews.

PROBLEM 1 Modeling Digital Systems in PRA: Existing guidance does not provide sufficient clarity on how to use current methods to properly model digital systems in PRAs for design certificate applications or license applications (COL) under Part 52. The issue includes addressing common-cause failure modeling and uncertainty analysis associated with digital systems.

PROBLEM 2 Risk Insights: Using current methods for PRAs, NRC has not determined how or if risk-insights can be used to assist in the resolution of specific key digital system issues.

PROBLEM 3 State-of-the-Art: An acceptable state-of-the-art method for detailed modeling of digital systems has not been established. An advancement in the state-of-the-art is needed to permit a comprehensive risk-informed decision making framework in licensing reviews of digital systems

4. DELIVERABLES:

1. Modeling Digital Systems in PRA:

- a. Issue guidance addressing use of current methods in modeling of digital systems for design certification and COL application PRAs.
- b. In the longer-term, update regulatory guidance as needed (SRP, Regulatory Guides, etc.).

2. Risk Insights:

- a. Develop, if possible, an acceptable approach for using risk insights to assist in the resolution of specific key digital system issues. Include consideration of proposed industry methods.
- b. If an acceptable approach can be established, issue guidance and acceptance criteria for use of risk insights in digital systems.
- c. In the longer-term, update regulatory guidance as needed (SRP, Regulatory Guides, etc.).

3. State-of-the-Art:

- a. Identify an approach to implement appropriate collaboration with and leverage the capabilities of the industry, international counterparts, other industries and NRC staff and contractors to develop the technical basis for state-of-the-art methods for modeling of digital systems to support risk-informed decision-making for digital systems, including: (1) review of current modeling methods (including software modeling), (2) characteristics of acceptable modeling methods, (3) assessment of failure data, (4) criteria for level of modeling detail, (5) assessment of uncertainties, and (6) defining how to interface digital system models with the rest of the PRA.
- b. Issue regulatory guidance on risk-informed decision-making review methods applicable to digital I&C systems.
- c. Update NRC PRA data, models and tools to support NRC assessment of digital system risk and reliability.

5. MILESTONES, ASSIGNMENTS, AND DELIVERABLES:

TWG#3: RISK-INFORMING					
Milestones, Assignments and Deliverables	Deliverable	Due date	Fcst/Actual	Lead	Support
NEAR-TERM					
Problem 1: Modeling Digital Systems in PRA					
Industry to provide white paper discussing lessons-learned and proposed guidelines associated with modeling of digital systems for DC and COL applications	✓	Jul 3	A	NEI	n/a
Develop draft Interim Staff Guidance		Nov 23	F	NRC	n/a
Issue draft Interim Staff Guidance	✓	Nov 28	F	NRC	n/a
Discuss draft Interim Staff Guidance in public meeting		Nov 30	F	NRC	NEI
Receive comments		Dec 7	F	NRC	n/a
Issue Interim Staff Guidance	✓	Mar 2008	F	NRC	n/a
Problem 2: Risk Insights					
Industry provides white paper that proposes simplified modeling methods using risk insights to support reviews of digital systems.	✓	Aug	F	NEI	n/a
Problem 3: State-of-the-Art					
No near-term deliverables					

TWG#3: RISK-INFORMING					
Milestones, Assignments and Deliverables	Deliverable	Due date	Fcst/Actual	Lead	Support
LONG-TERM					
Problem 1: Modeling Digital Systems in PRA					
No long-term deliverables					
Problem 2: Risk Insights					
Consider industry white paper		TBD	F	NRC	n/a
Initiate Regulatory Guidance revisions as appropriate		TBD	F	NRC	n/a
Problem 3: State-of-the-Art					
Develop risk-informed decision-making review methods applicable to digital systems	✓	TBD	F	NRC	n/a
Initiate Regulatory Guidance revisions as appropriate		TBD	F	NRC	n/a

TWG#3: RISK-INFORMING					
Milestones, Assignments and Deliverables	Deliverable	Due date	Fcst/Actual	Lead	Support
Common Long-Term Actions for All Problem Statements					
Work with other organizations to incorporate risk assessment guidance into consensus standards, as appropriate				NRC	NEI
Recommend revisions to SRP and other regulatory documents, e.g., NUREG or Regulatory Guides, as appropriate.	✓	TBD	F	NRC	n/a
ACRS interaction (as needed)		TBD	F	NRC	n/a
CRGR interaction (as needed)		TBD	F	NRC	n/a
Issue revised RG	✓	TBD	F	NRC*	n/a
Issue revised SRP	✓	TBD	F	NRC*	n/a

* Issuance of revisions to RGs and SRP will be conducted through established agency process.

TWG #4: HIGHLY-INTEGRATED CONTROL ROOM— COMMUNICATIONS

1. BACKGROUND:

The Highly Integrated Control Room-Communications Issues (HICRc) Task Working Group (TWG) will address HICR design issues related to communications involving digital equipment in nuclear safety service. This action is needed to support development of the design and procurement specification for simulators for new plants and for the design and implementation of digital retrofits at existing plants. Specifically, this TWG will address all communication design provisions between safety divisions¹, and between safety and non safety divisions. In this context, “communication” means any transmittal or reception of data, information, or commands.

There are clear potential advantages to the implementation of some types of cross-divisional communication within digital systems. However, preservation of adequate independence for digital systems communications is essential. The objective of this task working group is to evaluate cross-divisional communication interactions and to clarify design and licensing criteria by which beneficial interactions may be accomplished while maintaining adequate safety margin.

2. SCOPE:

The following types of communication interactions will be addressed by TWG #4:

- a. Communication among redundant electrical divisions
- b. Communication between any safety channel and anything external to that channel's division
- c. Control of safety equipment in multiple divisions from a single workstation
- d. Control of safety equipment from a nonsafety workstation
- e. Commingling of safety and nonsafety controls or indications on a single workstation
- f. Connection of nonsafety programming, maintenance, and test equipment to redundant safety divisions during operation

The following are explicitly excluded from the scope of this task:

- g. Communication within a single safety division
- h. Communications which do not involve a safety channel

¹ The terms “channel” and “division” are used herein in accordance with the definitions of those terms in IEEE 603-1991.

Cyber-Security, Diversity and Defense-in-Depth, and Human Factors (HF) considerations are all closely related to the general concept of cross-divisional communications. These issues are being addressed by TWGs #1, #2, and #5, respectively. Therefore coordination with each associated TWG will be necessary to ensure that HICRc TWG #4 activities are consistent with, and supportive of, the solutions that they will provide.

Except as specifically addressed in the resolution of the issues identified above, physical separation and electrical isolation requirements for digital equipment are the same as for non-digital equipment. Physical separation and electrical isolation will not be addressed separately in this task. Similarly, seismic and environmental qualification requirements are not included in this task.

3. PROBLEM STATEMENT:

- Problem 1 Inter-Divisional Communications Independence: Industry and NRC guidance documents do not define at a sufficient level of detail the requirements for inter-divisional communications independence.
- a. Industry Standards (e.g. IEEE 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations") do not provide sufficient guidance for inter-divisional communications independence within digital systems.
 - b. NRC regulatory guidance (e.g. Regulatory Guide 1.152, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants") does not provide explicit guidance for inter-divisional communications independence within digital systems.
 - c. The protection system division separation and isolation requirements in existing regulations (10CFR50.55a (h), "Protection and Safety Systems," which incorporates IEEE603-1991, "Criteria for Safety Systems for Nuclear Power Generating Stations," among other things) does not define for digital systems "the degree [of independence] necessary to retain the capability to accomplish the safety function during and following any design basis event requiring that safety function."
 - d. Existing Standard Review Plan (SRP) Chapter 7 includes conflicting guidance regarding communication independence.

4. DELIVERABLES:

1. Inter-Divisional Communications Independence:
 - a. Issue Interim Staff Guidance (ISG) that will document an acceptable degree of communications independence for digital systems.
 - b. Facilitate a revision to IEEE 7-4.3.2.
 - c. Recommend revisions to Regulatory Guide 1.152.
 - d. Recommend updates to the Standard Review Plan guidance to provide acceptable regulatory and licensing criteria for communications independence of digital systems.

5. DISCUSSION:

TWG #4 will consider the possibility that the needs of new and existing facilities are different, and will include accommodation of such differences in the guidance documentation, if necessary. It is initially anticipated that there will be no difference in the guidance for new and existing facilities.

Final guidance relating to control room design is needed to support final specification and design of the simulators for new plants. It is anticipated that the first simulators will need to be ordered in mid-2009, and that about 18 months will be required between the time the guidance is issued and the first simulators are ordered. The guidance is therefore needed by early 2008. To allow for a reasonable amount of schedule float, TWG #4 anticipates completing its ISG by September 30, 2007.

It is noted that support of simulator procurement requires only that the conceptual design of the control room be completed. It does not require that the details of the internal workings of the operator interfaces be fully developed. The efforts of TWG #4 will influence the nature and layout of the control room in that requirements relating to the disposition and application of operator interface workstations could be affected, but those influences will be limited to whether various operator-interface design provisions will or will not be considered acceptable (for example, whether or under what design constraints it might be acceptable for a single control station to include both safety and nonsafety functions). The efforts of other TWGs will have greater influence upon control room design and layout, such as TWG #2 working on Diversity and Defense-in-Depth (D3) requirements, and TWG #5 working on details of Human-Machine Interfaces (HMI) from a Human Factors (HF) standpoint.

TWG #4 will produce guidelines describing appropriate design provisions and limitations. These guidelines will include a statement of the fundamental requirements and specific regulatory criteria that must be observed. The HICRc TWG #4 will also provide recommendations for revisions to RG1.152, IEEE 7-4.3.2, applicable SRP sections, and other regulatory guidance and industry standards as deemed necessary.

TWG #4 will give due consideration to the burdens that might be imposed upon both applicants and NRC staff as a result of specific guidance. For example, acceptance of a certain provision might require detailed staff review in an area not presently subject to such review. This would impose a burden upon an applicant in that additional materials must be assembled for inclusion in the application package, some of which may be proprietary and thus require the development of a redacted version as well as the full version, and upon the NRC in the actual review of the subject details. The cost of such a provision in terms of resources, review effort, and review time extension should be considered in relation to the potential benefits of such an approach relative to an approach that is simpler from a regulatory point of view.

6. CRITICAL PATH AND STEPS TO SUCCESS:

In order to accomplish its mission, the HICRc TWG #4 may need to have timely access to detailed information concerning proposed reactor designs. The TWG will make every reasonable effort to obtain specific design information needed to support its work, relying principally upon the efforts of the industry contacts assigned by NEI. However, if extended correspondence with reactor vendors is required in an effort to obtain the needed information, or if information availability is restricted by intellectual property rights issues or other issues, the TWG may recommend deferral of review of the respective designs until such design details are made available, or recommend other compensatory action to the NRC Digital I&C Steering Committee. In such a case, the TWG would proceed on the basis of generic considerations. The NRC Digital I&C Steering Committee should be advised promptly if such a situation occurs.

The primary efforts of TWG will include the following:

- a. Develop a statement describing the existing regulatory requirements and regulatory guidance associated with cross-divisional interactions, without consideration of specific proposed designs. This statement will establish the fundamental restrictions and requirements, or boundaries, for the ultimate products of TWG #4.
- b. Develop a detailed and prioritized listing of the design concepts to be considered by TWG #4. The TWG will address the associated design and licensing issues in accordance with this prioritization. To support the development and prioritization of this listing, the TWG will request that the industry contacts provide their collective best estimate of the types of cross-channel interactions that have actually been proposed or planned, with indication of the level of interest in the use of each type. Consideration should include new plants, existing plants, and fuel cycle facilities. The objective of this information is to ensure that TWG #4 addresses the types of interactions that are of greatest interest to industry. For example, perhaps many system designers plan to use scratchpad-based data exchange and some but very few plan to use Ethernet-based direct communication between safety processors: then TWG #4 would address the more widespread practice first and the less widespread practice later. If it determines that some type of interaction is planned for use by only a very few

suppliers but that type of interaction is highly desirable or problematical, TWG #4 may choose to address that issue early in order to inform stakeholders of the type of interaction that may be easy or difficult to license.²

- c. Obtain preliminary results of the on-going NRC/RES research project concerning communications issues regarding highly-integrated control rooms. This research is exploring similar issues in other countries, and it is expected that the results may be useful to TWG #4.
- d. Develop a list of regulatory and design requirements applicable to each type of interaction. Include the basis for each requirement.
- e. Develop a draft annotated outline for the guidance document(s), including draft acceptance criteria for each item.
- f. Industry (via its TWG representative) review and comment on the draft outline and proposed acceptance criteria.
- g. Develop detailed guidance recommendations to be implemented in the Interim Staff Guidance document(s).
- h. Develop regulatory and design guidance document(s) addressing communications independence for digital systems. The guidance should include specific acceptance criteria for types of interactions found to be acceptable, and should also include descriptions of types of interactions found to be unacceptable.

² This prioritization will not preclude or affect NRC consideration of interactions proposed in license requests that have already been submitted or that are submitted in the future. License requests that fall outside the recommendations of the TWG or that are contrary to them will be considered by the NRC on a case-by-case basis.

7. MILESTONES, ASSIGNMENTS, AND DELIVERABLES:

TWG #4: Highly-Integrated Control Room—Communications					
Milestones, Assignments and Deliverables	Deliverable	Due date	Fcst/Actual	Lead	Support
NEAR-TERM					
Problem 1: Communications Independence					
Identify regulatory & design requirements with basis for each type of interaction		Mar 8	A	NRC	NEI
Receive industry proposals for HICR communication design concepts	✓	Jun 1	A	NEI	n/a
Issue draft Interim Staff Guidance	✓	Aug 10	F	NRC	n/a
Discuss draft Interim Staff Guidance in public meeting		Aug 14	F	NRC	NEI
Receive comments		Aug 22	F	NRC	n/a
Issue Interim Staff Guidance	✓	Sep 28	F	NRC	n/a
LONG-TERM					
Problem 1: Communications Independence					
Industry to work with IEEE on modifications to 7-4.3.2 and issue	✓	TBD	F	NEI	NRC
Recommend revisions to SRP and other regulatory documents, e.g., NUREG or Regulatory Guides (RG 1.152), as appropriate.	✓	TBD	F	NRC	n/a
ACRS Interaction (as needed)		TBD	F	NRC	n/a

TWG #4: Highly-Integrated Control Room—Communications					
Milestones, Assignments and Deliverables	Deliverable	Due date	Fcst/Actual	Lead	Support
CRGR Interaction (as needed)		TBD	F	NRC	n/a
Issue revised RG 1.152	✓	TBD	F	NRC*	n/a
Issue revised SRP	✓	TBD	F	NRC*	n/a

* Issuance of revisions to RGs and SRP will be conducted through established agency process.

TWG #5: HIGHLY INTEGRATED CONTROL ROOM— **HUMAN FACTORS**

1. BACKGROUND:

Nuclear power plant personnel play a vital role in the productive, efficient, and safe generation of electric power, whether for conventional light water reactors (LWRs), advanced light water reactors (ALWRs), new reactors, or fuel cycle facilities. Operators monitor and control plant systems and components to ensure their proper functioning. Test and maintenance personnel help ensure that plant equipment is functioning properly and restore components when malfunctions occur. In order for them to accomplish their tasks safely they need access to accurate and timely information to maintain situation awareness, make informed decisions, and take appropriate actions. The role of the human factors engineering (HFE) regulatory review process is to ensure that the needed information is available.

Operating reactors, new reactors, and fuel-cycle facilities with modernized control stations are expected to present new operational and maintenance environments due to the expanded use of digital systems. This could lead to concepts of operation and maintenance that are significantly different from conventional control rooms. New control rooms are expected to be fully computer-based, that is, fully digitized with computer displays and soft controls. Procedures are likely to be computerized and control actions may be taken directly from the procedure display or automated, with the operator only in the position to monitor and bypass the automation. Different training and qualifications may be required for the plant staff because of the need to focus on monitoring and bypassing automatic systems, rather than taking active control as they do now. Higher-levels of knowledge and training may be needed to respond to situations when automatic systems fail. These activities will pose new and challenging situations for operators and maintainers. Regulatory staff will need new tools, developed from the best available technical bases, to support licensing and oversight tasks. The ultimate goal is to minimize human error contribution to the risk associated with the design, construction, operation, testing, and maintenance of these new facilities.

Current regulations and guidance that address human performance issues were developed primarily for the review of conventional LWRs. New or revised regulations and guidance may need to be developed to address the new generation of control rooms. A sound technical basis needs to be developed as part of the guidance development process. The HFE aspects of new control stations should be developed, designed, and evaluated on the basis of a structured systems analysis using accepted HFE principles at the same time as other systems are being designed. The needs of personnel must be considered as a part of the system design from the initial concept development stage so that the role allocated to personnel is appropriate, as specified in regulatory review guidance such as, NUREG-0711; consensus standards from IEEE and ANS; and industry design guidance from NEI and EPRI.

2. SCOPE:

The scope of this effort is limited to human factors issues for new reactors, conventional LWRs, and, where applicable, fuel cycle facilities. The scope includes human-system interfaces, human to human interface and personnel issues, during design, construction, testing, operations, and maintenance of these facilities. Because of the cross-cutting nature of human factors, the Highly Integrated Control Rooms - Human Factors Task Working Group (TWG #5) will interface with all other Digital I&C TWGs.

3. PROBLEM STATEMENT:

Existing Human Factors Engineering review guidance, regulatory positions, and acceptance criteria could be modified or developed, as needed, to facilitate consistent and efficient licensing of new digital Human-System Interface technology at operating and new reactors and certain fuel facilities.

1. Minimum Inventory. Review existing NRC regulatory positions and acceptance criteria, and make necessary changes, to better define minimum inventory of alarms, controls, and displays needed to implement the emergency operating procedures and bring the plant to a safe condition; eliminate any inconsistencies in the use of minimum inventory that exist in current NRC guidance; and consider development of a process approach to the development of a plant-specific minimum inventory of alarms, displays and controls.
2. Computerized Procedures and Soft Controls. Review existing NRC regulatory guidance, positions, and acceptance criteria, and make necessary changes, to facilitate consistent and efficient licensing of computerized procedures and soft controls in highly integrated control rooms. Develop guidance and acceptance criteria, if necessary, to minimize the impact of degraded digital instrumentation and controls associated with computerized procedures and soft controls on human performance.
3. Safety Parameter Display System (SPDS). Review existing NRC regulatory guidance, positions, and acceptance criteria to determine the need to revise 10CFR50.34 (f)(iv) and associated guidance, and make necessary changes, relative to safety parameter display consoles to ensure consistent understanding of the term "console."
4. Graded Approach to Human Factors. Review existing NRC regulatory guidance, positions, and acceptance criteria, and make necessary changes, to facilitate consistent and efficient licensing using a graded approach to the review of human factors aspects of highly-integrated control rooms.

4. DELIVERABLES:

1-4. All Problem Statements

- a. A listing of regulatory guidance documents, industry standards, and regulations (if needed) that should be revised.
- b. Written feedback/comments on papers prepared by NEI concerning minimum inventory, graded approach to human factors, and manual operator actions in support of TWG #2 and human factors aspects of multi-channel VDUs in support of TWG #4.
- c. Interim Staff Guidance describing or clarifying the current regulatory guidance and acceptance criteria on each of the identified problem areas will be developed.
- d. Final guidance, acceptance criteria, and regulations (if needed) addressing each of the problem areas will be developed.
- e. Recommend revisions to the Standard Review Plan and other regulatory guidance document, as appropriate, to provide acceptable regulatory and licensing criteria for new reactors, modernized LWRs, and fuel facilities.

5. MILESTONES, ASSIGNMENTS, AND DELIVERABLES:

TWG #5: Highly-Integrated Control Room—Human Factors					
Milestones, Assignments and Deliverables	Deliverable	Due Date	Fcst/Actual	Lead	Support
NEAR-TERM					
Problem 1. Minimum Inventory					
Received industry proposal on minimum inventory	✓	May 25	A	NEI	n/a
Industry to provide input for consideration in development of Interim Staff Guidance	✓	Jul 20	F	NEI	n/a
Prepare Interim Staff Guidance		Aug 6	F	NRC	n/a
Issue draft Interim Staff Guidance	✓	Aug 10	F	NRC	n/a
Discuss draft Interim Staff Guidance in public meeting		Aug 14	F	NRC	NEI
Receive comments		Aug 22	F	NRC	n/a
Issue Interim Staff Guidance	✓	Sep 28	F	NRC	n/a
Problem 2. Computerized Procedures and Soft Controls					
Industry to provide input for consideration in development of Interim Staff Guidance	✓	Jul 20	F	NEI	n/a
Prepare Interim Staff Guidance		Aug 6	F	NRC	n/a
Issue draft Interim Staff Guidance	✓	Aug 10	F	NRC	n/a
Discuss draft Interim Staff Guidance in public meeting		Aug 14	F	NRC	NEI
Receive comments		Aug 22	F	NRC	n/a
Industry to provide white paper	✓	Aug 31	F	NEI	n/a
Issue Interim Staff Guidance	✓	Sep 28	F	NRC	n/a

TWG #5: Highly-Integrated Control Room—Human Factors					
Milestones, Assignments and Deliverables	Deliverable	Due Date	Fcst/Actual	Lead	Support
Problem 3. Safety Parameter Display System					
No near-term deliverables					
Problem 4. Graded Approach to Human Factors					
No near-term deliverables					
LONG-TERM					
Problem 1. Minimum Inventory					
Develop guidance revision as appropriate		TBD	F	NRC	n/a
Problem 2. Computerized Procedures and Soft Controls					
Develop guidance revision as appropriate		TBD	F	NRC	n/a
Problem 3. Safety Parameter Display System					
Review safety parameter display system and related guidance to determine if gaps or inadequacies exist as related to digital systems to determine if 10CFR50.34(f) needs to be revised so that exemptions would not be needed to address SPDS and related functions		TBD	F	NRC	NEI
Document results of review					
Develop guidance and/or make revisions as appropriate		TBD	F	NRC	n/a
Problem 4. Graded Approach to Human Factors					
Receive industry proposal on graded approach to human factors		Sep	F	NEI	n/a
Review and comment on industry proposal		TBD	F	NRC	n/a
Develop guidance revision as appropriate		TBD	F	NRC	n/a

TWG #5: Highly-Integrated Control Room—Human Factors					
Milestones, Assignments and Deliverables	Deliverable	Due Date	Fcst/Actual	Lead	Support
Common Long-Term Actions for All Problem Statements					
Recommend revisions to SRP and other regulatory documents, e.g., NUREG or Regulatory Guides, as appropriate.	✓	TBD	F	NRC	n/a
ACRS interaction (as needed)		TBD	F	NRC	n/a
CRGR interaction (as needed)		TBD	F	NRC	n/a
Issue revised RG	✓	TBD	F	NRC*	n/a
Issue revised SRP	✓	TBD	F	NRC*	n/a

* Issuance of revisions to RGs and SRP will be conducted through established agency process.

TWG # 6: LICENSING PROCESS

1. BACKGROUND:

Guidance for the content of license applications and amendments involving licensing digital instrumentation and control (I&C) systems and components is contained in Regulatory Guide 1.206 (Combined License Applications for Nuclear Power Plants - LWR Edition) and Chapter 7 (Instrumentation and Controls) of NUREG-0800 (Standard Review Plan (SRP) for the Review of Safety Analysis Reports for Nuclear Power Plants). RG 1.206 was issued for preliminary use on March 30, 2007, and several revised sections of the SRP have been published recently.

However, licensing of digital instrumentation and control applications for operating reactors, has generally involved significant regulatory and industry efforts in specifying, developing, and reviewing the appropriate level of information needed to obtain regulatory approval. This is in part related to the clarity of the existing guidance, and in part as a result of seeking regulatory review, and approval of "first-of-a-kind" technology for which there is little or no direct precedent. The Licensing Process Technical Working Group (TWG #6) will address the safe, secure, and efficient licensing of digital technology for both new and operating reactors and fuel cycle facilities. The outcomes from each of the technical working groups will consider, as longer term goals, the adequacy and applicability of the guidance as it relates to licensing process.

The Licensing Process TWG #6 has the following objectives:

1. Identify the regulatory requirements, acceptance criteria, and guidelines that are to be addressed in Chapter 7 of the COL applicant's safety analyses report (SAR), which contains information about the plant's I&C systems, or 10CFR70, Subpart H.
2. Develop proposed resolutions to licensing process issues that emerge during the development and implementation of digital I&C technology for new plants.

To accomplish its objectives, TWG #6 will access up-to-date versions of relevant guidance documents and to information released by the other TWGs.

2. SCOPE:

TWG #6 will monitor the following licensing topics and add others as needed:

- a. The requirements and guidance for submitting, processing, and documenting digital I&C licensing actions, with emphasis on Regulatory Guide 1.206 and SRP Chapter 7.
- b. The stability and repeatability of the digital I&C licensing process.

- c. The interests of the agency, the industry, and public stakeholders.
- d. The resolution of licensing process disagreements about, for example:
 - i. policy and procedural issues
 - ii. the clarity of guidance and acceptance criteria for licensing submittal format and content
 - iii. the level of detail in licensing submittals
 - iv. the sequence of steps in the licensing process
 - v. scheduling conflicts
 - vi. thresholds for regulatory review

3. PROBLEM STATEMENT:

The NRC and the nuclear power industry share common goals for the safe, secure and efficient licensing of digital technology for both new reactors and operating reactors and fuel facilities. Key attributes that need to be addressed to facilitate digital technology licensing include:

- Problem 1 Level of Detail: Adequate guidance on the level of detail in COL applications for new reactors and licensing actions for operating reactors and fuel cycle facilities necessary to begin and complete the regulatory reviews.
- Problem 2 Applicability: Clear applicability of guidance for operating reactors and fuel cycle facilities compared to new reactors, including the applicability of operating reactor change processes to new plant COLs and the applicability of Chapter 7 and Chapter 18 of the Standard Review Plan (NUREG-0800) to digital instrumentation and control upgrades for operating reactors and fuel facilities.
- Problem 3 Clear Process Protocols: Clear licensing process protocols for developing the application and NRC review of digital technology licensing actions.

4. DELIVERABLES:

- 1. Issue Interim Staff Guidance addressing future Nuclear Energy Institute (NEI) Guideline (such as NEI 06-02 "License Amendment Request Guidelines"), which will provide specific guidance on the level of detail for digital instrumentation and control applications and applicability of NRC guidance for operating reactors, new reactors, and fuel cycle facilities;
- 2. Develop recommendations for conforming changes for licensing process to Chapter 7 and Chapter 18 of NUREG-0800 and Regulatory Guide 1.206, as necessary, to support outcomes of the other task working groups.

3. NRC Regulatory Issue Summary (RIS) 2002-22, dated November 25, 2002, endorsed the EPRI/NEI joint task force report, EPRI TR-102348, Rev. 1, NEI 01-01. The subject of that report was licensing digital upgrades. The issues discussed in that NRC endorsed report will be reviewed to assure the effectiveness of licensing process protocols. Discrepancies identified will be addressed by proposing changes to guidance documents.

5. MILESTONES, ASSIGNMENTS, AND DELIVERABLES:

TWG #6: Licensing Process					
Milestones, Assignments and Deliverables	Deliverable	Due Date	Fcst/Actual	Lead	Support
NEAR-TERM					
Problem 1: Level of Detail					
Problem 2: Applicability of Guidance					
Problem 3: Process Improvement					
No near-term deliverables					
LONG-TERM					
Problem 1: Level of Detail					
Industry to provide white paper	✓	TBD	F	NEI	n/a
Review and comment on industry white paper	✓	TBD	F	NRC	n/a
Problem 2: Applicability of Guidance					
Industry to provide white paper	✓	TBD	F	NEI	n/a
Review and comment on industry white paper	✓	TBD	F	NRC	n/a
Problem 3: Process Improvement					
Industry to provide white paper	✓	TBD	F	NEI	n/a
Review and comment on industry white paper	✓	TBD	F	NRC	n/a
Common Long-Term Actions for All Problem Statements					
Review guidance revisions from other TWGs		TBD	F	NRC	NRC
Work with other organizations to incorporate guidance into consensus standards, as appropriate		TBD	F	NRC	NEI

TWG #6: Licensing Process					
Milestones, Assignments and Deliverables	Deliverable	Due Date	Fcst/Actual	Lead	Support
Recommend revisions to SRP and other regulatory documents, e.g., NUREG or Regulatory Guides, as appropriate.	✓	TBD	F	NRC	n/a
ACRS interaction (as needed)		TBD	F	NRC	n/a
CRGR interaction (as needed)		TBD	F	NRC	n/a
Issue revised RG	✓	TBD	F	NRC*	n/a
Issue revised SRP	✓	TBD	F	NRC*	n/a

* Issuance of revisions to RGs and SRP will be conducted through established agency process.

**CYBER SECURITY ASSOCIATED WITH
DIGITAL INSTRUMENTATION AND CONTROLS
Interim Staff Guidance-XX**

**Interim Resolution of Concerns Regarding Programmatic Implementation of Cyber
Security Requirements at Nuclear Power Plants**

Issue:

The nuclear power industry requested clarification of conflicting guidance associated with implementation of cyber security measures at nuclear power plants. Specifically, the industry asserted that certain guidance provided in Regulatory Guide 1.152 Revision 2, *Criteria for Use of Computers in Safety Systems of Nuclear Power Plants*, conflicts with the industry-developed, NRC-accepted NEI 04-04 *Cyber Security Program for Power Reactors, Rev. 1*, document with regard to the protection of safety-related digital instrumentation and control systems. Additionally, the industry requested clarification of the NRC staff's position on the "acceptance" of NEI 04-04 as a means for establishing and maintaining an effective cyber security program at nuclear power plants.

This issue is addressed in the Interim Staff Guidance (ISG) provided below.

Purpose:

The purpose of this ISG is to clarify the NRC staff's expectations with regard to the implementation of cyber security requirements for nuclear power plant safety systems, and to clarify what is meant by the staff's acceptance of NEI 04-04 as an effective method for maintaining a cyber security program.

Background:

In response to the September 11, 2001, terrorist attacks and subsequent information provided by intelligence and law enforcement agencies, the NRC completed the following actions to enhance the protection of nuclear facilities from both physical and cyber threats:

- NRC Order EA-02-026, *Interim Safeguards and Security Compensatory Measures for Nuclear Power Plants*, February 2002

This order specified numerous interim compensatory measures to address the elevated threat environment. Part of this order contained cyber security requirements mandating nuclear power plant licensees to identify digital systems critical to the operation of the facility, and to evaluate the potential consequences to the facility should these systems be compromised. The material aspects of EA-02-026 are withheld from public disclosure in accordance with 10 CFR 73.21, "Requirements for the Protection of Safeguards Information."

- NRC Order EA-03-086, *Design Basis Threat for Radiological Sabotage*, April 2003

This order supplemented the Design Basis Threat (DBT) for nuclear power plants specified

in 10 CFR 73.1. Among other things, this order established requirements for the development of a cyber security program at each nuclear power plant. The material aspects of EA-03-086 are withheld from public disclosure in accordance with 10 CFR 73.21, "Requirements for the Protection of Safeguards Information."

- NUREG/CR-6847, *Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants*, October 2004

In conjunction with Pacific Northwest National Laboratory personnel, the NRC staff developed a cyber security self-assessment methodology that could be used by licensees to assess the risk to systems deemed critical to the operation of nuclear power plants. The method was developed utilizing a multidisciplinary team that included nuclear power industry personnel. The material aspects of NUREG/CR-6847 are withheld from public disclosure in accordance with 10 CFR 2.390, "*Public Inspections, Exemptions, Requests for Withholding.*"

- NEI 04-04 Rev. 1, *Cyber Security Program for Power Reactors*, November 2005

In a letter dated December 23, 2005, after providing considerable in-depth review and comment, the NRC staff notified the Nuclear Energy Institute (NEI) that the industry-generated document, NEI 04-04, would be an acceptable method for establishing and maintaining a cyber security program at nuclear power plants. The material aspects of NEI 04-04 are withheld from public disclosure in accordance with 10 CFR 2.390, "*Public Inspections, Exemptions, Requests for Withholding.*"

- Regulatory Guide 1.152 Rev. 2, *Criteria for Use of Computers in Safety Systems of Nuclear Power Plants*, January 2006

This document provides specific cyber security guidance for nuclear power plant licensees in the development and implementation of protection measures for digital instrumentation and controls used in safety system applications. This guidance addressed aspects of the implementation of cyber security within safety systems that were not adequately covered in IEEE Standard 7-4.3.2-2003, *Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations*.

- 71 Federal Register 62664, *Power Reactor Security Requirements - Proposed Rule*, October 26, 2006

The NRC proposed new cyber security requirements for nuclear power plants in a proposed 10 CFR 73.55 (m). The proposed rule maintains the intent of the previously-issued security orders (i.e., EA-02-026 and EA-03-086) and would require licensees to implement an effective program to detect and prevent cyber attacks on plant computer systems associated with safety, security, and/or emergency response.

- Branch Technical Position 7-14 Rev. 5, *Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems*, March 2007

This document provides NRC staff review guidelines for evaluating software life-cycle processes associated with safety-related digital instrumentation and control systems at nuclear power plants. It also addresses characteristics that should be present within an acceptable software management plan (e.g., licensees should provide a description of the

methods employed to prevent corruption of the software by viruses, Trojan horses or other malicious intrusions).

- 72 Federal Register 12705, *Design Basis Threat – Final Rule*, March 19, 2007

This final rule requires licensees to protect against "cyber attacks."

- NEI 04-04 Rev. 2, *Cyber Security Program for Power Reactors*, August 2007

Following numerous discussions with NRC staff, industry personnel revised NEI 04-04 primarily to provide clarification with respect to the requirements for securing safety-related digital instrumentation and control systems. The material aspects of NEI 04-04 are withheld from public disclosure in accordance with 10 CFR 2.390, "*Public Inspections, Exemptions, Requests for Withholding.*"

Discussion:

Subsequent to the issuance of NEI 04-04 Rev. 1, as nuclear power plant licensees worked to identify and implement security enhancements to further secure their facilities from internal and external cyber threats, the industry identified what they perceived to be inconsistencies between certain guidance provided in Regulatory Guide 1.152 and programmatic aspects of NEI 04-04. The details of these perceived inconsistencies are not described here since NEI 04-04 is designated as 10 CFR 2.390 information that is exempt from public release under the Freedom of Information Act (5 U.S.C. 522).

In October 2006, the NRC staff, NEI and industry representatives met to discuss methods to resolve the perceived inconsistencies between the various guidance documents listed above. Subsequently, an NRC Task Working Group (TWG) was established to address these issues, and to ensure that the cyber security guidance provided was coherent and consistent for both existing licensees and future combined operating license applicants.

To resolve the perceived inconsistencies between Regulatory Guide 1.152 and NEI 04-04, the TWG conducted a "gap" analysis to identify areas where the two documents overlapped or were inconsistent. The gap analysis concentrated on Regulatory Positions 2.1-2.9 of Regulatory Guide 1.152 and the programmatic elements of NEI 04-04. The TWG also reviewed all previously-issued cyber security guidance to identify any other possible areas of inconsistency.

The TWG met with industry representatives on May 8, 2007, to review the gap analysis. The ensuing discussion and review of the gap analysis revealed that no major inconsistencies existed between the two documents. Rather, the TWG found that Regulatory Guide 1.152 was complementary to NEI 04-04 on the subject of cyber security related to safety systems. The perceived inconsistencies originally identified by industry were due largely to misinterpretation of certain technical content within NEI 04-04. Clarification provided by one of the primary authors of NEI 04-04 eliminated the misunderstanding.

Although no major inconsistencies were revealed, the TWG determined that there was overlapping guidance in a few programmatic areas. The industry suggested consolidating the overlapping guidance to alleviate confusion going forward. Accordingly, NEI offered to revise NEI 04-04 to minimize the possibility of misinterpretation and to provide clarification with respect

to the requirements for securing safety-related digital instrumentation and control systems. Following the revision, the document would be resubmitted to the NRC staff for review.

NEI also suggested that, following the review of the revised NEI 04-04, the NRC staff should provide written direction that would allow the use of either Regulatory Guide 1.152 or NEI 04-04 when seeking to secure safety-related systems. Though the staff agreed that the proposed modifications to NEI 04-04 would help to minimize confusion going forward, it was nonetheless viewed as a sub-optimal solution for the long-term. The staff noted that because of the likelihood of changes in this area due to emerging threats and advances in technology, regulatory guidance to address these changes would also need to be modified, necessitating changes to NEI 04-04. As such, the NRC staff did not consider NEI 04-04 to be an appropriate long-term repository for such guidance, but rather that a new Regulatory Guide be developed to address cyber security defense measures required by 10 CFR 73.1 and the proposed new 10 CFR 73.55(m). In the meantime, the TWG acknowledged that NEI would submit a revision to NEI 04-04 consistent with the foregoing discussion as a short-term solution.

NEI submitted NEI 04-04 Rev. 2 to the TWG on August 6, 2007. The TWG reviewed the changes to NEI 04-04 and found them acceptable. The NRC staff's interim position on the application of NEI 04-04 Rev. 2 and RG 1.152 are provided below.

Staff Position:

Until such time when the NRC provides additional guidance on this subject, licensees, permit holders, and applicants involved in the design, construction, implementation, or upgrade of safety-related digital instrumentation and control systems in nuclear power plants, who rigidly adhere to the programmatic guidance and recommendations set forth in NEI 04-04 Rev 2, *Cyber Security Program for Power Reactors*, August 4, 2007 may address Regulatory Positions 2.1-2.9 of Regulatory Guide 1.152 Rev 2, *Criteria for Use of Computers in Safety Systems of Nuclear Power Plants*, January 2006, through implementation of their respective NEI 04-04 program.

Licensees, permit holders and applicants are still required to identify, consider, and address all other applicable regulations, standards, and guidance when designing, constructing, implementing and upgrading digital safety systems. This NRC staff position is strictly bounded to the applicability of Regulatory Positions 2.1-2.9 found in Regulatory Guide 1.152 Rev. 2. No extrapolation or extension of this concept is inferred, approved or authorized for any other portion of Regulatory Guide 1.152 Rev. 2.

Further, the NRC staff notes that NEI 04-04 Rev. 2 establishes a framework for the development, implementation and maintenance of an effective cyber security program, but does not necessarily contain or describe all of the implementing details necessary to demonstrate an ability to defend against a determined cyber attack with high assurance. The NRC plans to provide additional regulatory guidance in support of the ongoing 10 CFR 73.55(m) rulemaking to clarify the regulatory expectations related to this topic.

Viewing NEI 04-04 Rev. 2 as a programmatic framework document does not in any way diminish its importance to the industry or to the NRC. NEI 04-04 Rev. 2 represents the collective effort of a majority of industry representatives that sought to develop a means to define what elements would be essential to the construction of an effective cyber security

program. The NRC finds NEI 04-04 Rev. 2 to be a highly constructive and informative reference in the development of its cyber security regulations and guidance documents.

Rationale:

After providing in-depth review and comment, the NRC staff determined that NEI 04-04 Rev. 2, *Cyber Security Program for Power Reactors*, August 4, 2007, is an acceptable method for establishing and maintaining a cyber security program at nuclear power plants. Further, the NRC staff has determined that the changes made within this revision adequately incorporate and address Regulatory Positions 2.1-2.9 of Regulatory Guide 1.152 Rev. 2, *Criteria for Use of Computers in Safety Systems of Nuclear Power Plants*, January 2006.

Nonetheless, the NRC staff notes that NEI 04-04 Rev. 2 does not establish minimum standards of acceptable risk and lacks the specific measures needed to mitigate such risks. In addition, NEI 04-04 does not establish quantifiable metrics to enable a meaningful assessment of cyber security program effectiveness. Due to its performance-based (i.e., non-prescriptive) nature, NEI 04-04 does not provide the type of directive statements typically found within NRC regulatory guidance documents. As such, NEI 04-04 leaves licensees and applicants open to develop their own criteria and standards. The NRC staff is concerned that this lack of specificity will result in standards that are inconsistently determined and applied throughout the industry. As such, the staff plans to develop a Regulatory Guide, in support of the ongoing 10 CFR 73.55(m) rulemaking effort, to assist licensees, permit holders, and applicants in understanding *how* to meet the acceptable standards.

Recommendation:

Until further notice, this ISG should be used when developing and implementing cyber security programs or when engaging in the design, construction, implementation, or upgrade of digital safety systems in nuclear power plants.

Applicability:

This ISG is applicable to all existing nuclear power plant licensees, permit holders and applicants.

References:

NRC Order EA-02-026, *Interim Compensatory Measures*, dated February 25, 2002

NRC Order EA-03-086, *Design Basis Threat for Radiological Sabotage*, April 29, 2003

IEEE Standard 603-1998, *Standard Criteria for Safety Systems for Nuclear Power Generating Stations*, July 1, 1998

IEEE Standard 7-4.3.2, *Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations*, December 19, 2003

NRC Standard Review Plan NUREG-0800, Appendix 7.1-D, *Guidance for Evaluation of the Application of IEEE STD 7-4.3.2*

NRC Standard Review Plan NUREG-0800, Branch Technical Position 14, *Guidance on Software Reviews for Digital computer-Based Instrumentation and Control Systems*

NRC Regulatory Guide 1.152, Rev. 2, *Criteria for Use of Computers in Safety Systems of Nuclear Power Plants*, January 2006

Federal Register Vol. 71, No. 207, *Power Reactor Security Requirements*, October 26, 2006

NEI 04-04 Rev. 1, *Cyber Security Program for Power Reactors*, November 18, 2005

NEI 04-04 Rev. 2, *Cyber Security Program for Power Reactors*, August 4, 2007

NEI White Paper, *Cyber Security Guidance for Nuclear Power Plants - The Need for a Coherent Approach*, March 5, 2007

DRAFT

DRAFT INTERIM GUIDANCE FOR EVALUATION OF DIVERSITY AND DEFENSE-IN-DEPTH IN DIGITAL COMPUTER-BASED INSTRUMENTATION AND CONTROL SYSTEMS

This draft interim guidance provides one acceptable method of complying with the requirements for diversity and defense-in-depth in digital instrumentation and control systems. This guidance is consistent with current Commission policy on digital I&C systems and it is not intended to be a substitute for NRC's regulations. The purpose of the draft interim guidance is to clarify the criteria the staff would use in evaluating whether an applicant/licensee meets the requirements for diversity and defense-in-depth when making licensing decisions in the interim until final guidance is developed and promulgated. The staff intends to continue working with stakeholders in refining the guidance and in developing final guidance.

There should be no distinction between the requirements for diversity and defense-in-depth (D3) in new (future) reactors and current operating plants.

While common cause failures in digital systems are considered to be beyond design basis, digital reactor protection systems should be protected against common cause failures.

In order to demonstrate that vulnerabilities to a common cause failure (CCF) have been adequately addressed, a D3 analysis should be performed. NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," dated December 1994, and BTP-19 are an acceptable means for a D3 analysis. If the D3 analysis determines the system or systems are subject to a CCF, an analysis of the plant responses to all Chapter 15 events calculated using best-estimate methods with realistic assumptions should be performed to determine the time frame for necessary protective actions.

In those instances where the protective action is required in less than 30 minutes, an independent and diverse automated backup, achieving the same or equivalent function, should be required. This independent and diverse automated backup function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function(s) under the associated event conditions. These independent and diverse automated backup systems should be similar in quality to the systems required by the Anticipated Transient Without Scram (ATWS) rule (10 CFR 50.62), as described in the enclosure to Generic Letter 85-06, "Quality Assurance Guidance for ATWS Equipment That Is Not Safety-Related," dated April 16, 1985 (Accession No. 8504120206).

In those cases where plant response analysis shows that the protective action is not required for at least 30 minutes, the protective action may be performed by manual operator actions. The licensee will be required to demonstrate that sufficient information and controls (safety or non-safety), independent and diverse from the RPS discussed above, are provided in the main control room, and that the information displays and controls are not subject to the same CCF.

In addition to the above, a set of displays and controls (safety or non-safety) should be provided in the main control room for manual actuation and control of safety equipment to manage plant critical safety functions, including reactivity control, reactor core cooling and heat removal from the primary system, reactor coolant system integrity, radioactivity control, and containment conditions. The displays and controls should be independent and diverse from the RPS discussed above. However, these displays and controls could be those used for manual operator action as described above. Where they serve as required backup capabilities, the

DRAFT INTERIM GUIDANCE FOR EVALUATION OF DIVERSITY AND DEFENSE-IN-DEPTH IN DIGITAL COMPUTER-BASED INSTRUMENTATION AND CONTROL SYSTEMS

displays and controls should be hard-wired downstream of the lowest-level software-based components.

Example 1: The RPS is designed so that for each safety function, two channels use one type of digital system, and the other two channels use a diverse digital system. The D3 analysis, e.g., performed in accordance with NUREG/CR-6303 and BTP-19, determines the two diverse digital systems are not subject to a CCF. In this case, no additional diversity would be required.

Example 2: The safety functions are performed on a common computer system replicated in the redundant channels. The D3 analysis shows that certain safety functions could be subject to a CCF; therefore, a documented basis for a diverse means of accomplishing the safety functions should be provided. The D3 analysis of the plant responses to all Chapter 15 events determines that the RPS protective action is required in less than 30 minutes. In this instance, an independent and diverse automated backup system is required to perform the safety function to adequately respond to the postulated accident or anticipated operational occurrence. The non-safety independent and diverse automated backup system is required to be of enhanced quality, similar to systems required by the ATWS rule.

Example 3: As in example 2, the safety functions are determined to be subject to a CCF; however, the analysis of the plant responses to all Chapter 15 events determines that the RPS protective action is not required for at least 30 minutes. In this instance, the diverse method of responding to the postulated accident or anticipated operational occurrence may be accomplished by manual operator action.

Draft Interim Staff Guidance on Diversity and Defense-in-Depth (D3) Task Working Group Problems 3, 4, 5, and 6 in Digital Instrumentation and Control Systems

Draft Interim Staff Guidance on D3 TWG Problem 3

Problem 3:

BTP-19 Position 4 Challenges: Current Commission policy addresses system-level actuation in BTP-19, Position 4. Further clarification is required for whether credit can be taken for component-level versus system-level actuation of equipment. The NRC should clarify the rationale for applying BTP-19, Position 4 for digital system upgrades in existing plants.

Background

BTP-19, Position 4 states:

“A set of displays and controls located in the main control room should be provided for manual system-level actuation of critical safety functions and for monitoring of parameters that support safety functions. The displays and controls should be independent and diverse from the computer-based safety systems identified in Points 1 and 3.”

The intent of requiring system level actuation was to assure that the actuation, however achieved, was possible using simple controls from within the control room, without requiring plant operators to activate or control individual equipment at various locations within the plant. The exact method of actuating the protective function is not as important as that the actuation be

- a) simple,
- b) possible from the control room,
- c) required with sufficient time available for the operators to determine the need for protective actions even with malfunctioning indicators,
- d) appropriate for the event, and
- e) supported by sufficient instrumentation that indicates that
 - 1) the protective function is needed,
 - 2) the safety-related automated system did not perform the protective function, and
 - 3) the manual action was successful in performing the protective function.

Draft Interim Staff Guidance

In the current Draft ISG on Problems 1 and 2, the staff recommended that BTP-19, Position 4 be re-written to state:

“In addition to the above, a set of displays and controls (safety or non-safety) should be provided in the main control room for manual actuation and control of safety equipment to manage plant critical safety functions, including reactivity control, reactor core cooling and heat removal from the primary system, reactor coolant system integrity, radioactivity control, and containment conditions. The displays and controls should be independent and diverse from the RPS discussed above. However, these displays and controls could be those used for manual operator action as described above. Where they serve as backup capabilities, the displays and controls should also be able to function downstream of the lowest-level software-based components subject to the same common cause failure (CCF) that necessitated the diverse backup system; one example would be the use of hard-wired connections.”

This draft interim guidance does not specify whether the diverse displays and controls be used for component-level or system-level actuation of equipment, as long as the criteria are met.

Draft Interim Staff Guidance on D3 TWG Problem 4

Problem 4:

Effects of Common-Cause Failure: BTP-19 guidance recommends consideration of CCFs that "disable a safety function." Additional clarity is required regarding the effects that should be considered (e.g., fails to actuate and/or spurious actuation).

Background

IEEE Standard 603-1991, incorporated into 10 CFR by reference in 10 CFR 50.55a(h), states in paragraph 5.1, Single-Failure Criterion: "The safety systems shall perform all safety functions required for a design basis event in the presence of: (1) any single detectable failure within the safety systems concurrent with all identifiable but non-detectable failures; (2) all failures caused by the single failure; and (3) all failures and spurious system actions that cause or are caused by the design basis event requiring the safety functions."

There are two inherent safety functions that safety-related trip and actuation systems provide. The first safety function is to provide a trip or system actuation when plant conditions necessitate that trip or actuation. However, in order to avoid challenges to the safety systems and to the plant, the second function is to not trip or actuate when such a trip of actuation is not required by plant conditions. A simple metric would be:

	Plant conditions require a trip or actuation	Plant conditions do not require a trip or actuation
Trip or Actuation occurs	Proper System Operation	System Failure (Spurious Actuation)
Trip or Actuation does not occur	System Failure (Actuation does not occur or incomplete activation)	Proper System Operation

Therefore, to be in conformance with the single failure criteria, both a failure to trip and a spurious trip are unacceptable.

Software CCF was declared a beyond design basis event by the Commission in Staff Requirements Memorandum dated July 21, 1993, issued in response to SECY-93-087, dated April 2, 1993. The industry has requested additional clarification regarding the effects of software CCF that should be considered.

Draft Interim Staff Guidance

When considering the possible types of protection system failures that may occur as a result of failure to actuate, a simple failure of the total system may not be the worst case failure, particularly when analyzing the time required to identify and respond to the condition. A failure to trip may not be as limiting as a partial actuation of an emergency core cooling system, with digital indications of a successful actuation, which may take longer to evaluate and correct than a total failure to send any actuation signal. For this reason, the evaluation of failure modes as a result of software CCF should include the possibility of partial actuation and failure to actuate with false indications, as well as a total failure to actuate.

Industry also requested that the staff determine whether spurious actuations should be considered when performing single failure analyses associated with software CCF. The primary concern is that an undetected failure within the digital system could prevent proper system operation. A failure or fault that is detected can be repaired; however, failures that are nondetectable may prevent a trip or actuation when required. Consequently, nondetectable faults are of concern. Therefore, a diverse means to provide the required safety function, or some other safety function that will adequately address each chapter 15 event should be provided.

Common cause failures that cause an undesired trip or actuation are detectable because the failure is self-announcing. There may be circumstances in which a spurious trip or actuation would not occur until a particular signal trajectory within the software is reached. In these cases, the spurious trip or actuation would not occur immediately upon system startup, but could occur under particular plant conditions. This circumstance is still self-announcing, even if the annunciation did not occur on initial test or startup. Use of design techniques (e.g., a constant and unchanging signal trajectory within the software that is unaffected by plant conditions), therefore, is recommended.

In general, spurious trips and actuations are lesser safety concern than failures to trip or actuate. There may be plant and safety system challenges and stresses; however, these challenges are not as significant as failure to respond to a chapter 15 event.

For these reasons, beyond design basis software common cause failures, a spurious trip, or actuation of a safety-related digital protection system does not need to be considered in the single failure analysis.

Draft Interim Staff Guidance on D3 TWG Problem 5

Problem 5:

Common-Cause Failure Applicability: Clarification is required on identification of design attributes that are sufficient to eliminate consideration of CCFs (e.g., degree of simplicity).

Draft Interim Staff Guidance

There are two design attributes that are sufficient to eliminate consideration of CCF:

(1) Diversity - In Example 1 for Problems 1 and 2, sufficient diversity exists in the protection system such that CCFs within the channels can be considered to be fully addressed without further action.

Example 1: A four-channel RPS is designed so that, for each safety function, two channels use one type of digital system and the other two channels use a diverse digital system. A D3 analysis performed consistent with the guidance in NUREG/CR-6303 and BTP-19 determines that the two diverse digital systems are not subject to a CCF. In this case, no additional diversity would be required in the safety system.

(2) Testability - A system is sufficiently simple such that every possible combination of inputs, internal and external initial states, and every signal path can be tested; that is, the system is fully tested and found to produce only correct responses.

In assessing the system states, the guidance provided in IEEE Std 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," clause 5.4.1, "Computer system [equipment qualification] testing," should be addressed:

Computer system qualification testing (see 3.1.36) shall be performed with the computer functioning with software and diagnostics that are representative of those used in actual operation. All portions of the computer necessary to accomplish safety functions, or those portions whose operation or failure could impair safety functions, shall be exercised during testing. This includes, as appropriate, exercising and monitoring the memory, the CPU, inputs and outputs, display functions, diagnostics, associated components, communication paths, and interfaces. Testing shall demonstrate that the performance requirements related to safety functions have been met.

Clause 5.4.1 requires the system developer/user to perform equipment qualification of the system (i.e., hardware and software) in its operational states while the system is operating at the limits of its equipment qualification envelope. The software and diagnostics should be representative of the software used in actual operation to a degree that provides assurance that the system states produced by the actual system will be tested during the equipment qualification process.

Draft Interim Staff Guidance on D3 TWG Problem 6

Problem 6:

Echelons of Defense: As described in NUREG-0737 Supplement 1, "Clarification of TMI Action Plan Requirements," sufficient information shall be provided to the operators to monitor (and thereby control) the following plant safety functions and conditions:

1. Reactivity control
2. Reactor core cooling and heat removal from the primary system
3. Reactor coolant system integrity
4. Radioactivity control
5. Containment conditions

BTP-19 guidance references the echelons of defense described in NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," (Accession No. 9501180332) for maintaining the above safety functions within safe margins for currently operating nuclear power plants:

1. Control systems
2. Reactor Trip System (RTS)
3. Engineered Safety Features Actuation System (ESFAS)
4. Monitoring and indications

Additional clarification is desired regarding how the echelons of defense for maintaining the above safety functions should factor into D3 analyses. A particular concern is that the current BTP-19 guidance does not consider plant design characteristics and operating procedures that affect how D3 is actually used to maintain the safety functions.

Background:

SECY-91-292, "Digital Computer Systems for Advanced Light Water Reactors," described the above four echelons of defense. SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," and the associated Staff Requirements Memorandum addressed defense against CCFs in digital I&C systems, among other issues. SECY-91-292 and SECY-93-087 did not address the consolidation of these echelons of defense-in-depth into one digital system, and neither did the Commission address combining echelons of defense at the time it established policy on digital system CCFs.

The industry is considering the use of digital I&C systems that combine all RTS and ESFAS functions within a single digital system software program. Combining two echelons of defense into a single software program could introduce new common-cause digital system failure mechanisms that do not exist in systems that use separate software programs, including software CCFs. These CCFs can be satisfactorily addressed if the criteria of ISG Problems 1 and 2 are met.

Draft Interim Staff Guidance

The RTS and ESFAS functions may be combined into a single digital platform if the criteria of the ISG addressing Problems 1 and 2 are met.

DRAFT

DRAFT

DRAFT

NOTE: This document is formatted for double-sided printing.
Single-sided printing will produce blank pages.

DIGITAL INSTRUMENTATION AND CONTROLS

Task Working Group #4: Highly-Integrated Control Rooms – Communications Issues (HICRc)

Interim Staff Guidance

Revision F

SCOPE

This Interim Staff Guidance addresses the design and review of digital systems proposed for safety-related service in nuclear power plants. These guidelines address only selected digital aspects of such systems. Such systems are also subject to other requirements germane to safety-related systems, such as requirements for separation, independence, electrical isolation, seismic qualification, Quality Requirements, etc.

This guidance specifically addresses issues related to interactions among safety divisions and between safety-related equipment and equipment that is not safety-related. This guidance is not applicable to interactions among entities that are all in the same safety division or that do not involve anything that is safety-related. This guidance does address certain aspects of digital control systems that are not safety-related but which may affect the plant conformance to safety analyses (accident analyses, transient analyses, etc.).

This guidance is intended to provide clarification and enhanced guidance in recognition of the inherent differences between digital systems that might be used in the future and analog / hardwired systems that have been used in the past.

These guidelines do not modify or supersede existing regulatory requirements or guidance. These guidelines present means acceptable to the staff for meeting existing requirements. Alternative means of meeting existing requirements will be considered if requested and adequately documented and justified. A documented technical basis showing that the proposed alternative measures provide equivalent assurance of safe and correct operation would be required.

Some of the provisions of this guidance may be interrelated, so acceptance of an alternative in one area may require that compensatory measures be taken in another. Thus acceptance of alternative provisions may require the imposition of other measures that would not otherwise be necessary for conformance to this guidance as-written. Such details must be addressed on a case-by-case basis.

In general, any failure to comply with any element of this guidance (expressed typically as "... should ...") is to be considered to be a proposed alternative design as described above. In some cases the guidance itself addresses alternative measures, but in most cases it will be up to the applicant to identify, present, and justify them.

Systems accepted by the staff in the past that are not fully in accordance with this guidance were accepted on the basis of detailed case-by-case review: that prior acceptance is not rescinded or diminished by this guidance, nor does it serve as precedent for waiving the guidance provided herein.

The extensive existing guidance (Regulatory Guides, SRP, etc.) on these subjects should also be taken into consideration in evaluating proposed digital systems. The provisions expressed herein are intended to supplement and clarify, not replace, the provisions of the existing guidance. The provisions of the existing guidance remain applicable even though many of those provisions are not addressed or referenced herein.

The purpose of Interim Staff Guidance is to clarify the criteria the staff will use in confirming that a proposed design meets applicable requirements. Interim Staff Guidance will remain in effect until final guidance is developed and promulgated and the interim guidance has been explicitly rescinded. The staff intends to continue working with stakeholders in refining the interim guidance and in developing final guidance.

ORGANIZATION

TWG4 has determined that HICRc is comprised of four basic areas of interest:

1. interdivisional communications: communications among different safety divisions¹ or between a safety division and a non-safety entity
2. command prioritization: selection of a particular command to send to an actuator when multiple and conflicting commands exist
3. multidivisional control and display stations: use of operator workstations or displays that are associated with multiple safety divisions and/or with both safety and nonsafety functions
4. digital system network configuration: the network or other interconnection of digital systems that might affect plant safety or conformance to plant safety analysis assumptions (interconnections among safety divisions or between safety and nonsafety divisions should also satisfy the guidance provided for interdivisional communications)

Areas of Interest #1 through 3 are each addressed in a separate section below. Area of Interest #4 has implications concerning each of the first three and is incorporated into those sections as needed.

¹ A *safety channel* as used herein is a set of safety-related instruments and equipment, along with the associated software, that together generate a protective actuation or trip signal to initiate a single protective function. While an analog/hardwired system would have each functional circuit clearly assigned to only one channel, the processor and other components in a digital system may be assigned to multiple channels. A *safety division* is the collection of all safety channels that are powered by a single power division. Different channels perform different functions. Different divisions perform the same set of functions, and are redundant to one another. Licensing credit can be taken only for redundancy among, not within, divisions.

1 INTERDIVISIONAL COMMUNICATIONS

BACKGROUND

As used in this document, interdivisional communications includes communications involving entities in different electrical safety divisions and communications between a safety division and an entity that is not safety-related. It does not include communications limited to a single division. Interdivisional communications may be bidirectional or unidirectional.

Bidirectional communications among safety divisions and between safety and nonsafety equipment is acceptable provided certain restrictions are enforced to ensure that there will be no adverse impact on safety systems.

Systems which include communications among safety divisions and/or bidirectional communications between a safety division and a nonsafety entity should adhere to the requirements described in the remainder of this section. Adherence to each point should be demonstrated by the applicant and verified by the reviewer. This verification should include detailed review of the system configuration and software specifications, and may also require review of selected software code.

CRITERIA

1. A safety channel must not be dependent upon any information from outside its own safety division to accomplish its safety function. This is a fundamental consequence of the independence requirements of IEEE603. It is recognized that division voting logic must receive inputs from multiple safety divisions.
2. The safety function of each safety channel must be protected from adverse influence from outside the division of which that channel is a member. This protection must be implemented within the affected division (rather than in the sources outside the division), must not itself be affected by any condition or information from outside the affected division, and must be sustained despite any operation, malfunction, design error, communication error, or software error or corruption, including errors or corruption that affect multiple channels/divisions.
3. A safety channel should not receive any communication from outside its own safety division unless that communication supports or enhances the performance of the safety function. Receipt of information that does not support the safety function would involve the performance of functions that are not directly related to the safety function. Receipt of such information and performance of such functions should be justified. It should be demonstrated that the added system/software complexity does not significantly increase the likelihood of software specification or coding errors, including errors which would affect more than one division. The applicant must justify the definition of “significantly” used in the demonstration.

4. The communication process itself should be carried out by a communications processor² separate from the processor that executes the safety function, so that communications errors and malfunctions will not interfere with the execution of the safety function. The communication and function processors should operate asynchronously, sharing information only by means of dual-ported memory or other shared but separately allocated memory resource. The function processor, the communications processor, and the shared memory, along with all supporting circuits and software, are all considered to be safety-related, and must be designed, qualified, fabricated, etc. accordingly. Access to the shared memory should be controlled in such a manner that the function processor has priority access to the shared memory to complete the safety function in a deterministic manner. For example, if the communication processor is accessing the shared memory at a time when the function processor needs to access it, the function processor should gain access within the allotted timeframe so as not to impact the loop cycle time. If the shared memory cannot support unrestricted simultaneous access by both processors, then the access controls should be configured such that the function processor always has precedence. If the function processor does not have priority access to the shared memory, then the safety function circuits and program logic must ensure that the safety function will be performed within the established timeframe and without the data from the shared memory.
5. The cycle time for the safety function processor should be determined in consideration of the longest possible completion time for each access to the shared memory. This longest-possible completion time should include the response time of the memory itself and of the circuits associated with it, and should also include the longest possible delay in access to the memory by the function processor assuming worst-case conditions for the transfer of access from the communications processor to the function processor. Failure of the system to meet the limiting cycle time should be detected and alarmed.
6. The safety function processor should perform no communication handshaking and should not accept interrupts from outside its own safety division.
7. Only predefined data sets may be used by the receiving system. Unrecognized messages and data should be identified and dispositioned by the receiving system in accordance with the prespecified design requirements. Data from unrecognized messages must not be used within the safety logic executed by the safety function processor. Message format and protocol should be pre-determined. Every message should have the same message field structure and sequence, including message identification, status information, data bits, etc. in the same relative locations in every message. Every datum should be included in every transmit cycle, whether it has changed since the previous transmission or not, to ensure deterministic system behavior.
8. Data exchanged between redundant safety divisions or between safety and nonsafety divisions must be processed in a manner that does not adversely affect the safety function of the sending divisions, the receiving divisions, or any other independent divisions.
9. Incoming message data should be stored in fixed predetermined locations in the shared memory and in the memory associated with the function processor. These memory locations should not be used for any other purpose. The memory locations should be allocated such that input data and output data are segregated from each other in separate memory devices or in separate prespecified physical areas within a memory device.

² "Processor" may be a CPU or other processing technology such as simple discrete logic, logic within an FPGA, an ASIC, etc.

10. Safety division software should be protected from alteration while the safety division is in operation. On-line changes to safety system software should be prevented by hardwired interlocks or by physical disconnection of maintenance/monitoring equipment. A workstation (e.g. engineer/programmer station) may alter addressable constants, setpoints, parameters, and other settings associated with a safety function only by way of the dual-processor / shared-memory scheme described in this guidance, or when the associated channel is inoperable. Such a workstation must be physically restricted from making changes in more than one division at a time. The restriction should be by means of physical cable disconnect, or by means of keylock switch that either physically opens the data transmission circuit or interrupts the connection by means of hardwired logic. Provisions that rely on software are not acceptable.
11. Provisions for interdivisional communication should explicitly preclude the ability to send software instructions directly to a safety function processor when that processor is operable. The progress of a safety function processor through its instruction sequence should not be affected by any message from outside the divisions. For example, the received messages should not direct the processor to execute a subroutine or branch to a new instruction sequence.
12. Communication faults must not adversely affect the performance of required safety functions in any way. Although the single-failure criterion indicates that such failures should be presumed to originate in only one safety channel at a time, there is no such restriction on assumed faults for nonsafety channels. Examples of credible communications faults include, but are not limited to, the following:
 - Messages may be corrupted due to errors in communications processors, errors introduced in buffer interfaces, errors introduced in the transmission media, or from interference or electrical noise.
 - Messages may be repeated at an incorrect point in time.
 - Messages may be sent in the incorrect sequence.
 - Messages may be lost, which includes both failures to receive an uncorrupted message or to acknowledge receipt of a message.
 - Messages may be delayed beyond their permitted arrival time window, including errors in the transmission medium, congested transmission lines, interference, or by delay in sending buffered messages.
 - Messages may be inserted into the communication medium, from unexpected or unknown sources.
 - Messages may be sent to the wrong destination, which could treat the message as a valid message.
 - Messages may be longer than the receiving buffer, resulting in buffer overflow and memory corruption.
 - Messages may contain data that is outside the expected range.
 - Messages may appear valid, but data may be placed in incorrect locations within the message.
 - Messages may occur at a high rate that degrades or causes the system to fail (i.e., broadcast storm).
 - message IP headers or addresses may be corrupted.

13. Vital communications, such as the sharing of channel trip decisions for the purpose of voting, should include provisions for ensuring that received messages are correct and are correctly understood. Such communications should employ error-detecting or error-correcting coding along with means for dealing with corrupt, invalid, untimely or otherwise questionable data. The effectiveness of error detection/correction should be demonstrated in the design and proof testing of the associated codes, but once demonstrated is not subject to periodic testing. Error-correcting methods, if used, should be shown to always reconstruct the original message exactly or to designate the message as unrecoverable. None of this activity is to affect the operation of the safety-function processor.
14. Vital communications should be point-to-point by means of a dedicated medium (copper or optical cable). In this context, "point-to-point" means that the message is passed directly from the sending node to the receiving node without the involvement of equipment outside the division of the sending or receiving node. Implementation of other communication strategies should provide the same reliability and must be justified.
15. Network communication for safety functions should communicate a fixed set of data (called the "state") at regular intervals, whether data in the set has changed or not.
16. Safety, liveness, and real-time properties required by the safety application should be verified in the protocol. Liveness, in particular, is taken to mean that no connection to another network can cause an RPS/ESFAS communication protocol to stall, either deadlock or livelock. (Note: This is also required by the independence criteria of GDC 24 and IEEE 603-1991 IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations.) (Source: NUREG/CR-6082, 3.4.3)
17. The medium used in a vital communications channel must be qualified for the anticipated normal and post-accident environments. For example, some optical fibers and components may be subject to gradual degradation as a result of prolonged exposure to radiation or to heat. In addition, new digital systems may require susceptibility testing for EMI/RFI and power surges, if the environments are significant to the equipment being qualified.
18. Provisions for communications should be analyzed for hazards and performance deficits posed by unneeded functionality and complication.
19. If data rates exceed the capacity of a communications link or the ability of nodes to handle traffic, the system will suffer congestion. All links and nodes should have sufficient capacity to support all functions. The applicant should identify the true data rate, including overhead, to ensure that communication bandwidth is sufficient to ensure proper performance of all safety functions. Communications throughput thresholds and safety system sensitivity to communications throughput issues should be confirmed by testing.
20. The safety system response time calculations should assume a data error rate that is greater than or equal to the design basis error rate and is supported by the error rate observed in design and qualification testing.

2 **COMMAND PRIORITIZATION**

BACKGROUND

This section presents guidance applicable to a prioritization device or software function block, hereinafter referred to simply as a “priority module.”

A priority module receives device actuation commands from multiple safety and non-safety sources, and sends the command having highest priority on to the actuated device. The actuated device is a safety-related component such as a motor actuated valve, a pump motor, a solenoid operated valve etc. The priority module must also be safety-related.

Existing Diversity and Defense-in-Depth guidance indicates that diverse actuation signals should be applied to plant equipment control circuits downstream of the digital system to which they are diverse, in order to ensure that the diverse actuation will be unaffected by digital system failures and malfunctions. This requires that the priority modules which combine the diverse actuation signals with the actuation signals generated by the digital system cannot be executed in the digital system software that may be subject to common-cause failures (CCF).

Software implementation of priority modules not associated with diverse actuation would result in the availability of two kinds of priority modules, one type suitable for diverse actuation and one type not suitable for diverse actuation. An applicant should demonstrate that there are adequate configuration control measures in place to ensure that software-based priority modules that might be subject to CCF will not be used later for credited diversity, either deliberately or accidentally (for example, there is protection from design error and from maintenance / implementation error). This applies both to existing diversity provisions and to diversity provisions that might be credited later. The applicant should show how such provisions fit into the overall Appendix B quality program.

CRITERIA

1. A priority module is a safety related device or software function, and it must meet all requirements (design, qualification, quality, etc.) applicable to safety-related devices or software.
2. Priority modules used for diverse actuation signals must be independent of the remainder of the digital system, and must function properly regardless of the state or condition of the digital system.
3. Safety-related commands that direct a component to a safe state (as opposed to commands originating in a safety-related channel but which only cancel or enable cancellation of the safe-state command and have no intrinsic safety function), and that originate in protection system sense and command features, must always have the highest priority and must override all other commands. It should be shown that the unavailability or spurious operation of the actuated device is included in the plant safety analysis.
4. A priority module may control one or more components. If a priority module controls more than one component, then all of these provisions apply to each of the actuated components.

5. Communication isolation for each priority module should be as described in the guidance for interdivisional communications.
6. Software used in the design, testing, maintenance, etc. of a priority module is subject to all of the applicable guidance in Regulatory Guide 1.152, which partially endorses IEEE Standard 7-4.3.2. This includes software applicable to any programmable device used in support of the safety function of a prioritization module, such as processors, programmable logic devices (PLDs), Programmable Gate Arrays, Programmable Logic Controllers (PLCs) or other such devices. Section 5.3.2 is particularly applicable to this subject. If the device is 100% tested (that is, every possible combination of inputs and every possible sequence of device states is tested, and all outputs are verified for every case), then validation of the design tools is not required.
7. Any software program which is used in support of the safety function within a priority module must be treated as safety-related software. All requirements that apply to safety-related software also apply to prioritization module software. Burned-in memory should be changeable only through removal and replacement of the memory device. Design provisions should ensure that static memory and programmable logic cannot be altered while installed in the module. The contents and configuration of field programmable memory should be considered to be software, and should be developed, maintained, and controlled accordingly.
8. To minimize the probability of failures due to common software, the priority module design should be fully tested (This refers to proof-of-design testing, not to individual testing of each module and not to surveillance testing.). If the tests are generated by any automatic test generation program then all the test sequences and test results should be manually verified. Testing should include the application of every possible combination of inputs and the evaluation of all of the outputs that result from each combination of inputs. If a module includes state-based logic (that is, if the response to a particular set of inputs depends upon past conditions), then all possible sequences of input sets should also be tested. If testing of all possible sequences of input sets is not considered practical by an applicant, then the applicant should identify the testing that is excluded and justify that exclusion. The applicant should show that the testing planned or performed provides adequate assurance of proper operation under all conditions and sequences of conditions. Note that it is possible that logic devices within the priority module include unused inputs: assuming those inputs are forced by the module circuitry to a particular known state, those inputs can be excluded from the “all possible combinations” criterion. For example, a priority module may include logic executed in a gate array that has more inputs than are necessary. The unused inputs should be forced to either “TRUE” or “FALSE” and then can be ignored in the “all possible combinations” testing.
9. Automatic testing (including failure of automatic testing features) must not inhibit the safety function of the module in any way. Failure of automatic testing software would constitute common-cause failure if were to result in the disabling of the module safety function.
10. The priority module must ensure that the completion of a protective action as required by IEEE Standard 603 is not interrupted by commands, conditions, or failures outside the module’s own safety division.

3 MULTIDIVISIONAL CONTROL AND DISPLAY STATIONS

BACKGROUND

This section presents guidance concerning operator workstations used for the control of plant equipment in more than one safety division and for display of information from sources in more than one safety division. This guidance also applies to workstations that are used to program, modify, monitor, or maintain safety systems that are not in the same safety division as the workstation.

Multidivisional control and display stations addressed in this guidance may themselves be safety-related or not safety-related, and they may include controls and displays for equipment in multiple safety divisions and for equipment that is not safety-related, provided they meet the conditions identified herein.

Even though the use of multidivisional control and display stations is relatively new to the nuclear industry, the concepts to maintain the plant safety contained in this guidance is in line with the current NRC regulations.

CRITERIA

3.1 Independence and Isolation

The following provisions are applicable to multidivisional control and display stations. These provisions do not apply to conventional hardwired control and indicating devices (hand switches, indicating lamps, analog indicators, etc.).

1. **Nonsafety stations receiving information from one or more safety divisions:**
All communications with safety-related equipment should be as described in the guidelines for interdivisional communications.
2. **Safety-related stations receiving information from other divisions (safety or nonsafety):**
All communications with equipment outside the station's own safety division, whether that equipment is safety-related or not, should be as described in the guidelines for interdivisional communications. Note that the guidelines for interdivisional communications cite requirements relating to the nature and limitations concerning such communications, as well as guidelines relating to the communications process itself.
3. **Nonsafety stations monitoring and / or controlling the operation of safety-related equipment:**
Nonsafety stations may monitor and / or control the operation of safety-related equipment, provided the following restrictions are enforced:
 - The nonsafety station should access safety-related plant equipment only by way of a priority module associated with that equipment. Priority modules should be in accordance with the guidance on priority modules.

- A nonsafety station must not affect the operation of safety-related equipment when the safety-related equipment is performing its safety function. This provision must be implemented within the safety-related system, and must be unaffected by any operation, malfunction, design error, software error, or communication error in the nonsafety equipment. In addition:
 - The nonsafety station must be able to bypass a safety function only when the affected division has itself determined that such action would be acceptable.
 - The nonsafety station must not be able to suppress any safety function. (If the safety system itself determines that termination of a safety command is warranted as a result of the safety function having been achieved, and if the applicant demonstrates that the safety system has all information and logic needed to make such a determination, then the safety command may be reset from a source outside the safety division. If operator judgment is required to establish the acceptability of resetting the safety command, then reset from outside the safety division is not acceptable because there would be no protection from inappropriate or accidental reset.)
 - The nonsafety station should be able to bring a safety function out of bypass condition only when the affected division has itself determined that such action would be acceptable.

4. Safety-related stations monitoring and / or controlling the operation of equipment in other safety-related divisions:

Safety-related stations monitoring and / or controlling the operation of equipment in other divisions are subject to constraints similar to those described above for nonsafety stations that monitor and / or control the operation of safety-related equipment.

- A control station should access safety-related plant equipment outside its own division only by way of a priority module associated with that equipment. Priority modules should be in accordance with the guidance on priority modules.
- A station must not influence the operation of safety-related equipment outside its own division when that equipment is performing its safety function. This provision must be implemented within the affected (target) safety-related system, and must be unaffected by any operation, malfunction, design error, software error, or communication error outside the division of which those controls are a member. In addition:
 - The extra-divisional (that is, “outside the division”) control station must be able to bypass a safety function only when the affected division itself determined that such action would be acceptable.
 - The extra-divisional station must not be able to suppress any safety function. (If the safety system itself determines that termination of a safety command is warranted as a result of the safety function having been achieved, and if the applicant demonstrates that the safety system has all information and logic needed to make such a determination, then the safety command may be reset from a source outside the safety division. If operator judgment is required to establish the acceptability of resetting the safety command, then reset from outside the safety division is not acceptable because there would be no protection from inappropriate or accidental reset.)
 - The extra-divisional station should be able to bring a safety function out of bypass condition only when the affected division has itself determined that such action would be acceptable.

5. Malfunctions and Spurious Actuations:

The result of malfunctions of control system resources (e.g., workstations, application servers, protection/control processors) shared between systems must be consistent with the assumptions made in the safety analysis of the plant. Design and review criteria for complying with this requirement include but are not limited to the following:

- Control processors that are assumed to malfunction independently in the safety analysis should not be affected by common software.
- No single control action (for example, mouse click or screen touch) should generate commands to plant equipment. Two positive operator actions should be required to generate a command, for example, “do you want to proceed?” followed by a “Yes” or “No” choice, for all safety functions and other important functions. (The second operation as described here is to provide protection from spurious actuations, not protection from operator error. Protection from operator error may involve similar but more restrictive provisions, as addressed in guidance related to Human Factors.)
- Each control processor or its associated communication processor should detect and block commands from the shared resources that do not pass the communication error checks.
- Multidivisional control and display stations should be qualified to withstand the effects of adverse environments, seismic conditions, EMI/RFI, power surges, and all other design basis conditions applicable to safety-related equipment at the same plant location. This qualification need not demonstrate complete functionality during or after the application of the design basis condition unless the station is safety-related. Stations which are not safety-related should be shown to produce no spurious actuations and to have no adverse effect upon any safety-related equipment or device as a result of a design basis condition, both during the condition and afterwards. For example, a nonsafety station should not cause the spurious operation or stoppage of any safety-related or nonsafety device during the condition, and should not fail in such a manner as to do so after the condition spontaneously or as a result of a misinterpreted operator action. If spurious or abnormal actuations or stoppages are possible as a result of a design basis condition, then the plant safety analyses must envelope those spurious and abnormal actuations and stoppages. Qualification should be supported by testing rather than by analysis alone. D3 considerations may impose additional qualification considerations in addition to those described herein.
- Loss of power, power surges, power interruption, and any other credible event to any operator workstation or controller should not result in spurious actuation or stoppage of any plant device or system unless that spurious actuation or stoppage is enveloped in the plant safety analyses.
- The design should have provision for an “operator workstation disable” switch to be activated upon abandonment of the main control room, to preclude spurious actuations that might otherwise occur as a result of the condition causing the abandonment (such as control room fire or flooding). The means of disabling control room operator stations should be immune to short-circuits, environmental conditions in the control room, etc. that might restore functionality to the control room operator stations and result in spurious actuations.
- Processors should be configured and functionally distributed so that processor malfunction or software error will not result in spurious actuations that are not enveloped in the plant design bases, accident analyses, ATWS provisions, or other provisions for abnormal conditions. This includes spurious actuation of more than one plant device or system as a result of processor malfunction or software error.

- Failure or malfunction of any operator workstation must not result in a plant condition (including simultaneous conditions) that is not enveloped in the plant design bases, accident analyses, and anticipated transients without scram (ATWS) provisions, or in other unanticipated abnormal plant conditions

3.2 Human Factors Considerations

Safety-related plant equipment should have safety-related controls and displays:

- as required by IEEE 603
- as recommended or required in connection with the TMI accident
- as referenced in:
 - plant safety or transient analyses
 - emergency or normal operation procedures
 - D3 or ATWS analyses
 - other analyses
- as suggested in the plant control and display “minimum inventory” interim staff guidelines
- as indicated in other requirements or analyses.

For any safety-related equipment not having safety-related controls and displays, an applicant should demonstrate that safety-related controls and displays are not needed in consideration of the above criteria or of any other considerations or requirements.

Safety-related controls and displays may be provided via operator workstations, or they may be provided via hardwired devices such as switches, relays, indicators, and analog signal processing circuits. In either case, the safety-related controls and indications must consist of safety-related devices with safety-related software and must be dedicated to specific safety divisions.

The need for a plant operator to use alternative controls and displays under upset or accident conditions could pose Human Factors concerns, since the need to use less-familiar provisions would coincide with the need for maximum effectiveness and timeliness in operator actions. Such an approach could also result in confusion if the nonsafety displays, as a result of lack of qualification and of lesser quality standards, present obsolete or erroneous information to the plant operator but fail to advise the operator of these potential inaccuracies.

An applicant would need to demonstrate that Human Factors considerations, including the foregoing considerations and also including operator response time and situation awareness, have been included in the system design, operating procedures, and accident analyses and shown to be both reasonable and adequate. This aspect of the application should be reviewed and found acceptable by appropriate Human Factors, Operations, and plant system experts within the NRC.

There are many other Human Factors considerations applicable to the design of operator workstations, whether multidivisional or not. Such considerations are not addressed here.

Guidance concerning general Human Factors considerations is provided separately.

DRAFT

3.3 Diversity and Defense-in-Depth (D3) Considerations

D3 considerations may influence the number and disposition of operator workstations and possibly of backup controls and indications that may or may not be safety-related. The guidance provided herein is not dependent upon such details.

D3 considerations may also impose qualification or other requirements or guidelines upon equipment addressed in this ISG. The guidance presented herein does not include such considerations.

Consideration of other aspects of D3 is outside the scope of this guidance.

Guidance concerning D3 considerations is provided separately.

APPENDIX:

HICRc PRIORITY LIST CROSS-REFERENCE

The priority list developed in the public meeting of March 29, 2007 is cross-referenced to the four basic considerations described herein.

Priority List Item	Area of Interest
1. Communication between safety divisions. - Functional Independence - Message Integrity	1 data communications
2. Control of both safety and non-safety components from a non-safety workstation (VDU) - via Non-safety function computer and priority module, or directly from a non-safety HMI to a safety function computer - component or group control	3 multidivisional control and display stations
3. Human-Machine Interface (HMI) to multiple divisions of safety digital systems (Safety and Non-safety HMI)	3 multidivisional control and display stations
4. Operating a reactor using information displayed on a non-safety VDU for all plant conditions	3 multidivisional control and display stations
5. Requirements for priority modules	2 priority modules
6. Safety HMI control of non-safety components	3 multidivisional control and display stations
7. Design requirements (e.g., Quality and Qualification) for Non-Safety devices involved in inter-channel communication - Non-safety VDU - Shared sensors	3 multidivisional control and display stations
8. Communication involving diverse non-safety systems	1 data communications
9. Safety Communication Protocols - Profibus between safety divisions - Ethernet between digital safety systems and safety HMI	4 network configuration (integrated w/ other sections)

INTERIM STAFF GUIDANCE - MINIMUM INVENTORY OF HUMAN SYSTEM INTERFACES

DESCRIPTION

The purpose of this interim staff guidance is to better define the minimum inventory of human system interfaces (i.e., alarms, controls, and displays) needed to implement the plant's emergency operating procedures, bring the plant to a safe condition, and to carry out those human actions shown to be important from the applicant's probabilistic risk assessment. The improved definition and associated review criteria should minimize any inconsistencies in the staff review of a design-specific or plant-specific minimum inventory of human system interfaces.

STAFF POSITION

Development Process

1. The minimum inventory of human system interfaces in the main control room and at the remote shutdown panel should be identified.
 - a. The main control room minimum inventory should include the human system interfaces that the operator always needs available to:
 - i. Monitor the status of fission product barriers,
 - ii. Perform and confirm a reactor trip,
 - iii. Perform and confirm a controlled shutdown of the reactor using the normal or preferred means,
 - iv. Actuate safety related systems that have critical safety functions of protecting the fission product barriers, and
 - v. For analyzed failure conditions of the normal human system interfaces, maintain the current plant operating condition and power level until the human system interfaces are restored in accordance with applicable regulatory requirements.
 - b. The minimum inventory at the remote shutdown panel should include the human system interfaces that the operator always needs available to:
 - i. Monitor the status of fission product barriers,
 - ii. Perform and confirm a reactor trip, and
 - iii. Perform and confirm a controlled shutdown of the reactor using the normal or preferred means.
 - c. The minimum inventory of human system interfaces in the main control room and at the remote shutdown panel should:
 - i. Be readily accessible to the operator and
 - ii. Meet all the applicable regulatory requirements for independence, diversity and defense-in-depth, equipment qualification, and quality.

Selection Criteria

2. Applicants seeking approval of a new main control room or remote shutdown panel should provide a description of the process that will be used to identify the minimum inventory in the main control room and at the remote shutdown panel.

At a minimum, the description of the identification process should include discussion of:

- a. the selection criteria,
 - b. the functions and tasks need to be supported by the minimum inventory human system interfaces,
 - c. the design requirements that apply to the human system interfaces including those imposed by regulatory requirements, and particularly addressing requirements related to qualification, independence, and accessibility,
 - a. the use of plant-specific probabilistic risk assessment that may identify operator actions or tasks that are risk significant,
 - b. the guidance provided in Regulatory Guide 1.97, Rev. 4,
 - c. the manual operator actions credited in the safety analysis or plant-specific emergency operating procedures (if available) for safety and non-safety success paths, and
 - d. the diversity and defense-in-depth evaluation that may identify any specific manual operator actions credited for coping with common cause failures of digital protection systems.
3. Applicants seeking approval of a new main control room or remote shutdown panel should provide a description of the process that will be used to verify the completeness of the minimum inventory in the main control room and at the remote shutdown panel.

At a minimum the description of the verification process should include discussion of:

- a. The use of generic technical guidelines for developing emergency operating procedures or plant-specific emergency operating procedures,
 - b. the function-based task analysis that describes the operator manual actions necessary to bring the reactor to a safe shutdown under conditions where the primary instrumentation is either available and unavailable,
 - c. the operator manual actions identified through the plant-specific probabilistic risk assessment or plant-specific human reliability analysis,
 - d. the critical operator manual actions credited for diversity and defense-in-depth (including those for coping with common cause failures), and
 - e. discussion of the use of a full-scope simulator that meets the guidance in ANSI/ANS 3.5.
4. The completeness of the minimum inventory should be verified once the control room design has been implemented (e.g., construction or modification of full-scope or plant-reference simulator).
 5. The as-built main control room and remote shutdown facility should be evaluated to assure that they contain all the minimum inventory determined from the development process and selection criteria.

6. The applicable sections of the plant's Design Certification Document and Update Final Safety Analysis Report should be updated to:
 - a. Include a description of the process used to identify the minimum inventory of human system interfaces (i.e., alarms, controls, displays) in the main control room and at the remote shutdown panel,
 - b. Include a description of the identified failure conditions of the normal human system interfaces, and
 - c. Include the list of the minimum inventory of human system interfaces (i.e., alarms, controls, displays) in the main control room and at the remote shutdown panel.

STAFF RATIONALE

The staff review of an applicant's minimum inventory will be multi-disciplinary consisting of inputs from human factors engineering; instrumentation and controls; risk assessment; plant, reactor, and electrical engineering.

As stated in SECY 92-053, the staff identified control room design and advanced instrumentation and controls as areas where detailed design information may not be available for staff review during a design certification. Since then, the staff has developed a two-part approach for the review of the human factor aspects of the control room design. The first part involves a review to establish the minimum inventory of human system interfaces necessary for the operators to implement the emergency operating procedures, bring the plant to a safe condition, and to carry out those human actions shown to be important from the applicant's PRA. The minimum inventory will be included in the design certification. The second part of the staff's review will utilize design acceptance criteria to ensure the implementation of a systematic approach to the incorporation of human factors principles in completing the design of the control room, such as alarms, displays, and controls.

REFERENCES

1. 10 CFR 50.34(f) - post-TMI requirements for improved safety monitoring and control
2. NUREG-0800 Chapter 18 - guidance on Safety Parameter Display Systems
3. NUREG-0700 - guidance on reviewing human factors aspects of HSI design
4. NUREG-0711 - guidance on task analysis, PRA/HRA, risk-important operator actions
5. Regulatory Guide 1.97 - criteria for accident monitoring instrumentation
6. Regulatory Guide 1.47 - guidance on bypassed and inoperable status indication
7. Regulatory Guide 1.62 - guidance on manual initiation of protective actions
8. NUREG-0800 Chapter 7, Branch Technical Position (BTP) 7-19 - guidance on diversity and defense-in-depth

9. IEEE 603 - standard criteria for safety systems
10. ANSI/ANS 3.5 - guidance for the design and application of nuclear power plant simulators
11. SECY 92-053 - guidance on the use of DAC
12. SECY 93-087 - guidance on policy, technical and licensing issues related to ALWR designs

DRAFT

DRAFT

INTERIM STAFF GUIDANCE - COMPUTER-BASED PROCEDURES

DESCRIPTION

The purpose of this interim staff guidance is to provide additional review guidance for computer-based procedure systems and computer-based procedures for use by NRC Staff. This guidance is intended to complement existing guidance for procedure review that can be found in NUREG-0700 and NUREG-0899 (see Ref 1 and 2). This additional guidance should minimize any inconsistencies in the staff review of design-specific or plant-specific computer-based procedure systems and computer-based procedures.

This guidance may be generalized to any procedure type that is presented on a video display unit.

STAFF POSITION

Applicants and licensees that plan to implement a computer-based procedure system should provide a description of the computer-based procedure system that includes discussion of:

1. Interaction between the operator and the computer-based procedure,
2. Interaction between the computer-based procedure system and the control and process systems,
3. The use of plant data, if any, in the computer-based procedure system,
4. The use of automation, if any, in the computer-based procedure system,
5. The use of soft controls, if any, in the computer-based procedure system,
6. Presentation of procedures on the computer-based procedure system, and
7. Implementation of backup system to the computer-based procedure system.

Computer-Based Procedures Systems

General Review Criteria:

1. A computer-based procedure system that displays operations procedures should be designed as an integral part of the Main Control Room.
2. The procedure user (e.g., operators) should always be in control of the procedure system. The computer-based procedure system should be designed to provide the user with sufficient information for the user to know they are in control.
3. The computer-based procedure system should indicate its current operating mode (e.g., waiting for user input; implementing a procedure step, continuously monitoring a plant parameter). The computer-based procedure system should indicate if there is a mode change. Mode errors should be minimized by limiting the number of modes a computer-based procedure system can have.
4. The computer-based procedure system should always present the most recent approved and issued version of a procedure.

5. Measures should be provided to ensure that the computer-based procedure system will display the selected procedure. Measures should be provided to inform the operator, if the selected procedure is not displayed.
6. The design of a computer-based procedure system should allow the operator to easily transition from one procedure to another procedure, at any time.
7. A computer-based procedure system should meet all the applicable regulatory requirements for equipment qualification and quality.

Plant Data Review Criteria:

The display of plant data may or may not be incorporated into the design of a computer-based procedure system.

8. Computer-based procedure systems that require the user to enter data should provide a method for data entry.
9. Measures should be provided to ensure that plant data, displayed in a computer-based procedure system, is correct. Measures should be provided to inform the operator if the plant data presented is unvalidated or invalid.

Automation Review Criteria:

The use of automation may or may not be incorporated into the design of a computer-based procedure system.

10. Automation of procedure steps should be predictable. The automation should be initiated by the operator. The operator should be able to easily interrupt the automated sequence and step, one-by-one, through each procedure step.
11. Automation should not select the procedure to be used. The user should be responsible for selecting the procedure. However, a computer-based system can recommend (e.g., via prompts) a procedure.
12. The computer-based procedure system should not automatically initiate control actions without first receiving a command from the operator to do so. The computer-based system can prompt the operator to take a specific manual action if an automatic control function fails
13. Hold points should be established to allow operators to effectively monitor automation progress, maintain adequate situation awareness, and evaluate decisions at critical points in the procedure.
14. If emergency operating procedures are designed to include automation the following guidance is appropriate. The computer-based procedure should:
 - a. Inform the operator when presenting concurrent steps, such as steps in

two different legs of a BWROG flowchart emergency operating procedures.

- b. Inform the user of "Result Not Obtained" and present contingency actions.
- c. Monitor procedure entry conditions, cautions, warnings, branches, and exits.
- d. Be integrated with alarms, system status, and critical safety functions.
- e. Continuously applicable steps should be identified to the operator.
- f. Concurrent use of multiple procedures should be addressed.

Soft Control Review Criteria:

The use of soft controls may or may not be incorporated into the design of a computer-based procedure system.

- 15. A computer-based procedure system should contain concise set of soft controls whose meaning should be obvious to the user. Soft controls have a single control function.
- 16. Soft controls should provide needed feedback to the user regarding the state of the control.
- 17. The control of plant equipment by an operator should take at least two discrete actions.
- 18. Soft control behavior should not violate stereotypes, of hard or soft controls, already in place in a Main Control Room.
- 19. A computer-based procedure system should provide a simple method to allow the operator to retract a command once issued.

Modernization Review Criteria:

- 20. When implementing a computer-based procedure system into a Main Control Room via a modernization project, the human system interface conventions should include plant-specific standards that are in place at the site where the computer-based procedure system will be implemented. Additional: Failure to understand local conventions can result in conflicting sets of mental models and lead to an operational error.

Computer-Based Procedures

General Review Criteria:

- 21. Computer-based procedures should be written and formatted to be readable and usable on the display device of choice. If the procedure is presented on more than one "page" then continuous scrolling should be implemented. The computer-based procedure system should only allow up/down scrolling.

22. The computer-based procedure should be written and verified in its entirety, per station procedure, prior to being turned over to the respective user group. The computer-based procedure system should not change the approved procedure.
23. Computer-based procedures should provide the user with a minimum set of information to allow the user to know the state of the procedure system and the plant as appropriate to the procedure. The minimum set of information should include:
 - a. The procedure title should be continuously displayed on the screen at all times.
 - b. Each procedure should be organized into sections of related steps.
 - c. emergency operating procedures entry conditions should be continuously displayed at all times.
 - d. Verification steps are used to ensure that objective(s) of a task or sequence of actions has been met.
 - e. If the computer-based procedure is such that conclusions or recommendations are presented, the computer-based procedure should provide easily retrievable information regarding how it reached its conclusions.
24. The computer-based procedures should provide a means to access all meta-data (e.g., author, plant name, Unit, procedure type, etc.). However, the meta-data does not need to be presented to the operator.

Backup Procedures Review Criteria:

25. Back-up procedures should be maintained to ensure the ability to perform all emergency operating procedures and safety-related functions. The backup procedures can be paper-based or on another computer-based procedure system that is safety-related.
26. Backup procedures should be available to those who need them in a manner and location that is timely for their use.
27. Backup procedure systems should be subject to the same procedural controls as the primary computer-based procedure system.
28. Backup procedures and the primary computer-based procedure system should have a consistent presentation.
29. A means should be provided to ensure the primary computer-based procedure system and the backup are consistent.
30. A means should be provided to ensure that the correct procedure and step will be displayed to the operator that needs to use the backup procedure.

STAFF RATIONALE

The staff review of an applicant's or licensee's computer-based procedure system will be multi-disciplinary consisting of inputs from human factors engineering, instrumentation and controls, and electrical engineering.

In the past, procedures were typically written documents (including both text and graphic formats) that present a series of decision and action steps to be performed by plant personnel (e.g., operators and technicians) in order to accomplish a goal safely and efficiently. Procedures are used for a wide variety of tasks from administration to testing, and plant operation. Computer-based procedure systems were developed as an alternate to paper-based procedures to assist personnel in performing their tasks in order to increase the likelihood that the goals of the tasks would be safely achieved.

The content and development of paper-based and computer-based procedures can be essentially the same. Both should be easy to use. However, there can be significant differences in how the procedures are presented, the method for providing information to operators, and how operators interact with the procedure. The differences (e.g., automation) possible with computer-based procedures should not limit the control or situational awareness of licensed operators, to have full knowledge of the plant.

REFERENCES

1. NUREG-0700
2. NUREG-0899
3. NUREG-0800
4. NUREG-0696
5. NUREG-0835
6. RG 1.47



About NRC

Digital Instrumentation and Controls

Overview

History of Digital I&C

Key Issues

Nuclear Reactors

Nuclear Materials

Radioactive Waste

Steering Committee

Nuclear Security

Public Meetings

Public Meetings & Involvement

Related Information

Frequently Asked Questions

Reports and Correspondence

Regulations and Guidance

Technical References

Regulatory References

Other Correspondence

Contact Us About Digital I&C

[Home](#) > [About NRC](#) > [How We Regulate](#) > [Research Activities](#) > [Digital I&C](#) > [Preapplication Review](#)

Preapplication Review

The nuclear industry has submitted, and will continue to submit, a number of digital I&C technical and topical reports for NRC review and approval in preparation for future applications for standard design certifications, combined operating licenses, and/or upgrades to the current operating nuclear facilities. The NRC staff is actively interacting with individual applicants and is promoting dialogues on the technical and topical reports.

Update of Guidance Documents

The NRC has been working to expeditiously revise and update various digital I&C regulatory documents such as regulatory guides and Standard Review Plan (SRP) [NUREG-0800](#).

Regulatory guides provide guidance to licensees, applicants, and stakeholders on the implementation of specific parts of NRC regulations, NRC staff review techniques, data needed for reviews by the NRC staff, and the preferred standard format and content for information submitted for NRC approval. The SRPs furnish guidance to the NRC staff for reviewing licensee applications.

Interface with Other Agencies and the International Community

The NRC has been interacting, and plans to interact, with other Federal agencies (such as the Department of Defense, Federal Aviation Administration, and National Aeronautics and Space Administration) to share operating experience and lessons learned.

The NRC staff is actively interacting with other countries, their agencies, and international partners to share operating experience, regulatory processes and practices, and information on current and future activities with respect to the deployment of digital I&C to nuclear facilities. For example, the NRC staff is working closely with countries such as Finland, Taiwan, Japan, Korea, France, and the United Kingdom on the subject.

In addition, the NRC continues to support the digital I&C and human-machine interface research that is being conducted at the OECD Halden Reactor Project. This work is aimed at addressing challenges that include the impact of rapidly changing technology, increasing complexity, new failure modes, system and human reliability metrics, new concepts of operation, and the need to update acceptance criteria and review procedures.



TOP

[Privacy Policy](#) | [Site Disclaimer](#)

Wednesday, July 11, 2007



Protecting People and the Environment

About NRC

Digital Instrumentation and Controls

Overview

• Nuclear Reactors

Key Issues

• Nuclear Materials

• Radioactive Waste

Steering Committee

• Nuclear Security

• Public Review

• Meetings

• Involvement

Related Information

Frequently Asked Questions

Reports and Correspondence

Regulations and Guidance

Technical References

Regulatory References

Other Correspondence

Contact Us About Digital I&C

[Home](#) > [About NRC](#) > [How We Regulate](#) > [Research Activities](#) > [Digital I&C](#) > [Design Certification](#)

Design Certification

In August 2005, General Electric Company submitted an application for final design approval and standard design certification of the economic simplified boiling-water reactor (ESBWR) standard plant design. The NRC staff is performing a detailed review of the application's digital I&C area. The NRC staff has previously certified the AP600, CE System 80+, AP1000 and advanced boiling-water reactor (ABWR) standard plant designs. The NRC expects to receive two additional applications for standard design certification for agency review in 2008, namely, for the evolutionary power reactor (EPR) and the advanced pressurized-water reactor (APWR).

[Privacy Policy](#) | [Site Disclaimer](#)

Wednesday, July 11, 2007