U.S.NRC

UNITED STATES NUCLEAR REGULATORY COMMISSION

Protecting People and the Environment

PROJECT PLAN

Digital Instrumentation and Control

DRAFT

Approved by the Digital I&C Steering Committee

Revision 2, December 9, 2008

U.S.NRC

UNITED STATES NUCLEAR REGULATORY COMMISSION

Protecting People and the Environment

PROJECT PLAN

Digital Instrumentation and Control

DRAFT

Approved by the Digital I&C Steering Committee

Revision 2, December 9, 2008

* - concurrence by e-mail

OFFICE		NRR/DE	NRO/DE	NMSS/FCSS
NAME		SBailey	MMayfield	MBailey
DATE				
OFFICE	NSIR/DSP	RES/DE	NRR/ADES	
NAME	SMorris	MCase	JGrobe	
DATE				

DIGITAL I&C PROJECT PLAN

LIST OF REVISIONS	
REVISION	DATE
0	JULY 12, 2007
1	MARCH 14, 2008
2	DECEMBER 9, 2008

DRAFT

DIGITAL I&C PROJECT PLAN

1. PURPOSE:

The purpose of the Digital Instrumentation and Controls (DI&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 DI&C Steering Committee and the Task Working Groups (TWGs). It describes the process to develop Interim Staff Guidance (ISG) for the review of DI&C technology for new reactors, operating reactors, and fuel cycle facilities. The DI&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.

2. OBJECTIVES:

The specific short-term objective of this plan is to identify DI&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 DI&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.

3. 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 DI&C Project Plan activities to support development of the final regulatory guidance on diversity and defense-in-depth.

4. DIGITAL I&C STEERING COMMITTEE:

The DI&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 DI&C issues, (2) to oversee and facilitate resolution of technical and regulatory issues related to the deployment of DI&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 DI&C Project Plan implementation and review specific goals and deliverables. The Steering Committee will approve the initial DI&C Project Plan and subsequent revisions to the plan. The Steering Committee will approve Interim Staff Guidance generated by the TWGs.

DRAFT

5. TASK WORKING GROUPS:

The DI&C Task Working Groups (TWGs) were established to include technical staff from appropriate NRC offices to focus on seven key areas. The TWG interactions with industry counterparts were designed to facilitate discussion of technical and regulatory issues and the development of recommendations to effectively address DI&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.

6. 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 provided 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.

7. 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 ISG and the long-term deliverables such as recommendations to revise regulatory guidance, and recommendations for revision to industry standards, as necessary.

8. INDIVIDUAL TWG PROJECT PLANS:

The TWGs have developed an individual TWG project plan for each of the 7 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
TWG #7: Fuel Cycle Facilities

DRAFT

9. 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 specifications for new plant simulators and for the design and implementation of digital retrofits at existing plants.

10. UPDATE PROCESS:

The Steering Committee will approve the initial Digital I&C Project Plan and subsequent revisions to the DI&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 periodic basis. As the TWG project efforts proceed and industry planning data becomes available, deliverable dates will be identified for long-term activities that reflect best-estimates based on standard agency processes. These estimates will also consider available resources, current schedules, and budgets.

11. 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
7. Project Plan - TWG # 7 Fuel Cycle Facilities

DRAFT

Appendix 1
TWG # 1: Cyber Security

1. BACKGROUND:

In December 2005 the NRC Office of Nuclear Security and Incident Response (NSIR) accepted Nuclear Energy Institute (NEI) guidance document NEI 04-04, "Cyber Security Programs for Power Reactors," Revision 1, dated November 18, 2005, as a 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, 10 CFR 73.54 (originally published as 10 CFR 73.55(m)), is generally considered to be beyond the scope of this working group. Development of these guidance documents is included as a long term action in Section 5 since they are needed to retire the ISG. The evaluation of specific cyber security technologies, such as firewalls and intrusion detection systems (IDS), is also not within the scope of this task working group.

3. PROBLEM STATEMENT:

Problem 1 <u>Cyber Security Requirements for Safety Systems</u>: 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.

Appendix 1
TWG # 1: Cyber Security

4. DELIVERABLES:

A. 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.

DRAFT

Appendix 1
TWG # 1: Cyber Security

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					
Issue draft Cyber Security Project Plan	√	03/29/07	A	NRC	n/a
Issue Cyber Security Project Plan	√	04/13/07	A	NRC	n/a
Complete gap analysis of RG 1.152R2 and NEI 04-04	√	04/30/07	A	NRC	NEI
Industry provides changes to NEI 04-04 to address issues identified in the gap analysis	√	08/17/07	A	NEI	n/a
Issue draft Interim Staff Guidance	√	08/17/07	A	NRC	n/a
Receive industry comments on draft Interim Staff Guidance	√	08/24/07	A	NEI	n/a
Industry provides cross-correlation table between RG 1.152 and NEI 04-04 for NRC Review/Comment	√	08/31/07	A	NEI	n/a
TWG revised cross-correlation table provided to Industry for Review/Comment	√	11/01/07	A	NRC	n/a
Industry provides revised NEI 04-04, revised cross-correlation table, and comments to draft ISG	√	12/04/07	A	NEI	n/a
Issue Interim Staff Guidance (ML072980159)	√	12/31/07	A	NRC	n/a
LONG-TERM *					
Problem 1: Cyber Security Requirements for Safety Systems					
Develop and Issue Regulatory Guide to Support Proposed Rule 10 CFR 73.54 (originally published as 10CFR73.55(m))					
Posting of Proposed Rule 10CFR73.54	√	04/18/08	A	NRC	n/a
Develop draft Regulatory Guide DG-5022 to support Proposed Rule	√	05/20/08	A	NRC	n/a
Issue DG for public comment to authorized stakeholders (comment period 6/9/08 - 7/24/08)	√	06/02/08	A	NRC	n/a
Brief ACRS		06/04/08	A	NRC	n/a

DRAFT

Appendix 1
TWG # 1: Cyber Security

TWG#1: CYBER SECURITY					
Milestones, Assignments and Deliverables	**Deliverable**	**Due Date**	**Fcst/Actual**	**Lead**	**Support**
Final rule wording re-posted to match submittal to Commission	√	07/11/08	A	NRC	n/a
DG-5022 re-drafted and released for comments	√	12/04/08	A	NRC	n/a
Disposition Stakeholder Comments		01/2009			
Brief ACRS on Final Regulatory Guide		02/2009	F	NRC	n/a
Publish Final Regulatory Guide to support Proposed Rule	√	Spring 09	F	NRC	n/a
Develop and Issue Revisions to SRP Chapter 7					
Develop Draft Revisions to SRP Chapter 7	√	06/30/09	F	NRC	n/a
Issue for Public Comment		**08/31/09**	F	NRC	n/a
Develop and Issue Revisions to Reg. Guide 1.152					
Develop Draft Revisions to Reg. Guide 1.152	√	06/30/09	F	NRC	n/a
Issue for Public Comment		**08/31/09**	F	NRC	n/a
Develop and Issue Revisions to SRP Chapter 13					
Develop Draft Revisions to SRP Chapter 13	√	06/30/09	F	NRC	n/a
Issue for Public Comment		**08/31/09**	F	NRC	n/a
NEI 04-04, Rev. 2, Cyber Security Program for Power Reactors					
Evaluate Need for NRC Endorsement of NEI 04-04, Rev. 2 (1)		11/04/08	A	NEI	n/a
TWG Ends		**08/31/09**	F	NRC	n/a

* Long term actions are those actions necessary to incorporate the ISG's into regulatory infrastructure (Reg. Guides, NUREG's, SRP, etc.). Long term actions are conducted through established agency processes, and are generally outside the control of the TWG's. Dates in bolded text reflect the end of significant TWG activity in completion of a particular action.

(1) This item was determined not to be necessary.

Appendix 2
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 have 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. 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.

E. Recommend ISG to be incorporated into NRC Standard Review Plans and other regulatory guidance.

F. Address the action items stemming from the Commission meeting with the ACRS.

DRAFT

Appendix 2
TWG # 2: Diversity and Defense-In-Depth

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 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 3 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 4 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 5 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:

Appendix 2
TWG # 2: Diversity and Defense-In-Depth

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 6 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:

A. 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.

B. 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.

C. 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).

Appendix 2
TWG # 2: Diversity and Defense-In-Depth

In accordance with the recommendation from the ACRS for the staff to further evaluate the subject of spurious actuations as part of the long-term development of the diversity and defense-in-depth guidance, the staff's long-term evaluation would include the areas of automatically reconfigurable systems and unintended functions actuated during the progression of a plant transient or accident. The staff will further assess spurious actuations and develop additional guidance, as needed, when the formal guidance document, SRP BTP-19, is updated incorporating the ISG and industry feedback.

D. 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.

E. Echelons of Defense: ISG will be developed to describe appropriate levels of defense-in-depth in safety system designs.

F. 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.

DRAFT

Appendix 2
TWG # 2: Diversity and Defense-In-Depth

5. MILESTONES, ASSIGNMENTS, AND DELIVERABLES:

TWG #2: DIVERSITY AND DEFENSE-IN-DEPTH					
Milestones, Assignments and Deliverables	**Deliverable**	**Due Date**	**Fcst/Actual**	**Lead**	**Support**
NEAR-TERM					
Problem 1: Adequate Diversity					
Develop draft Interim Staff Guidance		06/21/07	A	NRC	N/A
Issue draft Interim Staff Guidance	√	06/22/07	A	NRC	n/a
Discuss draft Interim Staff Guidance in public mtg		06/22/07	A	NRC	NEI
Receive comments		07/06/07	A	NRC	n/a
Issue Interim Staff Guidance (ML072540118)	√	09/28/07	A	NRC	n/a
Problem 1a: Manual Operator Action					
Develop draft Interim Staff Guidance		06/14/07	A	NRC	NEI
Issue draft Interim Staff Guidance	√	06/22/07	A	NRC	n/a
Discuss draft Interim Staff Guidance in public mtg		06/22/07	A	NRC	NEI
Receive comments		07/06/07	A	NRC	n/a
Issue Interim Staff Guidance (ML072540118)	√	09/28/07	A	NRC	n/a
Problem 2: BTP-19, Position 4 Challenges Problem 3: Effects of Common-Cause Failure Problem 4: Common-Cause Failure Applicability Problem 5: Echelons of Defense Problem 6: Single Failure					
Develop draft Interim Staff Guidance		08/07/07	A	NRC	NEI
Issue draft Interim Staff Guidance	√	08/07/07 (2, 3, 4, 5) 09/07/07 (6)	A	NRC	n/a

DRAFT

Appendix 2
TWG # 2: Diversity and Defense-In-Depth

TWG #2: DIVERSITY AND DEFENSE-IN-DEPTH					
Milestones, Assignments and Deliverables	**Deliverable**	**Due Date**	**Fcst/Actual**	**Lead**	**Support**
Discuss draft Interim Staff Guidance in public Meeting		08/09/07	A	NRC	NEI
Issue Interim Staff Guidance (ML072540118)	√	09/28/07	A	NRC	n/a
Edit Interim Staff Guidance re: IEEE-603 reference	√	01/30/09	F	NRC	n/a
LONG-TERM *					
Inventory and Classification of Digital Systems					
Develop draft assessment results	√	09/28/07	A	NRC	n/a
Provide assessment results with appropriate recommendations on staff guidance	√	02/29/08	A	NRC	n/a
Evaluation of Digital Systems Operating Experience Insights					
Develop draft assessment results	√	09/28/07	A	NRC	n/a
Industry to Provide White Paper on Evaluation of Operating Experience	√	06/13/08	A	NEI	n/a
Provide assessment results with appropriate recommendations on staff guidance	√	02/29/08	A	NRC	n/a

Appendix 2
TWG # 2: Diversity and Defense-In-Depth

TWG #2: DIVERSITY AND DEFENSE-IN-DEPTH					
Milestones, Assignments and Deliverables	**Deliverable**	**Due Date**	**Fcst/Actual**	**Lead**	**Support**
Problem 1: Adequate Diversity					
Receive Draft Report From ORNL	√	03/31/08	A	NRC	ORNL
Discuss Draft Report From ORNL in Public Mtg		07/08/08	A	NRC	NEI
Industry to Provide White Paper on Diversity/Defensive Measures Approach	√	TBD	F	NEI	n/a
Provide Comments to ORNL on Draft Report	√	06/15/08	A	NRC	n/a
ORNL Provides Final Report	√	12/2008	F	ORNL	n/a
Final draft NUREG	√	02/2009	F	NRC	n/a
Brief ACRS on NUREG		02/26/09	F	NRC	n/a
Industry to Provide Feedback on ORNL Draft Report	√	02/26/09	F	NEI	n/a
Publish NUREG (1)	√	**03/27/09**	F	NRC	n/a
Problem 2: BTP-19, Position 4 Challenges					
Industry to Provide Feedback to ISG	√	06/30/08	A	NEI	n/a
Problem 3: Effects of Common Cause Failure					
Industry to Provide Feedback to ISG	√	06/30/08	A	NEI	n/a
Problem 4: Common-Cause Failure Applicability					
Industry to Provide White Paper on Common Cause Failure Applicability	√	02/29/08	A	NEI	n/a
Problem 5: Echelons of Defense					
Industry to Provide Feedback to ISG	√	02/29/08	A	NEI	n/a

DRAFT

Appendix 2
TWG # 2: Diversity and Defense-In-Depth

TWG #2: DIVERSITY AND DEFENSE-IN-DEPTH					
Milestones, Assignments and Deliverables	**Deliverable**	**Due Date**	**Fcst/Actual**	**Lead**	**Support**
Problem 6: Single Failure					
Industry to Provide Feedback to ISG	√	06/30/08	A	NEI	n/a
Common Long-Term Actions					
Develop and Issue Revisions to SRP Chapter 7					
Develop Draft Revisions to SRP Chapter 7 and BTP 7-19	√	06/30/09	F	NRC	n/a
Issue for Public Comment		**08/31/08**	F	NRC	n/a
TWG Ends		**08/31/09**	F	NRC	n/a

* Long term actions are those actions necessary to incorporate the ISG's into regulatory infrastructure (Reg. Guides, NUREG's, SRP, etc.). Long term actions are conducted through established agency processes, and are generally outside the control of the TWG's. Dates in bolded text reflect the end of significant TWG activity in completion of a particular action.

(1) This NUREG is not expected to result in changes to the ISG. Changes that result from this NUREG will be incorporated in the SRP update.

DRAFT

Appendix 3
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 and new reactors. 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.

DRAFT

Appendix 3
TWG # 3: Risk Informing Digital I & C

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 these reliability methods are developed, additional NRC staff guidance to support risk-informing digital system reviews will be required.

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, there is a need for 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 the evaluation of digital system common cause failures.

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 acceptance guidelines to support licensing of operating reactor upgrades and new reactors 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.

DRAFT

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 (1) five key principles of risk-informed decision-making, and the (2) Commission PRA policy statements

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 limited 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 limited guidance on integrating risk insights into digital system reviews or risk-informing digital system reviews.

PROBLEM 1 Evaluation of digital systems in PRA: Existing guidance does not provide sufficient clarity on how to use current methods to properly evaluate digital systems in PRAs for DC or 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

Appendix 3
TWG # 3: Risk Informing Digital I & C

4. DELIVERABLES:

A. Evaluation of Digital Systems in PRA:

1. Issue review guidance for review of new reactor Digital I & C PRAs.

2. In the longer-term, update regulatory guidance as needed (SRP, Regulatory Guides, etc.).

B. Risk Insights:

1. 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.

2. If an acceptable approach can be established, issue guidance and acceptance criteria for use of risk insights in the evaluation of digital systems.

3. In the longer-term, update regulatory guidance as needed (SRP, Regulatory Guides, etc.).

Note: The Project Plan milestones for Problem 2 are outlined in Section 5 assuming there is a viable approach to risk-inform other ISGs or Regulatory Guides. The staff is reviewing several options for Problem 2 and will determine if additional work is justified.

C. State-of-the-Art:

1. Develop the technical basis and methods for modeling of digital systems to support risk-informed decision-making for digital systems, including: (1) review and assessment of 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. Identify and implement appropriate collaboration with and leverage the capabilities of the industry, international counterparts, other industries, and NRC staff and contractors in developing the technical basis and methods.

2. Issue regulatory guidance as appropriate on risk-informed decision-making review methods applicable to digital I&C systems.

3. Update NRC PRA data, models and tools to support NRC assessment of digital system risk and reliability.

DRAFT

Appendix 3
TWG # 3: Risk Informing Digital I & C

5. MILESTONES, ASSIGNMENTS, AND DELIVERABLES:

TWG#3: RISK-INFORMING					
Milestones, Assignments and Deliverables	**Deliverable**	**Due Date**	**Fcst/Actual**	**Lead**	**Support**
NEAR-TERM					
Problem 1: Guidance for Evaluation of New Reactor Digital I&C Systems PRA					
Industry to provide white paper discussing lessons-learned and proposed guidelines associated with modeling of digital systems for DC and COL applications	√	07/03/07	A	NEI	n/a
Develop Draft Interim Staff Guidance		11/06/07	A	NRC	n/a
Industry to Provide Additional Information Addressing the Staff's Input Concerning the Problem Statement # 1 White Paper	√	11/06/07	A	NEI	n/a
Issue draft Interim Staff Guidance	√	12/03/07	A	NRC	n/a
Receive Industry Feedback		01/04/08	A	NRC	n/a
Discuss Draft Interim Staff Guidance in public mtg		01/14/08	A	NRC	NEI
Discuss final version of the Draft interim Staff Guidance in public meeting		02/08/08	A	NRC	NEI
Issue Interim Staff Guidance	√	08/11/08	A	NRC	n/a
Problem 2: Risk Insights from DI&C PRA modeling Applied to Operating Reactors or New Reactors					
Industry identifies potential review areas where insights from PRA modeling of DI&C systems may be applied to risk-inform staff reviews (e.g., Technical Specifications, BTP-7-19 reviews)	√	01/14/08	A	NEI	n/a
Industry provides a white paper with specifics on (1) proposal to apply risk-insights to selected ISGs, and (2) the risk screening analysis from several plant-specific PRAs regarding D3 evaluations and the scope of a Diverse Actuation System.	√	05/16/08	A	NEI	n/a

DRAFT

Appendix 3
TWG # 3: Risk Informing Digital I & C

TWG#3: RISK-INFORMING					
Milestones, Assignments and Deliverables	**Deliverable**	**Due Date**	**Fcst/Actual**	**Lead**	**Support**
Industry provides a matrix comparison and gap analysis of industry's risk assessment approach versus (1) the NRC's draft NUREG on use of traditional PRA methods to model DI&C systems and (2) the draft ISG for problem statement #1	√	05/12/08	A	NEI	n/a
NRC reviews and comments on industry assessment of selected ISGs and proposed changes to regulatory guidance. NRC provides comments on the bases for the screening analysis inputs, assumptions, and conclusions.	√	11/03/08	A	NRC	n/a
Industry proposes pilot plant application and pilot charter consistent with treatment of other risk-informed initiatives (e.g., Tech Spec 4.b initiative)		11/03/08 (1)	A	NEI	n/a
NRC reviews and comments on charter for pilot plant application		11/03/08 (1)	A	NRC	n/a
Industry submits a topical report (methodology) to be used with pilot plant application and supporting basis demonstrating that the risk-informed principles of R.G. 1.174 are satisfied and other regulatory guides or policy related to the specific ISG being risk informed (e.g., SECY/SRM 93-087)	√	11/03/08 (1)	A	NEI	n/a
NRC completes acceptance review of industry submittal in accordance with staff procedures. If accepted, NRC reviews and comments on topical report and starts the pilot plant application review process - (staff uses available insights from NRC research work and others on the appropriate use of traditional methods)	√	11/03/08 (1)l	A	NRC	n/a
NRC staff endorses NEI topical report 2008-xx via a Safety Evaluation Report – draft ISG issued only if staff has exceptions to the topical report	√	11/03/08 (1)	A	NRC	n/a
Problem 3: State-of-the-Art					
EPRI to Draft MOU for DI&C	√	10/2008	A	EPRI	NRC

DRAFT

Appendix 3
TWG # 3: Risk Informing Digital I & C

TWG#3: RISK-INFORMING					
Milestones, Assignments and Deliverables	**Deliverable**	**Due Date**	**Fcst/Actual**	**Lead**	**Support**
NRC present DI&C Updated Research Plan for FY2010-FY2014 to ACRS		02/2009	F	NRC	n/a
Receive Industry Comments on Updated DI&C Research Plan		03/2009	F	NEI	NRC
NRC/EPRI Finalize MOU for DI&C Cooperative Research		04/2009	F	NRC	EPRI
NRC staff reviews final NUREGs on state-of-the art methods and assesses if further enhancements to regulatory guidance are warranted	√	08/31/09	F	NRC	NRC
Common Near Term Actions					
Industry to Provide Information Demonstrating How Their Approach Satisfies the Five Key Principles of Risk Informed Decision Making in RG 1.174	√	11/06/07	A	NEI	n/a
Industry to Provide Comments on initial Draft NUREG on Traditional Methods	√	11/16/07	A	NEI	n/a
LONG-TERM *					
Problem 1: Review Guidance for Evaluation of New Reactor Digital I&C Systems PRA					
Develop Draft Revisions to SRP Chapter 19.0	√	09/30/09	F	NRC	n/a
Issue for Public Comment	√	**11/30/09**	F	NRC	n/a
Problem 2: Risk Insights from DI&C PRA modeling Applied to Operating Reactors or New Reactors					
Develop Draft Revisions to SRP (e.g., Chapters 7, 19)	√	*11/03/08 (1) (2)*	*A*	*NRC*	*n/a*
Issue For Public Comment	√	*11/03/08 (1) (2)*	*A*	*NRC*	*n/a*
Problem 3: State-of-the-Art					
Develop risk-informed decision-making review methods applicable to digital systems if and when the methods are mature.	√	*(2)*	-	*NRC*	*n/a*

DRAFT

Appendix 3
TWG # 3: Risk Informing Digital I & C

TWG#3: RISK-INFORMING					
Milestones, Assignments and Deliverables	**Deliverable**	**Due Date**	**Fcst/Actual**	**Lead**	**Support**
Develop Draft Revisions to SRP Chapter 7 and other SRP Chapters if appropriate	√	*(2)*	-	*NRC*	*n/a*
Issue For Public Comment	√	*(2)*	-	*NRC*	*n/a*
TWG Ends		**11/30/09**	F	NRC	n/a

* Long term actions are those actions necessary to incorporate the ISG's into regulatory infrastructure (Reg. Guides, NUREG's, SRP, etc.). Long term actions are conducted through established agency processes, and are generally outside the control of the TWGs. Dates in bolded text reflect the end of significant TWG activity in completion of a particular action. *Items that are considered outside the scope of TWG activity are in italics.*

(1) It was determined that existing methods and data do not support using risk insights as described in these line items. This is discussed in the staff's letter dated 11/03/08.

(2) Further development of risk methods is being addressed by the 5-year research plan.

DRAFT

Appendix 4
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 divisions[1], 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

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.

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

Appendix 4
TWG # 4: Highly-Integrated Control Room – Communications

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:

A. Inter-Divisional Communications Independence:

1. Issue Interim Staff Guidance (ISG) that will document an acceptable degree of communications independence for digital systems.

2. Facilitate a revision to IEEE 7-4.3.2.

3. Recommend revisions to Regulatory Guide 1.152.

Appendix 4
TWG # 4: Highly-Integrated Control Room – Communications

4. 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.

DRAFT

Appendix 4
TWG # 4: Highly-Integrated Control Room – Communications

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.

DRAFT

Appendix 4
TWG # 4: Highly-Integrated Control Room – Communications

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.

Appendix 4
TWG # 4: Highly-Integrated Control Room – Communications

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		03/08/07	A	NRC	NEI
Receive industry proposals for HICR communication design concepts	√	06/01/07	A	NEI	n/a
Issue draft Interim Staff Guidance	√	08/10/07	A	NRC	n/a
Discuss draft Interim Staff Guidance in public meeting		08/14/07	A	NRC	NEI
Receive comments	√	08/14/07	A	NRC	n/a
Issue Interim Staff Guidance (ML072540138)	√	09/28/07	A	NRC	n/a
Clarify ISG re: use of non-safety controls	√	01/30/09	F	NRC	n/a
LONG-TERM *					
Problem 1: Communications Independence					
Issue Revised IEEE Standard 7-4.3.2 "Standard Criteria For Digital Computers In Safety Systems of Nuclear Power Generating Stations"					
IEEE Programmable Digital Computers to Safety Systems Working Group Meeting		01/22/08	A	IEEE	NRC/ NEI
IEEE Programmable Digital Computers to Safety Systems Working Group Meeting		07/14/08	A	IEEE	NRC/ NEI
IEEE Standards Meeting		01/2009	F	IEEE	NRC/ NEI

DRAFT

Appendix 4
TWG # 4: Highly-Integrated Control Room – Communications

TWG #4: Highly-Integrated Control Room—Communications					
Milestones, Assignments and Deliverables	**Deliverable**	**Due Date**	**Fcst/Actual**	**Lead**	**Support**
Letter to IEEE Subcommittee re: incorporating ISG into IEEE 7-4.3.2	√	01/30/09	F	NRC	n/a
Issue Revised IEEE Standard 7-4.3.2 "Standard Criteria For Digital Computers In Safety Systems of Nuclear Power Generating Stations" (1)	√	*06/30/10*	*F*	*NEI/ IEEE*	*NRC*
Develop and Issue Revisions to RG 1.152, Section 2					
Develop Draft Revisions to RG 1.152,	√	06/30/09	F	NRC	n/a
Issue For Public Comment	√	**08/31/09**	F	NRC	n/a
Develop and Issue Revisions to SRP Chapter 7					
Develop Draft Revisions to SRP Chapter 7	√	06/30/09	F	NRC	n/a
Issue For Public Comment	√	**08/31/09**	F	NRC	n/a
TWG Ends		**08/31/09**	F	NRC	n/a

* Long term actions are those actions necessary to incorporate the ISG's into regulatory infrastructure (Reg. Guides, NUREG's, SRP, etc.). Long term actions are conducted through established agency processes, and are generally outside the control of the TWG's. Dates in bolded text reflect the end of significant TWG activity in completion of a particular action. *Items that are considered outside the scope of TWG activity are in italics*

(1) This date is based on IEEE Standard Committee schedule for revising IEEE 7-4.3.2.

DRAFT

Appendix 5
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), or new reactors. 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 and new reactors with modernized control stations are expected to present new operational and maintenance environments due to the expanded use of digital systems. 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.

DRAFT

Appendix 5
TWG # 5: Highly-Integrated Control Room – Human Factors

2. SCOPE:

The scope of this effort is limited to human factors issues for new reactors and conventional LWRs. 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.

Problem 1 <u>Minimum Inventory.</u> 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.

Problem 2 <u>Computerized Procedures and Soft Controls.</u> 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.

Problem 3 <u>Safety Parameter Display System (SPDS).</u> 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."

Problem 4 <u>Graded Approach to Human Factors.</u> 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.

DRAFT

Appendix 5
TWG # 5: Highly-Integrated Control Room – Human Factors

Problem 5 Manual Operator Actions: Clarification is desired on the use of operator action as a defensive measure and corresponding acceptable operator action times.

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 and modernized LWRs.

5. Manual Operator Actions

F. 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 Diversity and Defense-in-Depth TWG # 2.

DRAFT

Appendix 5
TWG # 5: Highly-Integrated Control Room – Human Factors

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					
Receive industry proposal on minimum inventory	√	05/25/07	A	NEI	n/a
Industry to provide input for consideration in development of Interim Staff Guidance	√	07/20/07	A	NEI	n/a
Prepare Interim Staff Guidance		08/08/07	A	NRC	n/a
Issue draft Interim Staff Guidance	√	08/08/07	A	NRC	n/a
Discuss draft Interim Staff Guidance in public meeting		08/08/07	A	NRC	NEI
Receive Industry Comments	√	08/24/07	A	NRC	n/a
Issue Interim Staff Guidance (ML072540140)	√	09/28/07	A	NRC	n/a
Problem 2. Computer-Based Procedures and Soft Controls					
Industry to provide input for consideration in development of Interim Staff Guidance	√	07/20/07	A	NEI	n/a
Prepare Interim Staff Guidance		08/08/07	A	NRC	n/a
Issue draft Interim Staff Guidance	√	08/08/07	A	NRC	n/a
Discuss draft Interim Staff Guidance in public meeting		08/08/07	A	NRC	NEI
Receive Industry Comments	√	08/24/07	A	NRC	n/a
Industry to Provide White Paper on Computerized Procedures	√	07/30/07	A	NEI	n/a

DRAFT

Appendix 5
TWG # 5: Highly-Integrated Control Room – Human Factors

TWG #5: Highly-Integrated Control Room—Human Factors					
Milestones, Assignments and Deliverables	**Deliverable**	**Due Date**	**Fcst/Actual**	**Lead**	**Support**
Issue Interim Staff Guidance (ML072540140)	√	09/28/07	A	NRC	n/a
Problem 3. Safety Parameter Display System					
No near-term deliverables					
Problem 4. Graded Approach to Human Factors					
No near-term deliverables					
Problem 5: Manual Operator Action					
Industry to Provide White Paper on Manual Operator Action	√	08/2007	A	NEI	n/a
Provide Comments on White Paper on Manual Operator Action	√	01/16/08	A	NRC	n/a
Issue draft Interim Staff Guidance	√	08/20/08	A	NRC	n/a
Discuss Draft Interim Staff Guidance in Public Meeting		08/25/08	A	NRC	NEI
Receive and Disposition Stakeholders Comments	√	09/19/08	A	NRC	n/a
Issue Interim Staff Guidance	√	11/10/08	A	NRC	n/a
LONG-TERM *					
Problem 1. Minimum Inventory					
Industry to Provide Revision to White Paper on Minimum Inventory	√	12/21/07	A	NEI	n/a
Provide Comments on Revised Industry White Paper	√	02/20/08	A	NRC	n/a
Develop Draft Revisions to SRP Chapter 18		**01/29/09**	F	NRC	n/a

DRAFT

Appendix 5
TWG # 5: Highly-Integrated Control Room – Human Factors

TWG #5: Highly-Integrated Control Room—Human Factors					
Milestones, Assignments and Deliverables	**Deliverable**	**Due Date**	**Fcst/Actual**	**Lead**	**Support**
Issue For Public Comment	√	03/31/09	F	NRC	n/a
Problem 2. Computer-Based Procedures and Soft Controls					
Industry to Provide White Paper on Computer-Based Procedures	√	12/17/07	A	NEI	n/a
Provide Comments on Industry White Paper	√	01/16/08	A	NRC	n/a
Receive Additional Input from Stakeholders for Consideration to be included in revised or Supplemented Human Factors Review Guidance		12/2008	F	NRC	n/a
Develop draft NUREG revising or supplementing human factors guidance	√	09/30/09	F	NRC	n/a
Issue For Public Comment	√	**11/30/09**	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		08/2007	A	NRC	NEI
Document results of review		01/31/09	F	NRC	n/a
Prepare Technical Basis for Rulemaking		03/31/09	F	NRC	n/a
Request Approval for a Rulemaking from Rulemaking Coordination Committee		**05/31/09**	F	NRC	n/a
Publish Direct Final and Proposed Rule to Revise SPDS rule language	√	*05/2010*	*F*	*NRC*	*n/a*
Publish Confirmation of Effective Date for Direct Final Rule	√	*09/2010*	*F*	*NRC*	*n/a*

DRAFT

Appendix 5
TWG # 5: Highly-Integrated Control Room – Human Factors

TWG #5: Highly-Integrated Control Room—Human Factors					
Milestones, Assignments and Deliverables	**Deliverable**	**Due Date**	**Fcst/Actual**	**Lead**	**Support**
Problem 4. Graded Approach to Human Factors					
No long term deliverables					
Problem 5. Manual Operator Action					
Develop Draft Guide to Related to Manual Operator Action	√	09/30/09	F	NRC	n/a
Issue For Public Comment	√	**11/30/09**	F	NRC	n/a
TWG Ends		**11/30/09**	F	NRC	n/a

* Long term actions are those actions necessary to incorporate the ISG's into regulatory infrastructure (Reg. Guides, NUREG's, SRP, etc.). Long term actions are conducted through established agency processes, and are generally outside the control of the TWG's. Dates in bolded text reflect the end of significant TWG activity in completion of a particular action. *Items that are considered outside the scope of TWG activity are in italics*.

DRAFT

Appendix 6
TWG # 6: Licensing Process

1. BACKGROUND:

Guidance for the content of license applications and amendments involving licensing digital instrumentation and control (DI&C) systems and components is contained in Chapter 7 (Instrumentation and Controls) of NUREG-0800 (Standard Review Plan (SRP) for the Review of Safety Analysis Reports for Nuclear Power Plants).

However, licensing of DI&C 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 operating reactors. The outcomes from each of the other 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:

A. Identify the regulatory requirements, acceptance criteria, and guidelines that are to be addressed for a license amendment for an RPS/ESF upgrade using digital technology at existing plants.

B. Develop proposed resolutions to licensing process issues that emerge during the development and implementation of digital I&C technology for operating 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 address 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 SRP Chapter 7 and other applicable ISGs (i.e., communications and cyber security).

B. The stability and repeatability of the digital I&C licensing process.

C. The interests of the agency, the industry, and public stakeholders.

DRAFT

D. The resolution of licensing process uncertainties about, for example:

1. Policy and procedural issues
2. The clarity of guidance and acceptance criteria for licensing submittal format and content
3. The level of detail in licensing submittals
4. The sequencing of steps in the licensing process
5. Submittal and review schedule

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. 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 licensing actions for operating reactors necessary to begin and complete the regulatory reviews.

Problem 2 Applicability: Clear guidance for operating reactors regarding the applicability of Chapter 7 of the Standard Review Plan (NUREG-0800) to digital instrumentation and control upgrades.

Problem 3 Clear Process Protocols: Clear licensing process protocols for developing the application and NRC review of digital technology licensing actions.

Problem 4 Clear Guidance: Clear guidance on licensing criteria for cyber security in DI&C safety systems needs to be developed.

4. DELIVERABLES:

The deliverables for TWG#6 are intended to simultaneously address the first three problem statements. Problem statement 4 will be addressed as the information is developed.

A. Issue Interim Staff Guidance that provides specific guidance on (1) the applicable design requirements, (2) the information to be docketed, (3) the information to be available for staff audit or inspection, and (4) the timing for the development of this documentation.

B. Refine the NRR process governing the review and implementation of DI&C retrofits. This process will use a combination of headquarters review, vendor and/or site audit, and site inspection.

DRAFT

Appendix 6
TWG # 6: Licensing Process

C. Develop an inspection module to support the implementation of approved DI&C applications.

D. Develop recommendations for changes to the licensing process and Chapter 7 and/or 13 of the SRP, as necessary, to conform to the outcomes of the other task working groups.

DRAFT

Appendix 6
TWG # 6: Licensing Process

5. MILESTONES, ASSIGNMENTS, AND DELIVERABLES:

TWG #6: Licensing Process					
Milestones, Assignments and Deliverables	**Deliverable**	**Due Date**	**Fcst/Actual**	**Lead**	**Support**
NEAR-TERM					
Develop Interim Staff Guidance without Cyber Security					
Develop preliminary draft ISG		01/30/09	F	NRC	n/a
Discuss preliminary draft ISG with Industry		02/20/09	F	NRC	NEI
Further develop preliminary draft ISG		04/15/09	F	NRC	n/a
Discuss preliminary draft ISG with Industry		04/30/09	F	NRC	NEI
Develop Draft ISG (without cyber security)	√	06/15/09	F	NRC	NEI
Issue Draft ISG (without cyber security)	√	06/30/09	F	NRC	n/a
Discuss Draft Interim Staff Guidance in Public Mtg	√	07/15/09	F	NRC	NEI
Receive Comments		07/30/09	F	NEI	n/a
Issue Final ISG (without cyber security)	√	08/15/09	F	NRC	n/a
Develop Interim Staff Guidance with Cyber Security					
Develop draft ISG with Cyber Security info	√	07/30/09	F	NRC (NSIR)	NEI
Issue draft ISG with Cyber Security info to authorized stakeholders	√	08/15/09	F	NRC	n/a
Discuss ISG in Public Mtg with authorized stakeholders	√	08/30/09	F	NRC	NEI
Receive Comments		09/15/09	F	NEI	n/a
Issue Final ISG with Cyber Security Info to authorized stakeholders	√	09/30/09	F	NRC	n/a

DRAFT

Appendix 6
TWG # 6: Licensing Process

TWG #6: Licensing Process					
Milestones, Assignments and Deliverables	**Deliverable**	**Due Date**	**Fcst/Actual**	**Lead**	**Support**
Other Tasks to Support all Problem Statements					
Develop Draft Inspection Module	√	06/30/08	A	NRC	n/a
Issue Inspection Module	√	10/31/08	A	NRC	n/a
Brief ACRS of Review Process, If Requested		TBD	F	NRC	n/a
LONG-TERM *					
Update ISG to Conform to Other TWG ISGs					
Review Outcomes from Other TWGs and Develop Revisions to DI&C-ISG-06, if Applicable		(1)	-	NRC	NRC
Develop and Issue Revisions to SRP or Other Regulatory Documents					
Develop Draft Revisions to SRP or other regulatory documents	√	10/30/09	F	NRC	n/a
Issue For Public Comment	√	**11/30/09**	F	NRC	n/a
TWG Ends		**11/30/09**	F	NRC	n/a

* Long term actions are those actions necessary to incorporate the ISG's into regulatory infrastructure (Reg. Guides, NUREG's, SRP, etc.). Long term actions are conducted through established agency processes, and are generally outside the control of the TWG's. Dates in bolded text reflect the end of significant TWG activity in completion of a particular action. *Items that are considered outside the scope of TWG activity are in italics.*

(1) The schedule for DI&C-ISG-06 supports the incorporation of the results of other TWGs. Therefore, this item is not needed.

Appendix 7
TWG # 7: Fuel Cycle Facilities

1. BACKGROUND

Historically there has been minimal specific guidance pertinent to the development of the design of control systems that are used as items relied on for safety (IROFS) at fuel cycle facilities. During the licensing process for most of the existing fuel cycle facilities, control systems have been developed and reviewed in a manner that was largely unique to each facility. It is desired by both the NRC and industry to have a consistent set of design requirements for safety control systems that is commensurate with the level of risk to be mitigated by a particular control system relied on for safety. The development of a consistent set of requirements would facilitate the design and the licensing processes for fuel cycle facilities through standardization of appropriate sets of design criteria pertinent to the level of risk to be mitigated, thereby clearly defining expectations for licensees and license reviewers alike.

The design of fuel cycle facilities is increasingly relying on the use of electronic digital systems and components for controlling safety and material safeguards related risks in the following areas:

A. Worker, public and environmental protection
B. Physical protection of items relied on for safety (IROFS) and hazardous materials
C. Nuclear material control and accounting
D. Protection of sensitive information and material

It is largely believed that the application of well-designed digital system technology can result in an improvement in the reliability of control systems. However, the selection of digital system technology for use in safety applications also requires an appropriate assessment of the potential for new modes of control system failures, as well as the risks associated with the occurrence of natural phenomena, electromagnetic or other induced environmental phenomena, human error, hardware/software performance issues and malevolent acts.

Subpart H of 10 CFR 70 implements performance-based requirements for mitigating fuel cycle facility events. It requires that the licensee's safety program shall ensure that each item relied on for safety will be available and reliable to perform its intended function when needed and in the context of the performance requirements stated in the code. The industry advocates the use of a qualitative approach to assessing the reliability of digital control systems used as IROFS rather than a deterministic means of assessing the degree to which a particular reliability goal may have been achieved. Yet, a recent fuel cycle facility event has occurred in which a digital control system, considered qualitatively to be highly reliable, did not continue to perform its intended safety function following restoration of power after an outage, thereby resulting in an unsafe plant condition. It is the goal of this TWG to examine several key issues pertinent to the development of digital control systems in fuel cycle facilities, and develop a set of recommendations for selection and clarification of appropriate design criteria to be used

as interim guidance for addressing those issues until permanent changes to regulatory guides and/or standard review plans can be implemented.

2. SCOPE

The following areas and associated activities will be addressed by TWG #7:

The key design goals stated in 10 CFR Part 70 associated with the use of digital control systems in fuel cycle facilities pertain to the use of such systems in the prevention and/or mitigation of high likelihood, likely, and credible consequence events. Digital control systems used to address such events are designated as items relied on for safety (IROFS), and must be available and reliable to perform their intended functions to mitigate such events. In particular, the design of those IROFS performing criticality control functions must adhere to the double contingency principle. The facility and system design must be based on defense-in-depth practices, and shall contain features that enhance safety by reducing challenges to IROFS.

Key attributes and design features for digital control systems used as IROFS will be considered in order to identify appropriate design criteria that must be met in order to achieve the goals stated above. In particular, goals for digital system security; common cause failure and the level of diversity needed to prevent such failures; independence; channel separation and isolation in highly integrated control stations; and software quality requirements will be examined in light of their potential contribution to enhancing the availability and reliability of IROFS. If, during the conduct of this TWG, it is identified that additional digital control system design criteria (e.g., control system partitioning) may be appropriate to be examined due to their particular application within fuel cycle facilities, they may be added as well. If possible, where it appears that an existing industry standard (or standards) may be appropriate for use in meeting the criteria, they will be considered for use as potential licensee guidance.

In general, the scope of this TWG is to identify appropriate criteria and guidance relating to the availability and reliability requirements for digital control systems designated as IROFS, as stated in the code. To perform this task, the TWG will:

A. Characterize the use of digital control systems and components in terms of their potential contribution to safety and security related risks,
B. Consider controls for managing risk contribution:
    1. Design controls
    2. Configuration controls
    3. Controls for protection of the plant and for reducing challenges to IROFS, and
C. Determine the need for and the approach for reducing risk contribution.

DRAFT

Appendix 7
TWG # 7: Fuel Cycle Facilities

3. PROBLEM STATEMENT

Problem 1 Guidance is needed for reviewing and approving the adequacy of cyber security measures proposed for securing critical digital assets described within license and license amendment applications for fuel cycle facilities.

Problem 2 For Part 70 fuel cycle facilities, guidance is needed to identify an acceptable means of applying adequate diversity [as required in the performance requirements of 10 CFR 70.61 and 70.64 (a)(9)] and defense-in-depth [as stated in the context of 70.64(b)] in the design of digital systems.

Problem 3 Guidance is needed to define "independence" for control system IROFS and to identify an acceptable means of addressing independence or control system channels and functions used to meet the double contingency requirements of 10 CFR 70.64 (a) (9) for criticality safety. Guidance is also needed to clarify the applicability and need for channel independence for digital I&C equipment performing non-criticality related safety actions.

Problem 4 Guidance is needed to identify an acceptable means of addressing the need for isolation, separation, and protection of input signals, logic operations, operator information, and actuation functions of digital I&C systems performing safety-related functions from those performing non-safety functions when they may be sharing common operator interface devices.

Problem 5 Guidance is needed to clarify what is an acceptable means of achieving high quality software used in digital I&C applications used for safety functions within fuel cycle facilities to minimize the occurrence of potential common cause software failures.

4. DELIVERABLES

TWG #7 will develop one ISG document to include the following deliverables:

A. Problem 1: Determine the approach for addressing potential cyber security vulnerabilities for fuel cycle facilities. Evaluate recommendations and guidance being developed by Task Working Group (TWG) #1, Draft DI&C-ISG-01, CYBER SECURITY ASSOCIATED WITH DIGITAL INSTRUMENTATION AND CONTROLS. Interim staff guidance will be adopted or developed, as appropriate. In addition, the effects on Part 70 fuel cycle facilities due to the issuance of proposed rule 10 CFR

73.54, pertaining to the development and implementation of a cyber security program for Part 70 fuel cycle facilities will be evaluated.

B. Problem 2: Review FCSS ISG-04, CLARIFICATION OF BASELINE DESIGN CRITERIA and evaluate recommendations and guidance being developed by Task Working Group (TWG) #2, DI&C-ISG-02, DIVERSITY AND DEFENSE-IN-DEPTH ISSUES to determine if FCSS ISG-04 needs to be updated as needed or if separate interim staff guidance needs to be drafted or adopted.

C. Problem 3: Determine the significance of independence with respect to double contingency requirements in 70.64(a)(9). Evaluate FCSS-ISG-03 NUCLEAR CRITICALITY SAFETY PERFORMANCE REQUIREMENTS AND DOUBLE CONTINGENCY PRINCIPLE and determine if applicable or if there is a need to update this guidance.

D. Problem 4: Evaluate recommendations and guidance being developed by Task Working Group (TWG) #4, DI&C-ISG-04, HIGHLY-INTEGRATED CONTROL ROOMS—COMMUNICATIONS ISSUES (HICRc). Interim Staff Guidance (ISG) developed will be for applicability and pertinence to Part 70 fuel cycle facilities. Interim staff guidance will be adopted or developed, as appropriate. The new guidance will take into account standards which have been developed for evaluation of safety systems used at chemical facilities.

E. Problem 5: Develop a list of appropriate standards for software code validation and verification. The new guidance will take into account standards which have been developed for evaluation of safety systems used at chemical facilities.

DRAFT

Appendix 7
TWG # 7: Fuel Cycle Facilities

5. MILESTONES, ASSIGNMENTS, AND DELIVERABLES:

TWG #7: Fuel Cycle Facilities					
Milestones, Assignments and Deliverables	**Deliverable**	**Due Date**	**Fcst/Actual**	**Lead**	**Support**
NEAR-TERM					
Problem Statement 1: Cyber Security					
Prepare Interim Staff Guidance		11/13/08	A	NRC	n/a
Meet with NSIR Policy Organization for Control of Nuclear Materials		12/15/08	F	NRC	n/a
Issue Draft Interim Staff Guidance	√	02/2009	F	NRC	n/a
Discuss Draft Interim Staff Guidance in Public Meeting		03/2009	F	NRC	NEI
Receive Final Industry Comments	√	03/31/09	F	NRC	NEI
Issue Interim Staff Guidance	√	04/30/09	F	NRC	n/a
Problem Statement 2: Adequate Diversity and Defense-In-Depth					
Prepare Interim Staff Guidance		(1)	-	NRC	n/a
Receive NEI Product (White Paper, Etc.)	√	(1)	-	NEI	n/a
Issue Draft Interim Staff Guidance	√	(1)	-	NRC	n/a
Discuss Draft Interim Staff Guidance in Public Meeting		(1)	-	NRC	NEI
Receive Industry Comments	√	(1)	-	NRC	NEI
Issue Interim Staff Guidance	√	(1)	-	NRC	n/a
Problem Statement 3: Criticality Safety, Independence, and Double Contingency					
Prepare Interim Staff Guidance		04/30/08	A	NRC	n/a
Receive NEI Product (White Paper, Etc.)	√	07/22/08	A	NEI	n/a

DRAFT

Appendix 7
TWG # 7: Fuel Cycle Facilities

TWG #7: Fuel Cycle Facilities					
Milestones, Assignments and Deliverables	**Deliverable**	**Due Date**	**Fcst/Actual**	**Lead**	**Support**
Issue Draft Interim Staff Guidance	√	11/30/08	A	NRC	n/a
Discuss Draft Interim Staff Guidance in Public Meeting		12/10/08	F	NRC	NEI
Receive Final Industry Comments	√	01/15/09	F	NRC	NEI
Issue Interim Staff Guidance	√	04/30/09	F	NRC	n/a
Problem Statement 4: Isolation, Separation, and Protection of Digital I&C Systems					
Prepare Interim Staff Guidance		11/13/08	A	NRC	n/a
Issue Draft Interim Staff Guidance	√	02/2009	F	NRC	n/a
Discuss Draft Interim Staff Guidance in Public Meeting		03/2009	F	NRC	NEI
Receive Final Industry Comments	√	03/31/09	F	NRC	NEI
Issue Interim Staff Guidance	√	04/30/09	F	NRC	n/a
Problem Statement 5: Common Cause Software Failures					
Prepare Interim Staff Guidance		11/13/08	A	NRC	n/a
Issue Draft Interim Staff Guidance	√	02/2009	F	NRC	n/a
Discuss Draft Interim Staff Guidance in Public Meeting		03/2009	F	NRC	NEI
Receive Industry Comments	√	03/31/09	F	NRC	NEI
Issue Interim Staff Guidance	√	04/30/09	F	NRC	n/a

DRAFT

Appendix 7
TWG # 7: Fuel Cycle Facilities

TWG #7: Fuel Cycle Facilities					
Milestones, Assignments and Deliverables	**Deliverable**	**Due Date**	**Fcst/Actual**	**Lead**	**Support**
LONG-TERM *					
Common Long-Term Actions for All Problem Statements					
Develop and Issue Revisions to NUREG 1520					
Develop New NUREG to incorporate ISGs	√	06/30/09	F	NRC	NEI
Publish for Public Comment	√	08/31/09	F	NRC	n/a
Develop Final Revisions to NUREG-1520	√	09/30/09	F	NRC	NEI
Issue for Public Comment	√	**11/30/09**	F	NRC	n/a
TWG Ends		**11/30/09**	F	NRC	n/a

* Long term actions are those actions necessary to incorporate the ISG's into regulatory infrastructure (Reg. Guides, NUREG's, SRP, etc.). Long term actions are conducted through established agency processes, and are generally outside the control of the TWG's. Dates in bolded text reflect the end of significant TWG activity in completion of a particular action.

(1) This issue was determined to be adequately addressed by Problem Statement 3, such that interim staff guidance is not necessary.

DRAFT