DRAFT

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

DRAFT

DIGITAL INSTRUMENTATION AND CONTROLS

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

Interim Staff Guidance

This document presents the technical substance to be incorporated into the final interim staff guidance concerning HICRc. This material may be incorporated into either an appendix or the main body of the guidance document.

TWG4 has determined that HICRc is comprised of four basic considerations:

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

Each of these considerations is addressed separately below. The following sections present considerations and guidelines to be taken into consideration in the design and review of digital systems proposed for safety-related service in nuclear power plants. These guidelines address only the digital aspects of such systems. General requirements such as separation, independence, electrical isolation, and other requirements germane to safety-related systems also apply to digital systems used in safety-related service.

These guidelines are intended to provide clarification and enhanced guidance in recognition of the inherent differences between digital systems that might be used in the future and analog / hardwired systems that have been used in the past and which were tacitly presumed in the development of the existing guidance.

These guidelines do not modify or supersede any existing requirements. These guidelines present means acceptable to the staff for meeting existing requirements. Alternative means of meeting existing requirements may be considered if requested.

The final section of this document addresses modifications to existing guidance documents that result from the adoption of this guidance.

1 INTERDIVISIONAL COMMUNICATIONS

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

Bidirectional communications among safety divisions and between safety and nonsafety equipment is acceptable provided certain restrictions are enforced.

Each safety channel must be protected from undue influence from outside the division of which that channel is a member. In addition, the communication process itself should be carried out by a communications processor separate from the function processor that executes the channel safety function, so that communications errors and malfunctions will not interfere with the operation of the function processor. The communication and function processors should operate asynchronously, sharing information only by means of dual-ported memory or some similar shared resource. Access to the shared memory must be controlled in such a manner that the function processor is never impeded or interrupted when it needs to access the shared memory. For example, if the communication processor is accessing the shared memory at a time when the function processor needs to access it, the function processor must gain immediate access even if that means interfering with the communication process. If the shared memory cannot support unrestricted simultaneous access by both processors, then the access controls must be configured such that the function processor always has precedence.

The following criteria apply to digital communications between redundant safety divisions and between safety and non-safety systems to ensure high-quality <<from Att5 to March8 meeting summary, edited per comments in meeting of June14>>:

a) The safety function processor shall perform no communication handshaking or interrupts that could disrupt deterministic safety function processing.

b) Only predefined data sets shall be processed by the receiving system. Unrecognized data shall be identified and processed by the receiving system in accordance with the defined design requirements. Data from unrecognized messages must not be passed to the safety function processor. Message format and protocol must be pre-determined, with the same sort of information found in the same position in every message.

c) Data exchanged between redundant safety system channels or between safety and nonsafety channels must be processed in a manner that does not adversely affect the safety function of the sending channel, the receiving channel, or any other independent channel.

d) Incoming message data must be stored in fixed predetermined locations in the shared memory and in the memory associated with the function processor. These memory locations must be used for any other purpose. The memory locations shall be allocated such that input data and output data are segregated from each other.

e) Safety division software must be protected from alteration while the safety division is in operation. On-line changes to safety system software must be prevented by hardwired interlocks or by physical disconnection of maintenance/monitoring equipment. The engineer/programmer station must be able to alter the software, addressable constants, setpoints, parameters, and other settings associated with a safety function only when the associated channel(s) are in bypass, and must be physically restricted from connection to more than one channel at a time except that it may receive (not transmit) data from multiple divisions simultaneously by way of communications through the shared memory scheme described elsewhere in this guidance. <<No communication can alter software at all, except as needed from the engineer station, and then only when the division is in bypass. Data communication provisions must also explicitly preclude the ability to send commands to the safety processor. The progress of the safety processor through its software loop must not be altered by any message from outside the channel.>>

f) Provisions for interdivisional communication must explicitly preclude the ability to send commands to a safety processor when the associated channel(s) is performing its safety function. The progress of a safety processor through its software loop must not be affected by any message from outside the channel.

g) A communication fault (e.g., sleeping/frozen interface communications, erroneous data sets, and spurious data sets) shall not prevent performance of required safety functions.

1.1 Vital Communications

(communications necessary for the successful execution of a safety functions)

Vital communications, such as the sharing of channel trip decisions for the purpose of voting, must include provisions for ensuring that received messages are correct and are correctly understood. Such communications should employ error-detecting or error-correcting coding along with means for dealing witn corrupt, invalid, untimely or otherwise questionable data. None of this activity is to be executed in, or affect the operation of, the safety-function processor.

The communications channel must be suitably qualified for the anticipated normal and post-accident environments. For example, some optical fibers and components may be subject to gradual degradation as a result of prolonged exposure to radiation or to heat.

1.2 General Communications

(communications not supporting any safety function)

Communications not vital to the execution of safety functions may nevertheless impact plant safety by introducing the possibility of failures or spurious actuations, or combinations of actuations, that could place the plant in an unusual condition. Coincident events have not traditionally been considered in plant safety analyses because the respective control systems were not typically interconnected. With an integrated system, such coincidence might be a credible result of common-cause events or operating system or other digital system failures. It should be demonstrated that the accident analyses envelope such events.

As a specific example, designers and reviewers should consider the “data storm” event that disabled the recirculation pumps at Browns Ferry and resulted in a reactor trip. This event is described in Information Notice 2007-15 (ML071010303).

2 COMMAND PRIORITIZATION

1
2

2.1 General Considerations

xxx

2.2 Priority Module Own-Division Inputs

xxx

2.3 Priority Module Other-Division and Non-Safety Inputs

- nonsafety commands may be hardwired, would need separation & isolation
- nonsafety commands may enter through nonsafety network port

xxx

2.4 Priority Module Structure

qualification/acceptability of PLD, FPGA, flash memory, other "new" devices – why limit this to command prioritization – should be addressed for all kinds of electronic devices – where is this addressed in current guidance?

This draft guidance enumerates the requirements for a prioritization device/module that is used to prioritize commands from more then one source and passes them on for actuating a safety related component such as a motor actuated valve, a pump motor, a solenoid operated valve etc. This guidance is consistent with the current NRC regulations. The purpose of the draft interim guidance is to clarify the criteria the staff would use in evaluating whether an applicant/licensee meets the requirements for a prioritization device/module when making licensing decisions in the interim until final guidance is developed and promulgated. The staff intends to continue working with stakeholders in refining the guidance and in developing final guidance.

Prioritization device/module is a safety related component and its design shall meet all the requirements that are applicable to a safety device. The prioritization device/component shall be designed to meet all the applicable requirements of IEEE 603-1991.

Safety related commands originating from protection system shall always have the highest priority and shall override all other commands. Failure of a prioritization device/module or loss of power shall place the actuated component in the safe mode i.e. if an isolation valve's safety function is to close then it shall close the valve or if the safety related pump is to be started for safe operation then it shall start the pump. If the operation of the component leads to adverse consequences and the design organization decides that fail-safe mode should not be incorporated then it must assume that the actuated device is not available to perform the safety function or any other function that is executed by the use of the prioritization device/module. In addition, all modes of failure shall be analyzed to determine any adverse consequences

It is assumed that one prioritization device/module will control only a single active component. If an applicant/licensee uses a priority module for more then one component then the design approach outlined in the paragraph above shall apply to all of the actuated components.

The prioritization device/module shall meet the qualification requirements that are applicable to safety related equipment such as environmental, seismic, radiation, electromagnetic and electrostatic qualifications.

The prioritization device/module shall meet the electrical independence requirements of IEEE standard 384 as endorsed in Regulatory Guide 1.75. Communication isolation shall be met per the finalized requirements contained in Requirements and Acceptance Criteria Provisions for Interdivisional Communications (currently under HICRc TWG review and comment stage).

IEEE Standard 7-4.3.2 as endorsed by Regulatory Guide 1.152 shall be applicable to any programmable device used within the safety portion of a prioritization device/module i.e. any programmable device such as processors, programmable logic devices (PLDs), Programmable Gate Arrays, Programmable Logic Controllers (PLCs) or other such devices.

Any software program which is used in any part of the safety portion of the prioritization device/module shall be treated as safety related software. All the requirements that apply to safety related software shall also apply to prioritization device/module. Burnt-in memory shall not be changeable. Field programmable memory shall be considered as software.

Use of any software in any phase of design, production, or testing is subject common-cause failure. To minimize the probability of failures due to common software, the prioritization device/module shall be fully testable. If the tests are generated by any automatic test generation program then all the test sequences and test results shall be manually verified.

Any automatic online testing, if used, shall be automatically overridden if the prioritization device/module receives any actuation command during such testing. Automatic testing shall not inhibit the safety function of the device/module in any way.

The prioritization device/module shall ensure that the completion of a protective action as required by IEEE Standard 603 is not interrupted for any reason.

3 MULTIDIVISIONAL CONTROL AND DISPLAY STATIONS

The HICRc TWG is concerned that independence, isolation, and separation requirements may not be satisfied if multiple safety and nonsafety divisions are permitted to share a single VDU. Use of adequate physical and data isolation provisions, together with the use of dedicated single-division displays and controls, may mitigate these concerns, but such provisions may be problematical from a Human Factors standpoint since they could result in a need for an operator to utilize unfamiliar display and control provisions during an accident. Such an approach could also result in confusion if the nonsafety displays, as a result of lack of qualification and of lesser quality standards, present obsolete or erroneous information to the plant operator but fail to advise the operator of these potential inaccuracies.

ANS 58.8-1994 paragraph 3.3.3 says that safety-related equipment must be controlled ONLY via safety-related controls. Someplace nearby also says that there must be safety-related information feedback to the operator. 58.8 is not endorsed by the NRC, but may be endorsed soon.

3.1 Independence and Isolation

The following provisions are applicable to digital control and display stations. Provisions identified as applicable to display stations also apply to display provisions included in control stations. These provisions do not apply to conventional hardwired control and indicating devices (hand switches, indicating lamps, analog indicators, etc.).

1. **Nonsafety display stations receiving information from one or more safety divisions:**
   All connections to safety-related equipment must be as described in the guidelines for interdivisional communications.
2. **Safety-related display stations receiving information from other divisions (safety or nonsafety):**
   All connections to safety equipment in any division other than the division providing power to the station, and all connections to equipment that is not safety-related, must be as described in the guidelines for interdivisional communications.
3. **Nonsafety control stations controlling the operation of safety-related equipment:**
   Nonsafety control stations may control the operation of safety equipment, provided certain restrictions are enforced:
   - The nonsafety control station must access the safety equipment only by way of the safety-related controls associated with that equipment.
   - The safety-related controls for the subject equipment must include provisions that ensure that the safety-related operational requirements dominate. That is, if the safety system determines that the equipment must be in a certain state, then the equipment must assume that state regardless of what the nonsafety system might be requesting.
   - The safety-related controls << Is there a problem with the use of "controls" here? one might say that these are sometimes protection systems, not control systems, but sometimes they are control systems. >> must be designed so as to preclude the nonsafety control station from influencing the operation of the safety-related controls. This includes:
     - The nonsafety control station must not be able to bypass any safety function.

- The nonsafety control station must not be able to suppress any safety function.
- The nonsafety control station must be able to bring a safety channel out of bypass condition only when that channel has itself determined that such action would be acceptable.

4. **Safety-related control stations influencing the operation of equipment in other divisions:**
   Safety-related control stations influencing the operation of equipment in other divisions are subject to the same constraints described above for nonsafety control stations that influence the operation of safety equipment.
   - The control station must address equipment outside its own division only by way of the controls associated with that equipment.
   - The controls for the subject equipment must include provisions that ensure that the safety-related operational requirements dominate. That is, if the safety system in the equipment's own division determines that the equipment must be in a certain state, then the equipment must assume that state regardless of what the system in the other division might be requesting.
   - The controls for the subject equipment << Is there a problem with the use of "controls" here? one might say that these are sometimes protection systems, not control systems, but sometimes they are control systems. >> must be designed so as to preclude any control station outside the equipment's division from influencing the operation of the controls that are within the equipment's own division. This includes:
     - The extra-divisional control station must not be able to bypass any safety function originating in the equipment's own division.
     - The extra-divisional control station must not be able to suppress any safety function originating in the equipment's own division.
     - The extra-divisional control station must be able to bring a channel in the equipment's own division out of bypass condition only when that channel has itself determined that such action would be acceptable.

3.2 Human Factors Considerations

The advisability of, and any constraints upon the use of, multidivisional control or display stations is clearly an HF consideration and is not addressed herein. The design provisions addressed herein are needed to permit a control or display station to be connected to multiple divisions, regardless of the advisability of such connection from Human Factors standpoint.

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

Depending upon details of how they are implemented, the use of multidivisional VDU could have a positive or negative impact upon D3. Consideration of D3 is outside the scope of the HICRc TWG.

4 DIGITAL SYSTEM NETWORK CONFIGURATION

NOTES:

- address events such as browns Ferry data storm
- address possibility of new accident scenarios due to digital systems – related to BF data storm

This draft interim guidance provides a summary of acceptable methods of complying with the staff's reviews of data communication systems (DCS) and networks. This guidance does not attempt to duplicate the requirements and guidance given in IEEE nuclear power station standards IEEE 603 (Standard Criteria for Safety Systems), IEEE 384 (Criteria for Independence of Class 1E Equipment), IEEE 338 (Criteria for Periodic Surveillance Testing), or IEEE 379 (Application of the Single Failure Criterion). These standards should be consulted directly for criteria for independence, surveillance, and application of the single-failure criterion to a DCS important to safety. Allow the term "network" to be a subset of DCS and is interchangeable with "DCS" as described in the NRC Standard Review Plan (SRP), NUREG and standards. Some extensions or clarifications of these criteria are included later in this document the purpose of the draft interim guidance is to summarize and clarify the methods the staff would use in evaluating whether an applicant/licensee has addressed the issues related to DCS and protocols

The recently revised SRP section 7.9 provides enhanced guidance for reviews of data communications and also references NUREG/CR-6082 "Data Communications." This SRP section addresses both safety and non-safety communication systems. The NUREG discusses data communication technology and the technical rationale for review issues specific to data communication and includes background information to assist the reviewer in identifying critical technical features when reviewing a proposal for a data communication system that is essential or important to the safety of a nuclear reactor.

The SRP does declare that although the primary emphasis is on the equipment comprising the DCS, the reviewer should consider the DCS functions at the system level. The DCS design should be compatible with the design of the supported systems as described in the process system chapters of the SAR and their functions and performance as assumed in the SAR Chapter 15 design bases accident analyses. It is not sufficient to evaluate the adequacy of the DCS only on the basis of the design's meeting the specific requirements of IEEE Std. 279-1971 or IEEE Std. 603-1991.

Networks proposed for use, whether standard or proprietary, should be analyzed for hazards and performance deficits posed by unneeded functionality and complication. The possible use of a proprietary network is a departure from the IEC 61500 standard which states that data transmission systems should follow an internationally agreed format and protocol.

Use of a standard network is not a guarantee of suitability. The specification of distributed systems is a far more difficult task than specifying sequential single-thread systems. Computer communication protocols are one form of a distributed system. Standard networks exist whose specifications have not been validated by formal techniques and which may contain specification errors.

The recent ORNL draft report states that network links can be point-to-point (i.e., two nodes) or bus media (i.e., more than two nodes). Point-to-point links, which can be designed to operate very simply, are the preferred link for communications related to safety systems interconnection. Bus media operation is more complex having issues of media access contention, node addressing, and traffic congestion in addition to failure modes, fault propagation, and common cause failures due to the shared bus. The bus media's complexity requires a more complex design and testing effort.

In summary, this being a baseline for the summarization of reviews involving networks and DCSs, there is near sufficient criteria for reviews of data communication technology. The staff intends to continue working with stakeholders in refining the guidance and in developing the final guidance

APPENDIX:

HICRc PRIORITY LIST CROSS-REFERENCE

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

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