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

Revision ED

SCOPE

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

This guidance specifically addresses issues related to interactions among safety divisions and between safety-related equipment and equipment that is not safety-related. This guidance is not applicable to interactions among entities that are all in the same safety division or that do not involve anything that is safety-related. This guidance does address certain aspects of digital control systems that are not safety-related but that are able to affect transient initiation, progression, or initial conditions.

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

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

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

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

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

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

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

ORGANIZATION

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

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

Considerations 1 through 3 are each addressed in a separate section below. Consideration 4 has implications concerning each of the first three and is incorporated into those section as needed.

~~Each of these considerations is addressed in a separate section, below. These 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.~~

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

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 or guidance. These guidelines present means acceptable to the staff for meeting existing requirements. Alternative means of meeting existing requirements may be considered if requested and adequately documented and justified.

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

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

1 INTERDIVISIONAL COMMUNICATIONS

BACKGROUND

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

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

~~A fundamental guiding principle is that the safety system and the associated software must be as simple as possible. The safety function processor must be dedicated to the safety function, with as little additional functionality as possible. For example, cross-channel verification must be carried out by processors outside the safety-related system.~~

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

~~For systems which do not involve communications among safety divisions and in which communications between a safety division and a nonsafety entity either do not exist or satisfy the simple one-directional communications concept described above, including conformance to all items indicated as "should," adherence to the remainder of this section is not necessary.~~

CRITERIA

1. A safety channel must not be dependent upon any information from outside its own safety division to accomplish its safety function. This is a fundamental consequence of the independence requirements of IEEE603. It is recognized that division voting logic must receive inputs from multiple safety divisions.
2. The safety function of each safety channel must be protected from adverse influence from outside the division of which that channel is a member. This protection must be sustained despite external equipment malfunction and despite software error or corruption, including errors or corruption that affect multiple channels/divisions. ~~This protection must be implemented without the use of software.~~

3. A safety channel should not receive any communication from outside its own safety division unless that communication ~~that does not~~ supports or enhances the performance of the ~~its own~~ safety function. Receipt of such information would involve functions that are not directly related to the safety function. ~~, and which would therefore not be in accordance with the "simplicity" principle.~~ Receipt of such information and performance of such functions ~~would need to~~ should be justified. It ~~would need to~~ should be demonstrated that the added system/software complexity does not increase the likelihood of software specification or coding errors, including errors which would affect more than one division.

4. The communication process itself ~~must~~should be carried out by a communications processor[2] separate from the processor that executes the ~~channel~~ safety function, so that communications errors and malfunctions will not interfere with the execution of the safety function. ~~operation of the function processor.~~ The communication and function processors ~~must~~should operate asynchronously, sharing information only by means of dual-ported memory or other ~~some similar~~ shared but separately allocated memory resource. The function processor, the communications processor, and the shared memory, along with all supporting circuits and software, are all considered to be safety-related, and must be designed, qualified, fabricated, etc. accordingly. Access to the shared memory ~~must~~should be controlled in such a manner that the function processor has priority access to the shared memory to complete the safety function in a deterministic manner. For example, if the communication processor is accessing the shared memory at a time when the function processor needs to access it, the function processor ~~must~~should gain access within the allotted timeframe so as not to impact the loop cycle time ~~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~~ should be configured such that the function processor always has precedence. If the function processor does not have priority access to the shared memory, then the safety function circuits and program logic must ensure that the safety function will be performed within the established timeframe and without the data from the shared memory.

5. The ~~limiting~~ cycle time for the safety function~~s~~ processor ~~must~~should be determined in consideration of the longest possible completion time for each access to the shared memory. This longest-possible completion time ~~must~~should include the response time of the memory itself and of the circuits associated with it, and ~~must~~should also include the longest possible delay in access to the memory by the function processor assuming worst-case conditions for the transfer of access from the communications processor to the function processor. Failure of the system to meet the limiting cycle time ~~must~~should be detected and alarmed.

6. The safety function processor ~~must~~should perform no communication handshaking and ~~must~~should not accept interrupts from outside its own safety division.

7. Only predefined data sets may be used by the receiving system. Unrecognized messages and data ~~must~~should be identified and ~~processed~~ dispositioned by the receiving system in accordance with the prespecified design requirements. Data from unrecognized messages must not be used within the safety logic executed by the safety function processor. Message format and protocol ~~must~~should be pre-determined. Every message ~~must~~should have the same message field structure and sequence, ~~with~~ including message identification, status information, data bits, etc. in the same relative locations in every message. Every datum ~~must~~should be included in every transmit cycle, whether it has changed since the previous transmission or not, to ensure deterministic system behavior.

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

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

9. Incoming message data ~~must~~should be stored in fixed predetermined locations in the shared memory and in the memory associated with the function processor. These memory locations ~~must~~should not be used for any other purpose. The memory locations ~~must~~should be allocated such that input data and output data are segregated from each other in separate memory devices or in separate prespecified physical areas within a memory device.

10. Safety division software ~~must~~should be protected from alteration while the safety division is in operation. On-line changes to safety system software ~~must~~should be prevented by hardwired interlocks or by physical disconnection of maintenance/monitoring equipment. A workstation (e.g. engineer/programmer station) may alter ~~the software, ~~addressable constants, setpoints, parameters, and other settings associated with a safety function only by way of the dual-processor / shared-memory scheme described in this guidance, or when the associated channel is inoperable. Such a workstation ~~, and must~~should be physically restricted from making changes in more than one division at a time. The restriction should be by means of ~~(such as via~~ physical cable disconnect, or by means of ~~via~~ keylock switch that either physically opens the data transmission circuit or interrupts the connection by means of hardwired logic. Provisions that rely on software are acceptable only if it is shown that software errors, system malfunctions, and software specification errors cannot prevent or diminish the disabling of the connection. Software-based interlocks using common software would be subject to common-cause failures which could compromise diversity and priority and are therefore not acceptable.~~) 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 one-way communications through the shared memory scheme described above.~~

11. Provisions for interdivisional communication ~~must~~should explicitly preclude the ability to send software instructions directly to a safety function processor when that processor is operable. ~~performing its safety function. ~~The progress of a safety function processor through its instruction sequence ~~software loop must~~should not be affected by any message from outside the divisions. For example, the received messages ~~must~~should not direct the processor to execute a subroutine or branch to a new instruction sequence.

~~12.Communication errors, corrupted messages, etc. must be handled exclusively within the nonsafety system without the participation of the safety system.~~

~~13.~~12. Communication faults must not adversely affect the performance of required safety functions in any way. Although the single-failure criterion indicates that such failures should be presumed to originate in only one safety channel at a time, there is no such restriction on assumed faults for nonsafety channels. Examples of credible communications faults include, but are not limited to, the following:

- Messages may be corrupted due to errors in communications processors, errors introduced in buffer interfaces, errors introduced in the transmission media, or from interference or electrical noise.
- Messages may be repeated at an incorrect point in time.
- Messages may be sent in the incorrect sequence.
- Messages may be lost, which includes both failures to receive an uncorrupted message or to acknowledge receipt of a message.
- Messages may be delayed beyond their permitted arrival time window, including errors in the transmission medium, congested transmission lines, interference, or by delay in sending buffered messages.

- Messages may be inserted into the communication medium, from unexpected or unknown sources.
- Messages may be sent to the wrong destination, which could treat the message as a valid message.
- Messages may be longer than the receiving buffer, resulting in buffer overflow and memory corruption.
- Messages may contain data that is outside the expected range.
- Messages may appear valid, but data may be placed in incorrect locations within the message.
- Messages may occur at a high rate that degrades or causes the system to fail (i.e., broadcast storm).
- message IP headers or addresses may be corrupted.

13. Vital communications, such as the sharing of channel trip decisions for the purpose of voting, ~~must~~should include provisions for ensuring that received messages are correct and are correctly understood. Such communications should employ error-detecting or error-correcting coding along with means for dealing with corrupt, invalid, untimely or otherwise questionable data. The effectiveness of error detection/correction should be demonstrated in the design and proof testing of the associated codes, but once demonstrated is not subject to periodic testing. Error-correcting methods, if used, should be shown to always reconstruct the original message exactly or to designate the message as unrecoverable. None of this activity is to ~~be executed in, or~~ affect the operation of~~,~~ the safety-function processor.
14. ~~–~~Vital communications ~~must~~should be point-to-point by means of a dedicated medium (copper or optical cable). In this context, “point-to-point” means that the message is passed directly from the sending node to the receiving node without going through any other node and without the participation of any additional medium or equipment.
15. Network communication for safety functions should be deterministic. A deterministic communication system is a communication system that communicates a fixed set of data (called the "state") at regular intervals, whether data in the set has changed or not.
16. Safety, liveness, and real-time properties required by the safety application should be verified in the protocol. Liveness, in particular, is taken to mean that no connection to another network can cause an RPS/ESFAS communication protocol to stall, either deadlock or livelock. (Note: This is also required by the independence criteria of GDC 24 and IEEE 603-1991 IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations. (Source NUREG/CR-6082, 3.4.3)
~~15.~~17. The medium used in a vital communications channel must be qualified for the anticipated normal and post-accident environments. For example, some optical fibers and components may be subject to gradual degradation as a result of prolonged exposure to radiation or to heat. In addition, new digital systems may require susceptibility testing for EMI/RFI and power surges, if the environments are significant to the equipment being qualified.
18. Provisions for communications should be analyzed for hazards and performance deficits posed by unneeded functionality and complication.

19. If data rates exceed the capacity of a communications link or the ability of nodes to handle traffic, the system will suffer congestion. All links and nodes should have sufficient capacity to support all functions. The applicant should identify the true data rate, including overhead, to ensure that communication bandwidth is sufficient to ensure proper performance of all safety functions. Communications throughput thresholds and safety system sensitivity to communications throughput issues should be confirmed by testing.
20. The safety system response time calculations should include an assumed data error rate that is consistent with the communications system reliability and which bounds the actual anticipated data error rate under all conditions.

2 COMMAND PRIORITIZATION

BACKGROUND

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

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

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

~~Software implementation of priority modules not associated with diverse actuation would seem to violate both the simplicity principle and the criterion concerning avoidance of communications not important to safety (both presented in the section on interdivisional communications). Use of such modules must be justified in the light of those provisions.~~

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

CRITERIA

1. A priority module is a safety related device or software function, and it must meet all requirements (design, qualification, quality, etc.) applicable to safety-related devices or software.
2. Priority modules used for diverse actuation signals must be ~~physical modules~~ independent of the remainder of the digital system, and must function properly regardless of the state or condition of the digital system.

3. Safety-related commands that direct a component to a safe state (as opposed to commands originating in a safety-related channel but which only cancel or enable cancellation of the safe-state command and have no intrinsic safety function), and that originate~~ing from~~ in protection system~~s~~ sense and command features, must always have the highest priority and must override all other commands. ~~Failure of a priority module must place each actuated component in the safe state predetermined for that component. If the operation of the component would lead to adverse consequences and the design organization decides that fail-safe mode should not be incorporated, then it must be assumed that the actuated device is not available to perform the safety function or any other function that is passed through the priority module. It must also be assumed that the actuated component(s) may be in a state of operation contrary to safety. In addition, all modes of failure must be analyzed to determine any adverse consequences.~~ It ~~must~~should be shown that the unavailability or spurious operation of the actuated device is included in the plant safety analysis.
4. A priority module may control one or more components. If a priority module controls more then one component, then all of these provisions apply to each of the actuated components.
5. Communication isolation for each priority module ~~must~~should be as described in the guidance for interdivisional communications.
6. Software used in the design, ~~program execution,~~ testing, maintenance, etc. of a priority module is subject to all of the applicable ~~requirements~~ guidance in ~~of~~ Regulatory Guide 1.152, which partially endorses IEEE Standard 7-4.3.2. This includes software applicable to any programmable device used in support of the safety function ~~within the safety portion~~ of a prioritization module, such as processors, programmable logic devices (PLDs), Programmable Gate Arrays, Programmable Logic Controllers (PLCs) or other such devices. Section 5.3.2 is particularly applicable to this subject. If the device is 100% tested (that is, every possible combination of inputs and every possible sequence of device states is tested, and all outputs are verified for every case), then the requirements for validation of the design tools is reduced.
7. Any software program which is used in support of the safety function within a ~~any part of the safety portion of the~~ priority module must be treated as safety related software. All the requirements that apply to safety related software also apply to prioritization module. Burned-in memory ~~must~~should ~~not~~ be changeable only through removal and replacement of the memory device. Design provisions should ensure that static memory and programmable logic cannot be altered while installed in the module. The contents and configuration of field programmable memory ~~must~~should be considered to be software, and ~~must~~should be developed, maintained, and controlled accordingly.

8. To minimize the probability of failures due to common software, the priority module design ~~must~~should be fully tested (This refers to proof-of-design testing, not to individual testing of each module and not to surveillance testing.). If the tests are generated by any automatic test generation program then all the test sequences and test results ~~must~~should be manually verified. Testing should include the application of every possible combination of inputs and the evaluation of all of the outputs that result from each combination of inputs. If a module includes state-based logic (that is, if the response to a particular set of inputs depends upon past conditions), then all possible sequences of input sets should also be tested. If testing of all possible sequences of input sets is not considered practical by an applicant, then the applicant ~~must~~should identify the testing that is excluded and justify that exclusion. The applicant ~~must~~should show that the testing planned or performed provides adequate assurance of proper operation under all conditions and sequences of conditions. Note that it is possible that logic devices within the priority module include unused inputs: assuming those inputs are forced by the module circuitry to a particular known state, those inputs can be excluded from the "all possible combinations" criterion. For example, a priority module may include logic executed in a gate array that has more inputs than are necessary. The unused inputs should be forced to either "TRUE" or "FALSE" and then can be ignored in the "all possible combinations" testing.
9. ~~Any automatic online testing, if used, must be automatically overridden if the priority module receives any actuation command during such testing.~~ Automatic testing (including failure of automatic testing features) must not inhibit the safety function of the module in any way. Failure of automatic testing software would constitute common-cause failure if were to result in the disabling of the module safety function.
10. The priority module must ensure that the completion of a protective action as required by IEEE Standard 603 is not interrupted by commands, conditions, or failures outside the module's own safety division. ~~for any reason.~~

3 MULTIDIVISIONAL CONTROL AND DISPLAY STATIONS

BACKGROUND

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

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

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

CRITERIA

3.1 Independence and Isolation

Multidivisional control and display stations ~~must~~should permit control/modification of equipment in only one safety division at a time.

> Need further consideration: Operator should be able to issue one ctmt isolation command or one SI command (for example) and have it activate all divisions. Should also only need to issue one command to actuate a valve with solenoids in different divisions. But don't want failures, errors, spurious events, etc. to affect multiple divisions.

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

1. **Nonsafety stations receiving information from one or more safety divisions:** All communications with safety-related equipment ~~must~~should be as described in the guidelines for interdivisional communications.

2. **Safety-related stations receiving information from other divisions (safety or nonsafety):**
All communications with equipment outside the station's own safety division, whether that equipment is safety-related or not, ~~including communications with equipment that is not safety-related, must~~should be as described in the guidelines for interdivisional communications. No information received from other divisions (or from nonsafety sources) may have any influence upon a channel's trip decision. This protection from influence must be implemented within the safety division of the receiving system, must not itself be influenced by any condition or information from outside the division, and must protect the safety function regardless of any operation, malfunction, design error, software error, or communication error outside the division.

3. **Nonsafety stations influencing the operation of safety-related equipment:**
Nonsafety stations may influence the operation of safety-related equipment, provided the following restrictions are enforced:
   - The nonsafety station ~~must~~should access safety-related plant equipment only by way of a priority module associated with that equipment. Priority modules ~~must~~should be in accordance with the guidance on priority modules.
   - A nonsafety station must not influence the operation of safety-related controls when the safety-related controls are performing their safety function. This provision must be implemented within the safety-related system, and must be unaffected by any operation, malfunction, design error, software error, or communication error in the nonsafety equipment. In addition:
     - The nonsafety station must ~~not~~ be able to bypass a~~ny~~ safety function only when the affected division ~~unless that function's own safety system~~ has itself determined that such action would be acceptable.
     - The nonsafety station must not be able to suppress any safety function.
     - The nonsafety station ~~must~~should be able to bring a safety function out of bypass condition only when ~~that function's own safety system~~ the affected division has itself determined that such action would be acceptable.

4. **Safety-related stations influencing the operation of equipment in other safety-related divisions:**
Safety-related stations influencing the operation of equipment in other divisions are subject to constraints similar to those described above for nonsafety stations that influence the operation of safety-related equipment.
   - A control station ~~must~~should access safety-related plant equipment outside its own division only by way of a priority module associated with that equipment. Priority modules ~~must~~should be in accordance with the guidance on priority modules.
   - A station must not influence the operation of safety-related controls outside its own division when those controls are performing their safety function. This provision must be implemented within the affected (target) safety-related controls, and must be unaffected by any operation, malfunction, design error, software error, or communication error outside the division of which those controls are a member. In addition:
     - The extra-divisional (that is, "outside the division") control station must ~~not~~ be able to bypass a~~ny~~ safety function only when the affected division ~~unless that function's own safety system has~~ itself determined that such action would be acceptable.
     - The extra-divisional station must not be able to suppress any safety function.

- The extra-divisional station ~~must~~should be able to bring a safety function out of bypass condition only when ~~that function's own safety system~~ the affected division has itself determined that such action would be acceptable.

5. Malfunctions and Spurious Actuations:

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

- ~~No single unit of software shall generate commands to multiple c~~Control processors that are assumed to malfunction independently ~~by~~ in the safety analysis should not be affected by common software.
- No single control action (e.g., mouse click or screen touch) ~~shall~~ can generate commands to multiple control processors that are assumed to malfunction independently by the safety analysis. Additional confirmatory command should be added (e.g. do you want to proceed followed by a "Yes" and a "No" choice) for all safety functions and other important ~~critical~~ functions. (The second operation as described here is to provide protection from spurious actuations, not protection from operator error. Protection from operator error may involve similar but more restrictive provisions, as addressed in guidance related to Human Factors.)
- Each control processor or its associated communication processor ~~shall~~ should detect and block commands from the shared resources that do not pass the communication error checks.
- Multidivisional control and display stations ~~must~~should be qualified withstand the effects of adverse environments, seismic conditions, EMI/RFI, power surges, and all other design basis conditions applicable to safety-related equipment at the same plant location. This qualification need not demonstrate complete functionality during or after the qualification event unless the station is safety-related. Stations which are not safety-related should be shown to produce no spurious actuations and to have no adverse effect upon any safety-related equipment or device as a result of a qualification event both during the event and afterwards. For example, a nonsafety station should not cause the spurious operation or stoppage of any safety-related or nonsafety device during the event, and should not fail in such a manner as to do so after the event spontaneously or as a result of a misinterpreted operator action. If spurious or abnormal actuations or stoppages are possible as a result of a qualification event, then the plant safety analyses must envelope those spurious and abnormal actuations and stoppages.
- Loss of power, power surges, power interruption, and any other credible event to any operator workstation or controller ~~must~~should not result in spurious actuation or stoppage of any plant device or system unless that spurious actuation or stoppage is enveloped in the plant safety analyses.
- The design ~~must~~should have provision for an "operator workstation ~~shutdown~~disable" switch to be activated upon abandonment of the main control room, to preclude spurious actuations that might otherwise occur as a result of the condition causing the abandonment (such as control room fire or flooding). The means of disabling control room operator stations should be immune to hot shorts, environmental conditions in the control room, etc. that might restore functionality to the control room operator stations and result in spurious actuations.

- Processors ~~must~~should be configured and functionally distributed so that processor malfunction or software error will not result in ~~as to preclude~~ spurious actuations that are not enveloped in the plant design bases, accident analyses, ATWS provisions, or other provisions for abnormal conditions. This includes spurious actuation of more than one plant device or system. as a result of processor malfunction or software error.
- Failure or malfunction of any operator workstation must not result in a plant condition (including simultaneous conditions) that is not enveloped in the plant design bases, accident analyses, and anticipated transients without scram (ATWS) provisions, or in other unanticipated abnormal plant conditions
- Multiple spurious actuations due to failure or malfunction of one or more operator workstations ~~must~~should not be possible, or the impact of such multiple spurious actuations must be analyzed and shown to be acceptable under all plant conditions

3.2 Human Factors Considerations

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

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

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

There are many other Human Factors considerations applicable to the design of operator workstations, whether multidivisional or not. Such considerations are not addressed here. Guidance concerning general Human Factors considerations is provided separately.

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

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

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

4DIGITAL SYSTEM NETWORK CONFIGURATION

NOTES:

- address events such as browns Ferry data storm
- Sensor signals, actuation signals, and other signals critical to safety functions must not be multiplexed or exchanged over network resources. – need exception & constraints for distribution of trip/actuation signals to voting logic (w/ fail safe reception on receiving end?)?
- all vital communications must be point-to-point over dedicated media – xref communications section?
- need to define "the network" & how far it goes – ultimately connects to internet through layers of firewalls, switches, routers, etc. – what is needed to protect the safety function?

The following text is provided as a list of points to be taken into consideration in the development of the interim staff guidance on network configuration. It is not intended to be used as guidance in its own right. This text will be deleted and replaced with guidance in a later revision of this document.

There are general considerations as well as specific considerations to be addressed for network configurations. Due to the limited number of network designs reviewed and actual systems important to safety or safety related systems in operation to date, the guidance is predominately spawned from research in data network communications and good engineering review practice that should be used to ensure overall quality, reliability and comprehensibility of the network. The guidance becomes a comprehensive inventory of general and specific attributes which the network design should encompass.

4.1General Considerations

The specification of a network configuration that is essential or important to the safety of a nuclear reactor is a far more difficult task than specifying sequential single-thread systems of a safety system.

Use of a standard network is not a guarantee of suitability. Standard networks exist whose specifications have not been validated by formal techniques and which may contain specification errors. Networks proposed for use, whether standard or proprietary, should be analyzed for hazards and performance deficits posed by unneeded functionality and complication.

~~Proprietary media and protocols may have the disadvantages of having less reported experience in the literature and little or no theoretical support in the literature for performance and reliability. There also may be logistic considerations, which affect safety because of insufficient material support and inability to correct design faults discovered later.~~

~~The network may be proprietary or standard networks. In either case the network must be fully tested to ensure compliance with the network specification. Communication protocol must also be fully tested to ensure compliance with the specification.~~

~~Communication interconnections among safety divisions or between safety and nonsafety divisions must satisfy the guidance provided in interdivisional communications.~~

~~Cyber security, a key consideration in selection of networks and associated protocols, is addressed in the Cyber Security TWG guidance.~~

~~4.2Specific Considerations~~

~~The following are some of the specific attributes to be considered in the review, and design of, network configurations. This is not a complete listing nor supersedes good engineering practices or recommendations important to safety of the system such as separation, independence, electrical isolation and other requirements germane to safety related systems:~~

~~4.2.1Point-to-point or bus media~~

~~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.~~

~~4.2.2Data rates~~

~~If data rates exceed link capability or the ability of nodes to handle traffic, the system will suffer congestion. A node should have sufficient computational capacity left after handling communication traffic to perform its other functions. If a system vendor cannot answer this question, it may be a sign that the vendor has not considered the application very carefully.~~

~~Network communication data transfer rate or bandwidth must have sufficient capacity such that the cycle time is met under the worst case of data communication load. The data transfer rate load must consider not only the data but the overheads as well.~~

~~Communication with other networks or nodes must not lead to data overload or data storm that can potentially either slowdown the communication or disable the network communication.~~

~~4.2.3Message Mix~~

~~Data rates are usually specified in bulk bytes (or bits) per second. This does not include overhead (extra bits) incurred by various communication schemes, which is usually added to each message. If the message mix consists mainly of short messages, the bulk data rate supported by the links and nodes may not give a true picture of how the system will perform.~~

~~4.2.4Media Requirements~~

~~Each of these should be addressed for consideration:~~

- ~~Noise immunity~~
- ~~Physical robustness~~
- ~~Connectivity within and outside the network~~
- ~~Bandwidth should address data collisions & potential system wide lockups~~
- ~~Communication error handling~~

~~4.2.5Reliability~~

~~Assuring reliability of data transmission involves error detection and correction, or some means of requesting retransmission. It is a truism that communication media are always faulty. The conventional measure of quality is the number of failed bits per bits transmitted. This has the useful feature of being a dimensionless figure of merit that can be compared across any speed or type of communication media.~~

~~Network communications systems detect errors by transmitting a summary of the data with the data. In TCP (the internet's Transmission Control Protocol), the sum of the data bytes of packet is sent in each packet's header. Simple arithmetic sums do not detect out-of-order data, or cancelling errors. A bit-wise binary polynomial, a cyclic redundancy check, can detect these errors and more, but is slightly more expensive to calculate.~~

~~The network communication error rate must be tested and documented. Bit error rate should be as low as can be reasonably achieved.~~

~~Online data communication error detection and error handling schemes must be employed. If error correction is proposed to be implemented sufficient information will be provided to staff to prove that the error correction scheme will not recreate data which differs from the original data.~~

~~4.2.6Effectiveness~~

~~Needs to be specified in such a way, that engineers, designers, and in some cases software developers can implement and/or use it. In human-machine systems, its design needs to facilitate routine usage by humans. *Protocol layering* accomplishes these objectives by dividing the protocol design into a number of smaller parts, each of which performs closely related sub-tasks, and interacts with other layers of the protocol only in a small number of well-defined ways.~~

~~4.2.7Other Protocol considerations~~

~~Safety, liveness, and real-time properties required by the safety application should be verified in the protocol. Liveness, in particular, is taken to mean that no connection to another network can cause an RPS/ESFAS communication protocol to stall, either deadlock or livelock.~~

~~Network communication must be deterministic in nature.~~
~~(Notes: State based communication system should be used. If an event based or another system is proposed then the applicant must provide sufficient information to support that the communication accuracy and speed will not be impaired under the most adverse conditions. State-based communication system is a communication system that communicates a fixed set of data (called the "state") at regular intervals, whether data in the set has changed or not. State-based communication systems have more predictable performance under upset conditions than event-based systems, at the expense of less-efficient use of communications bandwidth.)~~

~~Safety, liveness, and real-time properties required by the safety application should be verified in the protocol. Liveness, in particular, is taken to mean that no connection to another network can cause an RPS/ESFAS communication protocol to stall, either deadlock or livelock. (Note: This is also required by the independence criteria of GDC 24 and IEEE 603-1991 IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations. (Source NUREG/CR-6082, 3.4.3)~~

APPENDIX:

HICRc PRIORITY LIST CROSS-REFERENCE

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

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