DIGITAL INSTRUMENTATION AND CONTROLS

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

Interim Staff Guidance

Revision H~~F~~ (note: change markings are relative to Rev. F)

SCOPE

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

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

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

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

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

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

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

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

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

ORGANIZATION

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

1. interdivisional communications: communications among different safety 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 should also satisfy the guidance provided for interdivisional communications)

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

[1] IEEE 603-1991 (cited in 10CFR50.55a(h)) provides the following definitions:

> *channel: "An arrangement of components and modules as required to generate a single protective action signal when required by a generating station condition. A channel loses its identity where single protective action signals are combined."*
>
> *division: "The designation applied to a given system or set of components that enables the establishment and maintenance of physical, electrical, and functional independence from other redundant sets of components."*

For the purposes of this guidance document, the terms *channel* and *division* are further described below. Note that the following is for illustrative purposes, and is not intended to impose requirements or new interpretations:

> 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 within a single division.
>
> 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 typically credits redundancy among divisions. ~~credit can be taken only for redundancy among, not within, divisions.~~ The voting logic that generates the final actuation signal to an item of plant equipment typically resides in one division and receives input from redundant channels in all divisions.

1 INTERDIVISIONAL COMMUNICATIONS

BACKGROUND

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

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

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

CRITERIA

1. A safety channel must not be dependent upon any information or resource 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. Information and signals originating outside the division must not be able to inhibit or delay the safety function. This protection must be implemented within the affected division (rather than in the sources outside the division), and must not itself be affected by any condition or information from outside the affected division. This protection ~~, and ~~must be sustained despite any operation, malfunction, design error, communication error, or software error or corruption existing or originating outside the division.~~, including errors or corruption that affect multiple channels/divisions.~~

3. A safety channel should not receive any communication from outside its own safety division unless that communication supports or enhances the performance of the safety function. Receipt of information that does not support or enhance the safety function would involve the performance of functions that are not directly related to the safety function. Safety systems should be as simple as possible. Functions which are not necessary for safety, even if they enhance reliability, should be done outside the safety system. Functions not directly related to the safety function would add complexity to the system, and could therefore increase the likelihood of failures and software errors and should be avoided within the safety system. For example, comparison of readings from sensors in different divisions may provide useful information concerning the behavior of the sensors (for example, On-Line Monitoring), however this could also involve unacceptable influence of one division over another, or could involve functions not directly related to the safety functions, and should then not be executed within the safety system. Receipt of ~~such~~ information from outside the division, and the performance of functions not directly related to the safety function, if used, ~~information and performance of such functions should~~ must be justified. It should be demonstrated that the added system/software complexity associated with the performance of functions not directly related to the safety function and with the receipt of information in support of those functions does not significantly increase the likelihood of software specification or coding errors, including errors which would affect more than one division. The applicant must justify the definition of “significantly” used in the demonstration.

4. The communication process itself should be carried out by a communications processor[2] separate from the processor that executes the safety function, so that communications errors and malfunctions will not interfere with the execution of the safety function. The communication and function processors should operate asynchronously, sharing information only by means of dual-ported memory or other shared ~~but separately allocated~~ memory resource that is dedicated exclusively to this exchange of information. The function processor, the communications processor, and the shared memory, along with all supporting circuits and software, are all considered to be safety-related, and must be designed, qualified, fabricated, etc. accordingly. Access to the shared memory should be controlled in such a manner that the function processor has priority access to the shared memory to complete the safety function in a deterministic manner. For example, if the communication processor is accessing the shared memory at a time when the function processor needs to access it, the function processor should gain access within the allotted timeframe so as not to impact the loop cycle time. If the shared memory cannot support unrestricted simultaneous access by both processors, then the access controls should be configured such that the function processor always has precedence. ~~If the function processor does not have priority access to the shared memory, then the~~ 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 in the event that the function processor is unable to gain access to the shared memory.

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

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

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

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

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

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

10. Safety division software should be protected from alteration while the safety division is in operation. On-line changes to safety system software should be prevented by hardwired interlocks or by physical disconnection of maintenance/monitoring equipment. A workstation (e.g. engineer/programmer station) may alter addressable constants, setpoints, parameters, and other settings associated with a safety function only by way of the dual-processor / shared-memory scheme described in this guidance, or when the associated channel is inoperable. Such a workstation must be physically restricted from making changes in more than one division at a time. The restriction should be by means of physical cable disconnect, or by means of keylock switch that either physically opens the data transmission circuit or interrupts the connection by means of hardwired logic. “Hardwired logic” as used here refers to circuitry that physically interrupts the flow of information, such as an electronic AND gate circuit (that does not use software or firmware) with one input controlled by the hardware switch and the other connected to the information source: the information appears at the output of the gate only when the switch is in a position that applies a “TRUE” or “1” at the input to which it is connected. Provisions that rely on software to effect the disconnection are not acceptable. It is noted that software may be used in the safety system and/or in the workstation to accommodate the effects of the open circuit or for status logging or other purposes.

11. Provisions for interdivisional communication should explicitly preclude the ability to send software instructions ~~directly~~ to a safety function processor unless all safety functions associated with that processor are either bypassed or otherwise not in service. ~~when that processor is operable.~~ The progress of a safety function processor through its instruction sequence should not be affected by any message from outside its division. ~~the divisions.~~ For example, ~~the~~ a received message~~s~~ should not be able to direct the processor to execute a subroutine or branch to a new instruction sequence.

12. Communication faults must not adversely affect the performance of required safety functions in any way. Although the single-failure criterion indicates that such failures should be presumed to originate in only one safety channel at a time, there is no such restriction on assumed faults for nonsafety channels. Examples of credible communications faults include, but are not limited to, the following:
    - Messages may be corrupted due to errors in communications processors, errors introduced in buffer interfaces, errors introduced in the transmission media, or from interference or electrical noise.
    - Messages may be repeated at an incorrect point in time.
    - Messages may be sent in the incorrect sequence.
    - Messages may be lost, which includes both failures to receive an uncorrupted message or to acknowledge receipt of a message.
    - Messages may be delayed beyond their permitted arrival time window, including errors in the transmission medium, congested transmission lines, interference, or by delay in sending buffered messages.
    - Messages may be inserted into the communication medium, from unexpected or unknown sources.
    - Messages may be sent to the wrong destination, which could treat the message as a valid message.
    - Messages may be longer than the receiving buffer, resulting in buffer overflow and memory corruption.
    - Messages may contain data that is outside the expected range.
    - Messages may appear valid, but data may be placed in incorrect locations within the message.
    - Messages may occur at a high rate that degrades or causes the system to fail (i.e., broadcast storm).
    - message ~~IP~~ headers or addresses may be corrupted.

13. Vital[3] communications, such as the sharing of channel trip decisions for the purpose of voting, should include provisions for ensuring that received messages are correct and are correctly understood. Such communications should employ error-detecting or error-correcting coding along with means for dealing with corrupt, invalid, untimely or otherwise questionable data. The effectiveness of error detection/correction should be demonstrated in the design and proof testing of the associated codes, but once demonstrated is not subject to periodic testing. Error-correcting methods, if used, should be shown to always reconstruct the original message exactly or to designate the message as unrecoverable. None of this activity is to affect the operation of the safety-function processor.

14. Vital[3] communications should be point-to-point by means of a dedicated medium (copper or optical cable). In this context, "point-to-point" means that the message is passed directly from the sending node to the receiving node without the involvement of equipment outside the division of the sending or receiving node. Implementation of other communication strategies should provide the same reliability and must be justified.

[3] "Vital" communications as used herein are communications that are needed to support a safety function. Failure of vital communications could inhibit the performance of the safety function. The most common implementation of vital communications is the distribution of channel trip information to other divisions for the purpose of voting.

15. ~~Network c~~Communication for safety functions should communicate a fixed set of data (called the "state") at regular intervals, whether data in the set has changed or not.

16. ~~Safety~~Network connectivity, 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~~ any network outside the division can cause an RPS/ESFAS communication protocol to stall, either deadlock or livelock. (Note: This is also required by the independence criteria of GDC 24 and IEEE 603-1991 IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations.) (Source: NUREG/CR-6082, 3.4.3)

17. The medium used in a vital[3] communications channel must be qualified for the anticipated normal and post-accident environments. For example, some optical fibers and components may be subject to gradual degradation as a result of prolonged exposure to radiation or to heat. In addition, new digital systems may require susceptibility testing for EMI/RFI and power surges, if the environments are significant to the equipment being qualified.

18. Provisions for communications should be analyzed for hazards and performance deficits posed by unneeded functionality and complication.

19. If data rates exceed the capacity of a communications link or the ability of nodes to handle traffic, the system will suffer congestion. All links and nodes should have sufficient capacity to support all functions. The applicant should identify the true data rate, including overhead, to ensure that communication bandwidth is sufficient to ensure proper performance of all safety functions. Communications throughput thresholds and safety system sensitivity to communications throughput issues should be confirmed by testing.

20. The safety system response time calculations should assume a data error rate that is greater than or equal to the design basis error rate and is supported by the error rate observed in design and qualification testing.

2 COMMAND PRIORITIZATION

BACKGROUND

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

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

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

Software implementation of priority modules not associated with diverse actuation would result in the availability of two kinds of priority modules, one type suitable for diverse actuation and one type not suitable for diverse actuation. An applicant should demonstrate that there are adequate configuration control measures in place to ensure that software-based priority modules that might be subject to CCF will not be used later for credited diversity, either deliberately or accidentally (for example, there is protection from design error and from maintenance / implementation error). This applies both to existing diversity provisions and to diversity provisions that might be credited later. The applicant ~~should~~ must 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~~ A priority module must meet all requirements (design, qualification, quality, etc.) applicable to safety-related devices or software.
2. Priority modules used for diverse actuation signals must be independent of the remainder of the digital system, and must function properly regardless of the state or condition of the digital system.

3. Safety-related commands that direct a component to a safe state ~~(as opposed to commands originating in a safety-related channel but which only cancel or enable cancellation of the safe-state command and have no intrinsic safety function), and that originate in protection system sense and command features, ~~must always have the highest priority and must override all other commands. Commands that originate in a safety-related channel but which only cancel or enable cancellation of the effect of the safe-state command (that is, a consequence of a Common-Cause Failure in the primary system that erroneously forces the plant equipment to a state that is different from the designated “safe state.”), and which do not directly support any safety function, have lower priority and may be overridden by other commands. In some cases, such as a containment isolation valve in an auxiliary feedwater line, there is no universal “safe state:” the valve must be open under some circumstances and closed under others. The relative priority to be applied to commands from a diverse actuation system, for example, is not obvious in such a case. This is a system operation issue, and priorities must be assigned on the basis of considerations relating to plant system design or other criteria unrelated to the use of digital systems. This issue is outside the scope of this ISG. The reasoning behind the proposed priority ranking should be explained in detail. The reviewer should refer the proposed priority ranking and the explanation to appropriate systems experts for review. The priority module itself must be shown to apply the required priority ranking correctly and should meet all other applicable guidance. It should be shown that the unavailability or spurious operation of the actuated device is included in or bounded by the plant safety analysis.

4. A priority module may control one or more components. If a priority module controls more than one component, then all of these provisions apply to each of the actuated components.

5. Communication isolation for each priority module should be as described in the guidance for interdivisional communications.

6. Software used in the design, testing, maintenance, etc. of a priority module is subject to all of the applicable guidance in Regulatory Guide 1.152, which partially endorses IEEE Standard 7-4.3.2-2003. This includes software applicable to any programmable device used in support of the safety function of a prioritization module, such as~~ processors~~, programmable logic devices (PLDs), programmable gate arrays, ~~Programmable Logic Controllers (PLCs) ~~or other such devices. Section 5.3.2 of IEEE 7-4.3.2-2003 is particularly applicable to this subject. Validation of design tools used for programming a priority module or a component of a priority module is not required if the device directly affected by those tools ~~If the device ~~is 100% tested before being released for service. 100% testing means that ~~(that is, ~~every possible combination of inputs and every possible sequence of device states is tested, and all outputs are verified for every case. The testing should not involve the use of the design tool itself.~~), then validation of the design tools is not required.~~ Software-based prioritization must meet all requirements (quality requirements, V&V, documentation, etc.) applicable to safety-related software.

7. Any software program which is used in support of the safety function within a priority module ~~must be treated as ~~is safety-related software. All requirements that apply to safety-related software also apply to prioritization module software. ~~Burned-in~~Nonvolatile memory (such as burned-in or reprogrammable gate arrays or random-access memory) should be changeable only through removal and replacement of the memory device. Design provisions should ensure that static memory and programmable logic cannot be altered while installed in the module. The contents and configuration of field programmable memory should be considered to be software, and should be developed, maintained, and controlled accordingly.

8. To minimize the probability of failures due to common software, the priority module design should be fully tested (This refers to proof-of-design testing, not to individual testing of each module and not to surveillance testing.). If the tests are generated by any automatic test generation program then all the test sequences and test results should be manually verified. Testing should include the application of every possible combination of inputs and the evaluation of all of the outputs that result from each combination of inputs. If a module includes state-based logic (that is, if the response to a particular set of inputs depends upon past conditions), then all possible sequences of input sets should also be tested. If testing of all possible sequences of input sets is not considered practical by an applicant, then the applicant should identify the testing that is excluded and justify that exclusion. The applicant should show that the testing planned or performed provides adequate assurance of proper operation under all conditions and sequences of conditions. Note that it is possible that logic devices within the priority module include unused inputs: assuming those inputs are forced by the module circuitry to a particular known state, those inputs can be excluded from the "all possible combinations" criterion. For example, a priority module may include logic executed in a gate array that has more inputs than are necessary. The unused inputs should be forced to either "TRUE" or "FALSE" and then can be ignored in the "all possible combinations" testing.

9. Automatic testing within a priority module, whether initiated from within the module or triggered from outside, and ~~(~~including failure of automatic testing features,~~)~~ must not inhibit the safety function of the module in any way. Failure of automatic testing software ~~would~~ could constitute common-cause failure if it were to result in the disabling of the module safety function.

10. The priority module must ensure that the completion of a protective action as required by IEEE Standard 603 is not interrupted by commands, conditions, or failures outside the module's own safety division.

3 MULTIDIVISIONAL CONTROL AND DISPLAY STATIONS

BACKGROUND

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

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

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

CRITERIA

3.1 Independence and Isolation

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

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

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

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

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

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

DRAFT

5. Malfunctions and Spurious Actuations:

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

- Control processors that are assumed to malfunction independently in the safety analysis should not be affected by failure of a multidivisional control and display station.~~ common software~~.
- Control functions that are assumed to malfunction independently in the safety analysis should not be affected by failure of a single control processor.
- Safety and control processors should be configured and functionally distributed so that a single processor malfunction or software error will not result in spurious actuations that are not enveloped in the plant design bases, accident analyses, ATWS provisions, or other provisions for abnormal conditions. This includes spurious actuation of more than one plant device or system as a result of processor malfunction or software error. The possibility and consequences of malfunction of multiple processors as a result of common software error must be addressed.
- No single control action (for example, mouse click or screen touch) should generate commands to plant equipment. Two positive operator actions should be required to generate a command. ~~, f~~For example:~~,~~ When the operator requests any safety function or other important function, the system should respond “do you want to proceed?” The operator should then be required to respond ~~followed by a~~ “Yes” or “No” to cause the system to execute the function. Other question-and-confirm strategies may be used in place of the one described in the example. ~~choice, for all safety functions and other important functions. (~~The second operation as described here is to provide protection from spurious actuations, not protection from operator error. Protection from operator error may involve similar but more restrictive provisions, as addressed in guidance related to Human Factors.~~)~~
- Each control processor or its associated communication processor should detect and block commands ~~from the shared resources~~ that do not pass the communication error checks.
- Multidivisional control and display stations should be qualified to withstand the effects of adverse environments, seismic conditions, EMI/RFI, power surges, and all other design basis conditions applicable to safety-related equipment at the same plant location. This qualification need not demonstrate complete functionality during or after the application of the design basis condition unless the station is safety-related. Stations which are not safety-related should be shown to produce no spurious actuations and to have no adverse effect upon any safety-related equipment or device as a result of a design basis condition, both during the condition and afterwards. ~~For example, a nonsafety station should not cause the spurious operation or stoppage of any safety-related or nonsafety device during the condition, and should not fail in such a manner as to do so after the condition spontaneously or as a result of a misinterpreted operator action.~~ If spurious or abnormal actuations or stoppages are possible as a result of a design basis condition, then the plant safety analyses must envelope those spurious and abnormal actuations and stoppages. Qualification should be supported by testing rather than by analysis alone. D3 considerations may impose additional qualification ~~considerations~~ criteria or requirements in addition to those described herein.

- Loss of power, power surges, power interruption, and any other credible event to any operator workstation or controller should not result in spurious actuation or stoppage of any plant device or system unless that spurious actuation or stoppage is enveloped in the plant safety analyses.
- The design should have provision for an "operator workstation disable" switch to be activated upon abandonment of the main control room, to preclude spurious actuations that might otherwise occur as a result of the condition causing the abandonment (such as control room fire or flooding). The means of disabling control room operator stations should be immune to short-circuits, environmental conditions in the control room, etc. that might restore functionality to the control room operator stations and result in spurious actuations.
- ~~Processors should be configured and functionally distributed so that processor malfunction or software error will not result in spurious actuations that are not enveloped in the plant design bases, accident analyses, ATWS provisions, or other provisions for abnormal conditions. This includes spurious actuation of more than one plant device or system as a result of processor malfunction or software error.~~
- Failure or malfunction of any operator workstation must not result in a plant condition (including simultaneous conditions) that is not enveloped in the plant design bases, accident analyses, and anticipated transients without scram (ATWS) provisions, or in other unanticipated abnormal plant conditions

3.2 Human Factors Considerations

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

- as required by IEEE 603
- as recommended in Regulatory Guide 1.97~~ or required in connection with the TMI accident~~
- as referenced in:
  - ➢ plant safety or transient analyses
  - ➢ emergency or normal operation procedures
  - ➢ D3 or ATWS analyses
  - ➢ other design basis analyses
- as suggested in the plant control and display "minimum inventory" interim staff guidelines
- ~~as indicated in other requirements or analyses.~~

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

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

IEEE603-1991, Section 5.6.3.1, specifies that equipment "… that is used for both safety and nonsafety functions shall be classified as part of the safety systems…" Therefore equipment that is NOT classified as part of a safety system must NOT be used in support of safety functions. Therefore multidivisional control and display stations must not be used to provide safety functions under circumstances when those safety functions are needed to support plant safety. When safety functions are required, the control and monitoring of those functions and of the equipment that performs them must be by way of safety-related resources.

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. In addition, the presence on the nonsafety workstations of controls and displays that are associated with safety functions could lead an operator to erroneously select those nonsafety controls and displays, rather than the safety-related ones, when the safety functions are required.

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

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

Additional ~~G~~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.

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

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

Additional ~~G~~guidance concerning D3 considerations is provided separately.

APPENDIX:

HICRc PRIORITY LIST CROSS-REFERENCE

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

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