U.S.NRC

UNITED STATES NUCLEAR REGULATORY COMMISSION

Protecting People and the Environment

DIGITAL INSTRUMENTATION AND CONTROLS

DI&C-ISG-04

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

Interim Staff Guidance

Revision 0
(Initial Issue for Use)

DIGITAL INSTRUMENTATION AND CONTROLS

DI&C-ISG-04

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

Interim Staff Guidance

Revision 0
(Initial Issue for Use)

IMPLEMENTATION

Except in those cases in which a licensee proposes or has previously established an acceptable alternative method for complying with specified portions of the NRC's regulations, the NRC staff will use the methods described in this Interim Staff Guidance (ISG) to evaluate licensee compliance with NRC requirements as presented in submittals in connection with applications for standard plant design certifications and combined licenses.

This ISG provides acceptable methods for addressing HICRc in digital I&C system designs. This guidance is consistent with current Commission policy on digital I&C systems and is not intended to be a substitute for NRC regulations, but to clarify how a licensee or applicant may satisfy those regulations.

This ISG also clarifies the criteria the staff will use to evaluate whether an applicant/licensee digital system design is consistent with HICRc guidelines. The staff intends to continue interacting with stakeholders to refine digital I&C ISGs and to update associate guidance and generate new guidance where appropriate.

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 requirements germane to safety-related systems, such as requirements for separation, independence, electrical isolation, seismic qualification, quality requirements, etc. cited in the General Design Criteria of Appendix A to Part 50 of Title 10 of the Code of Federal Regulations. Additional guidance applicable to such systems is also provided in various other NRC and industry documents.

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 equipment 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 document presents guidance and also references requirements. In the interest of maintaining simplicity and focus upon the technical considerations, a distinction is not always clearly drawn between "guidance" and "requirements." In some cases, requirements are

described using the language of recommendations (for example, “should” rather than “must”). The reader is cautioned that this document does not alter any existing requirements, and that it is the responsibility of the applicant to ensure that all requirements are satisfied regardless of how they may be presented or addressed herein.

DEFINITION

The term "Highly-Integrated Control Room" (HICR) refers to a control room in which the traditional control panels, with their assorted gauges, indicating lights, control switches, annunciators, etc., are replaced by computer-driven consolidated operator interfaces. In an HICR:

- The primary means for providing information to the plant operator is by way of computer-driven display screens mounted on consoles or on the control room walls.
- The primary means for the operator to command the plant is by way of touch screens, keyboards, pointing devices or other computer-based provisions.

A digital workstation is in essence just one device. Unlike a conventional control panel, there is no way for its many functions to be independent of or separated from one another, because they all use the same display screen, processing equipment, operator interface devices, etc. Functions that must be independent must be implemented in independent workstations.

This ISG describes how controls and indications from all safety divisions can be combined into a single integrated workstation while maintaining separation, isolation, and independence among redundant channels. This ISG does not alter existing requirements for safety-related controls and displays to support manual execution of safety functions.

ORGANIZATION

Task Working Group (TWG) 4 has determined that HICRc is comprised of four basic areas of interest:

1. interdivisional communications: communications among different safety divisions[i] 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.

RATIONALE

In order to prepare this interim staff guidance, the Staff primarily relied upon:

(1) 10 C.F.R. §50.55a(h), which invokes IEEE 603-1991; and

(2) Regulatory Guide 1.152, which endorses IEEE 7-4.3.2-2003 (with comments).

IEEE 603-1991 requires, among other things, independence among redundant safety channels and redundant safety systems to be independent of one another. IEEE 7-4.3.2-2003 addresses digital communications (NOTE: Some provisions or IEEE 7-4.3.2 have been found to not be suitable for endorsement by the NRC. In addition, IEEE7-4.3.2 is currently undergoing revision and the final version may or may not be found to be suitable for endorsement and may or may not be consistent with the guidance provided herein).

The guidance provided herein adheres to the principles set forth in IEEE 603-1991 and IEEE 7-4.3.2-2003 by describing means for ensuring independence among redundant safety channels while permitting some degree of interconnection and commonality among those independent channels.

REFERENCES

1. 10 C.F.R. § 50.55a(h)
   U.S. Code of Federal Regulations, Part 50.55, “Conditions of construction permits,” Title 10, “Energy.” Washington, DC: U.S. Government Printing Office.
2. Regulatory Guide 1.152
   NRC (2006). “Criteria for Digital Computers in Safety Systems of Nuclear Power Plants.” Washington, D.C.: U.S. Nuclear Regulatory Commission.
3. IEEE 603-1991
   Institute of Electrical and Electronics Engineers (1991). “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations -Description.” New York: Institute of Electrical and Electronics Engineers.
4. IEEE 7-4.3.2-2003
   Institute of Electrical and Electronics Engineers (2003). “IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations.” New York: Institute of Electrical and Electronics Engineers.

1. INTERDIVISIONAL COMMUNICATIONS

SCOPE

As used in this document, interdivisional communications includes transmission of data and information among components in different electrical safety divisions and communications between a safety division and equipment that is not safety-related. It does not include communications within a single division. Interdivisional communications may be bidirectional or unidirectional.

STAFF POSITION

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 nonsafety equipment should adhere to the guidance 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 involve a review of selected software code.

1. A safety channel should not be dependent upon any information or resource originating or residing 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 should 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 must be sustained despite any operation, malfunction, design error, communication error, or software error or corruption existing or originating outside the division.
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 that are not necessary for safety, even if they enhance reliability, should be executed outside the safety system. A safety system designed to perform functions not directly related to the safety function would be more complex than a system that performs the same safety function, but is not designed to perform other functions. The more complex system would increase the likelihood of failures and software errors. Such a complex design, therefore, 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). Such a function executed within a safety system, however, could also result in unacceptable influence of one division over another, or could involve functions not directly related to the safety functions, and should not be executed within the safety system. Receipt of information from outside the division, and the performance of functions not

directly related to the safety function, if used, should 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 that would affect more than one division. The applicant should justify the definition of "significantly" used in the demonstration.

4. The communication process itself should be carried out by a communications processor[ii] 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 some other shared 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., in accordance with 10 C.F.R. Part 50, Appendix A and B. 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 a timeframe that does not impact the loop cycle time assumed in the plant safety analyses. 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. The safety function circuits and program logic should ensure that the safety function will be performed within the timeframe established in the safety analysis, and will be completed successfully without 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.
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 should be used by the receiving system. Unrecognized messages and data should be identified and dispositioned by the receiving system in accordance with the pre-specified 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 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 should 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 pre-specified 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 and monitoring equipment. A workstation (e.g. engineer or 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 should 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 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 to a safety function processor unless all safety functions associated with that processor are either bypassed or otherwise not in service. The progress of a safety function processor through its instruction sequence should not be affected by any message from outside its division. For example, a received message should not be able to direct the processor to execute a subroutine or branch to a new instruction sequence.
12. Communication faults should not adversely affect the performance of required safety functions in any way. Faults, including communication faults, originating in nonsafety equipment, do not constitute "single failures" as described in the single failure criterion of 10 C.F.R. Part 50, Appendix A. Examples of credible communication 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 for several reasons, 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 headers or addresses may be corrupted.

13. Vital[iii] 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 should affect the operation of the safety-function processor.
14. Vital[iii] 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 should be justified.
15. 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. Network connectivity, liveness, and real-time properties essential to the safety application should be verified in the protocol. Liveness, in particular, is taken to mean that no connection to 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: (1) 10 C.F.R. Part 50, Appendix A, General Design Criteria ("GDC") 24, which states, "interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired."; and (2) IEEE 603-1991 IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations.) (Source: NUREG/CR-6082, 3.4.3)
17. Pursuant to 10 C.F.R. § 50.49, the medium used in a vital[iii] communications channel should 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 need 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

SCOPE

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.

STAFF POSITION

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

1. A priority module is a safety related device or software function. A priority module must meet all of the 10 C.F.R. Part 50, Appendix A and B requirements (design, qualification, quality, etc.) applicable to safety-related devices or software.
2. Priority modules used for diverse actuation signals should be independent of the remainder of the digital system, and should function properly regardless of the state or condition of the digital system. If these recommendations are not satisfied, the applicant should show how the diverse actuation requirements are met.
3. Safety-related commands that direct a component to a safe state 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 should 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 should be shown to apply the commands correctly in order of their priority rankings, and should meet all other applicable guidance. It should be shown that the unavailability or spurious operation of the actuated device is accounted for 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 endorses IEEE Standard 7-4.3.2-2003 (with comments). This includes software applicable to any programmable device used in support of the safety function of a prioritization module, such as programmable logic devices (PLDs), programmable gate arrays, 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 necessary if the device directly affected by those tools is 100% tested before being released for service. 100% testing means that 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. Software-based prioritization must meet all requirements (quality requirements, V&V, documentation, etc.) applicable to safety-related software.
7. Any software program that is used in support of the safety function within a priority module is safety-related software. All requirements that apply to safety-related software also apply to prioritization module software. 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, should not inhibit

the safety function of the module in any way. Failure of automatic testing software 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

SCOPE

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.

NOTE: As used in connection with control and display stations, "control" refers to control provisions available to the plant operator by way of those stations. Such controls provide the plant operator with means to, for example, instruct the control system to open or close some valve. Control of safety-related plant devices in the sense of the process of generating and transmitting safety-related control signals must be accomplished by means of safety-related control equipment in the same safety division as that plant equipment. In some cases, a command originating from a control and display station outside the division may be superseded by a higher-priority command. The manner of combining the commands from control stations outside a safety division with the safety commands originating within the division is addressed below. This guidance explicitly DOES NOT endorse the exclusive or direct control of safety-related plant equipment by means of provisions outside the equipment's own safety division.

STAFF POSITION

3.1 Independence and Isolation

The following provisions are applicable to multidivisional control and display stations. These guidance 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 conform to 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 conform to the guidelines for interdivisional communications. Note that the guidelines for interdivisional communications refer to provisions relating to the nature and limitations concerning such communications, as well as guidelines relating to the communications process itself.

3. **Nonsafety stations controlling the operation of safety-related equipment:**
Nonsafety stations may control (see note above) 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 designed and applied as described in the guidance on priority modules.
   - A nonsafety station should not affect the operation of safety-related equipment when the safety-related equipment is performing its safety function. This provision should 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 should be able to bypass a safety function only when the affected division has itself determined that such action would be acceptable.
     - The nonsafety station should 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 needed 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 unless the affected division has itself determined that such action would be acceptable.

4. **Safety-related stations controlling the operation of equipment in other safety-related divisions:**
Safety-related stations controlling (see note above) the operation of equipment in other divisions are subject to constraints similar to those described above for nonsafety stations that 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 designed and applied as described in 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 should be implemented within the affected (target) safety-related system, and should 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 should be able to bypass a safety function only when the affected division itself determined that such action would be acceptable.
     - The extra-divisional station should 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 needed 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 unless the affected division has itself determined that such action would be acceptable.

5. Malfunctions and Spurious Actuations:

The result of malfunctions of control system resources (e.g., workstations, application servers, protection/control processors) shared between systems must be consistent with the assumptions made in the safety analysis of the plant. Design and review criteria for complying with these requirements, as set forth in 10 C.F.R. § 50.34 and 50.59, 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..
- 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. 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 “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. 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 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. 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 warrant the inclusion of additional qualification criteria or measures 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.
- 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
- 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

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 perform functions needed to support plant safety. The control and monitoring of functions credited with the protection of the plant in the plant safety analyses must be performed utilizing 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, are consistent with the system design bases, operating procedures, and accident analyses and are 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 guidance concerning 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 measures 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 guidance concerning D3 considerations is provided separately.

---

[i] 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. 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. For the purposes of this guidance, it is to be assumed that each of the actuation signals entering the voting logic that establishes the final actuation signal to an item of plant equipment is in a different division, regardless of the particular usage of the term "division" for a particular nuclear power plant.

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

[iii] "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.

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)