

DIGITAL I&C TASK WORKING GROUP

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

Outline of Guidance and Acceptance Criteria

This guidance is intended to supplement the applicable portions of the Standard Review Plan pertaining to communications independence among digital systems.

This guidance specifically addresses the technical and regulatory considerations associated with the implementation of the subject provisions, without regard to the associated Human Factors or Cyber-Security considerations. HF and CS are addressed separately by TWG commissioned specifically to address those considerations. Some of the considerations addressed herein may mitigate some CS concerns.

This guidance document addresses all communications (any transmittal or reception of data, information, or commands) and controls (anything which can affect the operation of a safety channel in any way, including both effects involving safety functions and effects involving functions not related to safety) which involve any digital safety channel¹ and anything outside the electrical division¹ of which that safety channel is a member. . For example, the following are within the scope of this guidance:

1. communication among redundant electrical divisions
2. communication between any safety channel and anything external to that channel's electrical division
3. control of safety equipment from a workstation in a different electrical safety division
4. control of safety equipment from a nonsafety workstation
5. commingling of safety and nonsafety controls or indications on a single workstation
6. connection and operation of programming, maintenance, and test equipment

The following are explicitly excluded from the scope of this guidance:

7. communication within a single safety division, even if physically dispersed
8. communication which do not involve a safety channel
9. cyber-security
10. Diversity and Defense-in-Depth (D3) considerations
11. Human Factors (HF) considerations

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

1

PROVISIONS FOR CROSS-DIVISIONAL COMMUNICATIONS

from SRP App 7.1D

5.6 Independence (IEEE Std 7-4.3.2-2003 Clause 5.6)

Consistent with the requirements of IEEE Std 603-1991, data communication between safety channels or between safety and non-safety systems should not inhibit the performance of the safety function. Additional guidance on physical, electrical, and communication independence is provided in SRP Appendix 7.1-C Subsection 5.6.

IEEE Std 603-1991 requires that safety functions be separated from non-safety functions such that the non-safety functions cannot prevent the safety system from performing its intended functions. In digital systems, software performing both safety and non-safety functions may reside on the same computer and use the same computer resources. However, IEEE Std 603-1991, Sub-Clause 5.6.3.1 also requires that equipment that is used for both safety and non-safety functions shall be classified as part of the safety system. The term "equipment" includes both software and hardware of the digital systems. For this reason, any software providing non-safety functions that resides on a computer providing a safety function must be classified as a part of the safety system. If an applicant/licensee desires that a non-safety function be performed by a safety computer, the software to perform that function must be classified as safety-related, with all the attendant regulatory requirements for safety software, including communications isolation from other non-safety software.

In some instances, vendors or applicants/licensees may wish to implement systems having some communication between the safety systems and non-safety systems. GDC 24, "Separation of protection and control systems," requires that the protection system be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system, and that interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired.

In practical terms, this means that for communications between safety and non-safety systems, the communications must be such that the safety system does not require any non-safety input to perform its safety function, and that any failure of the non-safety system, communications system, or data transmitted by the non-safety system will not prevent or influence that independent safety determination. The portion of the safety software which actually performs the safety function, i.e., determining whether or not to trip based on sensor inputs, should not receive input or influence from any non-safety system while the safety system is on-line and performing that safety function.

The following provides some of the possible design approaches that a reviewer may encounter for data communications. It is neither exhaustive nor limiting in the possible approaches. If the reviewer is not sufficiently familiar with the communications systems and methods being used, the reviewer should seek the assistance of other NRC personnel and/or supervisor for the appropriate review strategy to determine that the communications can not interfere with the safety function.

- A communications system which broadcasts data from the safety system to the non-safety system without the use of handshaking and acknowledgment signals would satisfy these requirements.
- If the communications system allows two way communications between the safety and non-safety systems, the determination may require more detailed examination of the communications method, including memory allocation methods, communications protocols and message formatting methodology.

One possibility may be to determine that the communications method is deterministic, that is, the same information is transmitted in the same way to the safety system, and is then used by the safety system in the same manner. This could be done by having the nonsafety system write data to a specific location in shared memory, and the safety system would read that data. The safety system would know what the data means and what to do with the data because the data in that memory location would be the latest written value of the same data. There would have to be

appropriate provisions for out-of-date data, garbled data, and communications link failure. This is, of course, one, but not the only possible method of deterministic communications.

The objective in the review is to determine that the applicant/licensee has satisfactorily demonstrated that the applicable requirements of 10 CFR 50.55a(h) and GDC-24 are met.

Additional guidance on communications independence is provided in SRP Appendix 7.0-A, SRP Appendix 7.1-C, and SRP Section 7.9.

As used in this document, cross-divisional 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. Cross-divisional communications may be bidirectional or unidirectional. Bidirectional communications should be assumed in the following discussions, unless indicated otherwise.

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

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

The following criteria apply to digital communications between redundant safety divisions and between safety and non-safety systems to ensure high-quality <<from Att5 to March8 meeting summary>>:

- a) The safety system shall perform no communication handshaking or interrupts that could disrupt deterministic safety function processing.
- b) Only predefined data sets shall be processed by the receiving system. Unrecognized data shall be identified and processed by the receiving system in accordance with the defined design requirements (e.g., the message format and protocol is pre-determined, that is, the same information is found in each section of every message).
- c) Data exchanged between redundant safety system channels shall be processed in a manner that does not adversely affect the safety function of other independent channels.
- d) The receipt and storage of the data is pre-determined, stored in the same memory locations each time, and these memory locations are not used for any other purpose. The memory locations shall be allocated such that input data and output data are segregated from each other.
- e) Data communication shall not alter safety system software while the safety system's channel is in operation (e.g., hardwired interlocks that prevent on-line changes to safety system software).

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

1. xxx:
xxx

1.1 Basic Communications

general information exchange not vital to any safety function

1.2 Vital Communications

information exchange such as in support of voting logic, where successful communication is essential to the successful completion of the safety function

1.3 Priority Modules

modules located downstream of the voting logic, to provide for alternative access to safety-related equipment when the safety system is in a "don't care" state.

2 MULTIDIVISIONAL CONTROL AND DISPLAY STATIONS

from SRP App 7.1D

5.8 Information Displays (IEEE Std 7-4.3.2-2003 Clause 5.8)

In the past, information displays only provided a display function, and therefore required no two-way communications. More modern display systems may also have included control functions, and therefore the reviewer should ensure that incorrect functioning of the information displays does not prevent the safety function from being performed when necessary. This is the same issue as in subsection 5.6, "Independence", and similar methods are appropriate. If the communications path is one-way from the safety system to the displays, or if the displays and controls are qualified as safety related, the safety determination is simplified. Two-way communications with non-safety control systems have the same isolation issues as any other non-safety to safety communications. In addition, however, the reviewer should ensure that inadvertent actions, such as an unintended touch on a touch sensitive display can not prevent the safety function.

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

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

1. Nonsafety display stations receiving information from one or more safety divisions:

All connections to safety-related equipment must be as described herein.

2. Safety-related display stations receiving information from other divisions:

All connections to safety equipment in any division other than the division providing power to the station, and all connections to equipment that is not safety-related, must be as described herein.

3. Nonsafety control stations controlling the operation of safety-related equipment:

Nonsafety control stations may control the operation of safety equipment, provided certain restrictions are enforced:

- The nonsafety control station must address the safety equipment only by way of the safety-related controls associated with that equipment.
- The safety-related controls for the subject equipment must include provisions that ensure that the safety-related operational requirements dominate. That is, if the safety system determines that the equipment must be in a certain state, then the equipment must assume that state regardless of what the nonsafety system might be requesting.
- The safety-related controls [« Is there a problem with the use of "controls" here? one might say that these are sometimes protection systems, not control systems, but sometimes they are control systems. »](#) must be designed so as to preclude the nonsafety control station from influencing the operation of the safety-related controls. This includes:
 - The nonsafety control station must not be able to bypass any safety function.
 - The nonsafety control station must not be able to suppress any safety function.
 - The nonsafety control station must be able to bring a safety channel out of bypass condition only when that channel has itself determined that such action would be acceptable.

4. Safety-related control stations influencing the operation of equipment in other divisions:

Safety-related control stations influencing the operation of equipment in other divisions are subject to the same constraints as described above for nonsafety control stations that influence the operation of safety equipment.

- The control station must address equipment outside its own division only by way of the controls associated with that equipment.
- The controls for the subject equipment must include provisions that ensure that the local safety-related operational requirements dominate. That is, if the safety system in the equipment's own division determines that the equipment must be in a certain state, then the equipment must assume that state regardless of what the system in the other division might be requesting.
- The controls for the subject equipment [« Is there a problem with the use of "controls" here? one might say that these are sometimes protection systems, not control systems, but sometimes they are control systems. »](#) must be designed so as to preclude any control station outside the equipment's division from influencing the operation of the controls that are within the equipment's own division. This includes:
 - The extra-divisional control station must not be able to bypass any safety function originating in the equipment's own division.
 - The extra-divisional control station must not be able to suppress any safety function originating in the equipment's own division.

DRAFT

- The extra-divisional control station must be able to bring a channel in the equipment's own division out of bypass condition only when that channel has itself determined that such action would be acceptable.