

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 Section 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 nonsafety 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 nonsafety functions that resides on a computer providing a safety function must be classified as a part of the safety system. If a licensee desires that a nonsafety 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 nonsafety software.

In some instances, vendors or 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 nonsafety 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 nonsafety system, communications system or data transmitted by the nonsafety 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 nonsafety 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 nonsafety 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 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.

DRAFT

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 section 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 nonsafety 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.

DRAFT