

DRAFT

12/11/2006

White Paper

Communication Between Redundant Safety Divisions and Between Safety and Non-Safety Systems

Summary

This white paper discusses current requirements for communications between redundant safety divisions and between safety and non-safety systems; describes examples of precedence; identifies potential changes to requirements in IEEE Standard 7-4.3.2-2003; and provides input to the current effort by the NRC to revise the Standard Review Plan (NUREG-0800). With digital I&C technology, judicious communication between redundant safety divisions and between safety and non-safety systems can provide reliability and safety enhancements that were not achievable when currently-operating plants were designed, using the analog technology of the day. Advanced plant designs include varying degrees of communications between redundant safety divisions and between safety and non-safety systems to validate signals and ensure high reliability. To enable nuclear plants to capture these benefits, NRC-approved guidance is needed to establish clear requirements and acceptance criteria whereby such communications can be designed and utilized, while maintaining reasonable assurance that they will not degrade safety functions through unintended behaviors or failure modes. This white paper was initially drafted by the NEI Digital Instrumentation Task Force to serve as a discussion vehicle with the NRC staff. It is anticipated that it will be revised as discussions proceed and will represent a combined industry / NRC roadmap for resolving outstanding issues related to communication between redundant safety divisions and between safety and non-safety systems.

Background

Section 5.6 of IEEE Std. 603-1998, "Criteria for Safety Systems for Nuclear Power Generating Stations," contains requirements for independence. Section 5.6 of IEEE Std. 603-1998 includes requirements for the following:

- Independence between redundant portions of a safety system.
- Independence between safety systems and effects of design basis events.
- Independence between safety systems and other systems, both interconnected equipment and equipment in proximity.
- Effects of a single random failure.
- Detailed criteria.

For application of the independence criterion to digital computer systems, a reference is made to IEEE Std. 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations." Additional detailed criteria for independence are contained in section 5.6 of IEEE Std. 7-4.3.2-2003. Guidance for establishing communication independence is provided in Annex E of IEEE Std. 7-4.3.2-2003. Annex E is an informative annex.

DRAFT

12/11/2006

The NRC endorsed IEEE Std. 7-4.3.2-2003 in Regulatory Guide 1.152, revision 2, but did not endorse Annex E. In the discussion contained in the regulatory guide, the NRC stated that Annex E provides insufficient guidance. The NRC stated that additional guidance is provided in Appendix 7.0-A, "Review Process for Digital Instrumentation and Control Systems," Appendix 7.1.C, "Guidance for Evaluation of Conformance to IEEE Std 603," and Section 7.9, "Data Communication Systems," in NUREG-0800. However, NUREG-0800 states that Annex E of IEEE 7-4.3.2-2003 (was Annex G in previous revision of IEEE 7-4.3.2) describes an acceptable means for providing communications independence. Review of NUREG-0800 fails to identify any guidance that is not in Annex E of IEEE Std. 7-4.3.2-2003. The NRC staff has agreed to resolve this disconnect between documents.

Recent licensee experience indicates that companies planning to use communication between redundant safety divisions and between safety and non-safety systems must perform a detailed analysis of all possible failure modes. Staff reviews of some designs have required "infallible" designs in this area. Based on recent experience, the NRC staff may be considering that communication between redundant safety divisions and between safety and non-safety systems is contrary to the general design criteria in Appendix A of 10 CFR 50 and IEEE-603 guidance. This paper shows precedence for communication between redundant safety divisions and between safety and non-safety systems, explains the benefits obtained by using this technology, and recommends more predictable review guidance that clearly defines the required method and extent of analysis.

Definitions

The following definitions are from IEEE Std. 603-1998:

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. (Section 3.8 of IEEE Std. 603-1998)

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. Note – A division can have one or more channels. (Section 3.14 of IEEE Std. 603-1998)

Redundant equipment or system – A piece of equipment or a system that duplicates the essential function of another piece of equipment or system to the extent that either may perform the required function, regardless of the state of operation or failure of the other. Note – Duplication of essential functions can be accomplished by the use of identical equipment, equipment diversity, or functional diversity. (Section 3.22 of IEEE Std. 603-1998)

DRAFT

12/11/2006

Safety function - One of the processes or conditions (for example, emergency negative reactivity insertion, post-accident heat removal, emergency core cooling, post-accident radioactivity removal, and containment isolation) essential to maintain plant parameters within acceptable limits established for a design basis event.

NOTE—A safety function is achieved by the completion of all required protective actions by the reactor trip system or the engineered safety features concurrent with the completion of all required protective actions by the auxiliary supporting features, or both. (See Annex A [of IEEE 603] for an illustrative example.) (Section 3.23 of IEEE Std. 603-1998)

It is important that these definitions be used consistently to provide a common basis for discussing the complex issue of communications between redundant safety divisions and between safety and non-safety systems. For example, there is one recent case where the term "channel" was inappropriately used by a licensee in the description of how individual protective action signals are combined for verification and validation purposes. The improper use of the term contributed to questions raised by the NRC concerning the acceptability of the design.

Detailed Requirements in IEEE Std. 603-1998

Section 5.6.1, Independence between redundant portions of a safety system

"Redundant portions of a safety system provided for a safety function shall be independent of, and physically separated from, each other to the degree necessary to retain the capability of accomplishing the safety function during and following any design basis event requiring that safety function."

Section 5.6.3, Independence between safety systems and other systems

"The safety system design shall be such that credible failures in and consequential actions by other systems, as documented in Clause 4, item h) of the design basis, shall not prevent the safety systems from meeting the requirements of this standard."

Section 5.6.3.1, Independence of Interconnected equipment

a) Classification. Equipment that is used for both safety and nonsafety functions shall be classified as part of the safety systems. Isolation devices used to effect a safety system boundary shall be classified as part of the safety system.

b) Isolation. No credible failure on the non-safety side of an isolation device shall prevent any portion of a safety system from meeting its minimum performance requirements during and following any design basis event requiring that safety function. A failure in an isolation device shall be evaluated in the same manner as a failure of other equipment in a safety system."

Applicable Regulatory Documents

DRAFT

12/11/2006

10CFR50.55a(h) requires a licensee of a new plant to meet IEEE Std. 603-1991. When making modifications to an existing plant, a licensee can either continue to meet IEEE Std. 279-1971 or voluntarily upgrade to IEEE Std. 603-1991.

Reg. Guide 1.152, Revision 2, section B, subparagraph (e), states,

"Annex E, 'Communication Independence,' [of IEEE Std. 7-4.3.2-2003] is not endorsed by the NRC because it provides insufficient guidance. Additional guidance is provided in Appendix 7.0-A, 'Review Process for Digital Instrumentation and Control Systems,' Appendix 7.1.C, 'Guidance for Evaluation of Conformance to IEEE Std 603,' and Section 7.9, 'Data Communication Systems,' in NUREG-0800."

NUREG-0800, Appendix 7.0-A

"Data communication systems are treated as support systems (see Section 7.9), although they are often composed of specialized hardware, embedded software, and communication protocol software that runs on the computers linked together by the data communication system. They may support protection systems, other safety systems, diverse I&C systems, control systems, or any combination thereof. A design may provide separate safety and non-safety data communication systems. The review topics applicable to any data communication system are the combination of topics applicable to the I&C systems supported by that data communication system.

Computer internal data communication is at present accomplished by high-speed data buses that are usually designed by the makers of the computer system package itself. There are a number of standardized computer internal buses, and, unlike data communication systems, no software is involved (other than operating system software). Operation of computer internal buses is usually under the control of hardware. Unless this situation changes, computer internal data communication should be reviewed by confirming critical hardware characteristics. If software is involved in computer internal data communication, the review should proceed as described above under data communication systems."

NUREG-0800, Appendix 7.1.C

"Section 5.6 — Independence

This section requires in part independence between (1) redundant portions of a safety system, (2) safety systems and the effects of design basis events, and (3) safety systems and other systems. Three aspects of independence should be addressed in each case:

- Physical independence.
- Electrical independence.
- Communications independence.

DRAFT

12/11/2006

Guidance for evaluation of physical and electrical independence is provided in Reg. Guide 1.75, "Physical Independence of Electrical Systems," which endorses IEEE Std. 384, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits." The applicant/licensee should confirm that the safety system design precludes the use of components that are common to redundant portions of the safety system, such as common switches for actuation, reset, mode, or test; common sensing lines; or any other features which could compromise the independence of redundant portions of the safety system. Physical independence is attained by physical separation and physical barriers. Electrical independence should include the utilization of separate power sources. (The EELB and Plant Systems Branch (SPLB) review power source requirements. HICB reviewers should coordinate with these branch requirements to confirm that I&C safety system power sources are adequate.) Transmission of signals between independent channels should be through isolation devices.

BTP HICB-11 provides guidance for the application and qualification of isolation devices.

Annex G of IEEE Std. 7-4.3.2, as discussed in SRP Section 7.1.II, describes an acceptable means for providing communications independence. The review of communications independence should include confirmation that the routing of signals related to safety maintains (1) proper channeling through the communication systems, and (2) proper data isolation between redundant channels.

Where data communication exists between different portions of a safety system, the analysis should confirm that a logical or software malfunction in one portion cannot affect the safety functions of the redundant portion(s). If a digital computer system used in a safety system is connected to a digital computer system used in a non-safety system, the review should confirm that a logical or software malfunction of the non-safety system cannot affect the functions of the safety system."

NUREG-0800, Section 7.9

This SRP section (12 pages) describes the review process and acceptance criteria for data communication systems (DCSs) that are part of or support the systems described in Sections 7.2 through 7.8 of the applicant's safety analysis report (SAR). The scope and depth of the review and the acceptance criteria will vary according to the importance to safety of the system that the DCS is supporting.

The objectives of the review are to confirm that DCSs (1) conform to applicable acceptance criteria and guidelines, (2) will perform the safety functions assigned to them, (3) will meet the reliability and availability goals assumed for the system, and (4) will tolerate the effects of random transmission failures. A particular concern is that the transmission of multiple signals over a single path may constitute a single point of failure that may have a larger impact on plant safety than would occur in previous analog systems.

DRAFT

12/11/2006

The complete text can be found at <http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr0800/ch7/>.

Precedence for Communications Between Redundant Safety Divisions and Between Safety and Non-Safety Systems

Numerous designs that include communications between redundant safety divisions and between safety and non-safety systems have been reviewed and approved by the NRC. These prior applications include coincidence voting, channel bypass interlocks, and calculated tuning parameters. The following are examples of safety-to-safety communications that have been approved by the NRC:

1. CE Reactor Protection Systems use relay-based communication between redundant safety divisions for like-parameter coincidence voting. The System 80+ ALWR PPS also replaced these relay interfaces with digital communication links
2. Most CE Reactor Protection Systems and Plant Protection Systems in operation today employ conventional relay-based communication between redundant safety divisions for channel bypass interlocks. These interlocks allow only one failed sensor channel to be placed in a bypassed condition. The System 80+ ALWR PPS also replaced these relay interfaces with digital communication links.
3. CE Core Protection Calculator Systems (CPCS) in operation today employ digital communication to process DNBR penalty factors that originate in other redundant safety divisions. This concept was also used in the System 80+ ALWR design.
4. AREVA's Topical Report for the Telerperm XS digital platform, EMF-2110(NP)(A) Revision 1, describes digital communication between redundant safety divisions for reactor trip and ESFAS functions. The NRC approved this design via SER dated May 5, 2000 ML003711856.

Section 2.0 "System Description" of the SER describes two examples of communication between redundant safety divisions:

"The signal acquisition layer in each channel acquires analog and binary input signals from sensors in the plant...Each signal acquisition computer distributes its acquired and preprocessed input signals to the data-processing computers in the next layer. Thus, each data-processing computer is provided with the same set of input information.

The data-processing computers perform signal processing for plant protective functions such as signal on-line validation, limit value monitoring and closed-loop control calculations. The data-processing computers then send their outputs to two

DRAFT

12/11/2006

independent voter computer units.”

The following are examples of non-safety to safety system communications that have been approved by the NRC:

1. At many operating CE plants, the charging pump control circuits are Class 1E because the charging pumps are controlled by the ESFAS during emergency conditions. However, during normal operation the charging pumps are also controlled by the non-safety Pressurizer Level Control System (PLCS). The non-safety PLCS signals are interfaced to the Class 1E charging pump control circuits using conventional relay-based communication. Class 1E logic circuits assure ESFAS priority. The proper processing of the non-safety related data within the safety system logic and the use of Class 1E isolation devices (i.e., relays) prevent a failure in the non-safety circuitry from affecting proper action of the ESFAS.
2. In some BWRs, the safety-related Power Range Neutron Monitoring system includes two-way communications between safety and non-safety components. Signals from individual local power range monitors (LPRMs) are transmitted to the plant process computer for use in the 3D Monicore program. One of the functions of 3D Monicore is to calculate LPRM and average power range monitor (APRM) gain factors. These gain factors are transmitted back to the LPRMs and the APRMs. The new gain factors are stored in a buffer within the LPRMs and APRMs. The reactor engineer must manually accept the value stored in the buffer before it is transferred within the LPRMs and APRMs to become the new gain factors. The design is described in NEDC-32410P-A, "Nuclear Measurement Analysis and Control Power Range Neutron Monitor (NUMAC PRNM) Plus Option III Stability Trip Function," volumes 1 and 2 and supplement 1. This design for two-way communications was reviewed and approved by the NRC in a letter to General Electric dated August 15, 1997.
3. The Topical Report for the Telerperm XS digital platform, EMF-2110(NP)(A) Revision 1, describes non-safety to safety communication for testing and configuring logic and setpoints for reactor trip and ESFAS functions. The NRC approved this design via SER dated May 5, 2000 ML003711856.

Section 2.0, "System Description," of the SER describes digital data communication from the non-safety service unit to multiple safety system divisions:

“The MSI serves as a gateway between the computers of the automatic path and other non-safety-related systems such as service units, process control computers and monitoring computers... The non-safety-related service unit requests access through the MSI to perform the diagnostic function at the safety-related processor. The service unit...can be installed temporarily or permanently.

The service unit contains the central data of the I&C system. It is the central means for interventions into the safety-relevant software of the function

DRAFT

12/11/2006

processors... The service unit is protected against unauthorized interventions. The control mechanisms are controlled by software so that only authorized persons may access the service unit, only authorized interventions may be performed, and interventions are restricted to a single redundant channel at a time.”

In Section 5.0 “Summary of Regulatory Compliance Evaluations” the staff states:

“The TXS system conforms to the guidelines in RG 1.75 for protection system independence. On the basis of its review, the staff concludes that the TXS system satisfies the requirements of IEEE-603 with regard to system independence. Therefore, the staff finds that the TXS system satisfies the requirements of GDC 22.

Based on its review of the interfaces between the TXS safety systems and plant operating control systems, the staff concludes that the TXS safety systems satisfy the requirements of IEEE-603 with regard to control and protection systems interactions. Therefore, the staff finds the TXS safety systems satisfy the requirements of GDC 24.”

- 4) The NRC staff has reviewed the concept of non-safety operator stations in Westinghouse plants and provided discussion in the following references:
 - a) SER, "Acceptance for referencing of Topical Report CENPD-396-P, Rev. 01, Common Qualified Platform and Appendices 1, 2, 3 and 4 Rev.01", dated August 11, 2000.
 - b) SER, "Safety Evaluation for the closeout of several of the Common Qualified Platform Category 1 open items related to reports CENPD-396-P, Revision 1 and CE-CES-195, Revision 1", dated June 22, 2001.

Benefits of Communications Between Redundant Safety Divisions and Between Safety and Non-Safety Systems

Communications between redundant safety divisions and between safety and non-safety systems in the precedence described above have the following benefits:

1. Communication within the CE and AREVA Reactor Trip and ESF actuation systems is used to prevent spurious plant trips due to drifting sensors, single failures, or erroneous trip calculations that may exist in one safety division.
2. Bypass interlocks ensure that only one channel is placed in a bypass condition at one time. This ensures the system is always in compliance with the single failure criterion.

DRAFT

12/11/2006

3. Sharing sensor data and DNBR penalty factors between channels in the CPC allows each channel to generate trips based on information that represents the entire reactor core.
4. Communication from non-safety controls to the safety system allows the charging pumps to be used for both normal operation and emergency conditions, eliminating the need for additional pumps.
5. Dynamically adjusting the LPRM and APRM gain factors allows the plant to operate closer to the trip limits without increasing the potential for spurious trips.
6. The user-friendly video-based interface of the Teleperm XS Service Unit allows system maintenance to be performed with less potential for human error that could lead to spurious plant trips or safety system failures.
7. Operator workstations that control both safety and non-safety equipment allow operators to control multiple plant functions from a single display screen. This facilitates improved human factors.

Design Criteria

The use of computers in safety systems has provided an opportunity for a high level of data communication between computers within a single safety division, between safety divisions, and between safety and non-safety computer systems. As described above, there are significant benefits to such data communications. However, improper communications could result in the loss of a computer's ability to perform its function or multiple functions and thereby inhibit the safety system from performing its function.

Whenever communication techniques are employed, the major concern relates to the need to eliminate the potential loss of safety functions as a result of communication activities. This includes transmission of data and any vehicle for acknowledging receipt of the data or indicating a failure in data transmission. The detection and correction of any communication failures cannot be allowed to impede or interfere with the performance of safety functions. Proper independence, both electrical and communication isolation must be ensured. It is noted that electrical and communication physical points of isolation may be different. IEEE Std. 384 provides electrical isolation requirements. Annex E of IEEE Std. 7-4.3.2-2003 provides detailed methods that can be employed to allow communication without negatively affecting the safety system.

The detailed methods for communications isolation described in Annex E of IEEE Std. 7-4.3.2-2003 are provided in the form of a recommended practice. A recommended practice typically uses "should" and "may" instead of "shall" as found in a standard. This language allows deviation from the recommended practice if an alternative practice is found acceptable.

DRAFT

12/11/2006

Discussion with an NRC staff member indicates the recommendations in Annex E of IEEE Std. 7-4.3.2-2003 are judged to provide a sound technical basis for communications isolation. However, a significant concern is the language used in the recommended practice. Therefore, Annex E was reviewed to identify changes that would make the recommended practice more enforceable from a regulatory viewpoint. The suggested changes are shown in red in attachment 1.

Annex E of IEEE Std. 7-4.3.2-2003 discusses use of a buffering feature between the communications link and the safety function to ensure integrity of the safety function. However, Annex E omits sufficient criteria to judge the acceptability of the buffering circuit. It is recommended that a buffering circuit meet the following criteria:

- 1) The buffering circuit shall be separate from the processor performing the safety function (e.g., a separate processor on the same card, separate memory on the same card, located on a separate card).
- 2) The operation of the processor performing the safety function shall be independent of the operation of the buffering circuit (e.g., the two devices operate asynchronously with respect to each other, no shared clocking device).
- 3) Verification and validation activities shall include the buffering circuit, including both normal operating requirements and credible failure modes.
- 4) The physical link between two buffering circuits in different divisions shall provide electrical isolation.

It is recommended that Annex E of IEEE Std. 7-4.3.2-2003 be modified to incorporate the above criteria.

Based on the precedence described above and input from subject matter experts, the following additional design practices were identified to ensure high-quality communications between redundant safety divisions and between safety and non-safety systems:

1. CPUs that perform safety system logic processing shall perform no communication handshaking or interrupts that could disrupt deterministic logic processing.
2. Unpredicted data cannot be transferred. Predefined data sets ensure only known data can be transmitted by the sending system or received by the receiving system. Unrecognized data is rejected by the receiving system. There is no file transfer capability within the safety systems.
3. On-line data communication cannot alter safety system software. Hardwired interlocks that are part of the safety system ensure changes to safety system software cannot be made through the data communication interface or can only be made during off-line operation (i.e., when the hardwired interlock is disabled).
4. Credible spurious communications (e.g., sleeping/frozen interface communications, erroneous data sets, and spurious data sets) shall not prevent performance of required safety functions.
5. All communications from non-safety-related equipment to safety-related equipment shall be from within the same cyber security defensive layer (refer to NEI 04-04, revision 1).

DRAFT

12/11/2006

It is recommended that these additional design practices be incorporated into Annex E of IEEE Std. 7-4.3.2-2003.

There has been discussion between the NRC and industry personnel about design criteria applicable to a workstation that controls both safety-related and non-safety-related systems and equipment. In addressing this topic, it is important that the term "safety function" be applied properly. A safety function is provided only by those components that are "essential" in maintaining plant parameters within acceptable limits established for a design basis event. If a design includes a workstation that controls both safety-related equipment and non-safety-related equipment, the workstation must be safety related or the workstation must be properly isolated from the safety-related circuitry. If the isolated workstation approach is used, the following apply:

- Controls on the isolated workstation must be limited to non-essential control of safety-related equipment. The isolated workstation is classified as non-safety since it is not performing a safety function per section 5.6.3.1 of IEEE Std. 603-1998.
- All safety functions must be capable of being performed solely by safety-related structures, systems, and components.
- Isolation provisions must provide both electrical and communication isolation as required by IEEE Std. 7-4.3.2-2003 and Regulatory Guide 1.152, revision 2.
- Safety-related accident monitoring instrumentation must be provided per the requirements of IEEE Std. 497-2002 and Regulatory Guide 1.97, revision 4.
- Additional non-safety-related accident monitoring instrumentation must be provided per the requirements of IEEE Std. 497-2002 and Regulatory Guide 1.97, revision 4. If the design and qualification requirements applicable to this portion of the accident monitoring instrumentation are met by the non-safety-related workstation, the workstation can be the sole indication for these additional non-safety-related parameters.

The requirements of IEEE Std. 7-4.3.2-2003 (subject to the enhancements suggested above) are judged sufficient to ensure that all safety functions can be performed when a design includes a workstation that controls both safety-related and non-safety-related systems and components.

During discussions about the use of an isolated workstation for control of both safety-related and non-safety-related systems and components, it was recognized that credible failures of the workstation and actions that result from spurious communication failures must be bounded by the safety analysis. Other existing criteria such as section 6.3, "interaction between the sense and command features and other systems," of IEEE Std. 603-1998 and requirements for transient analysis adequately address this concept.

DRAFT

12/11/2006

Proposed NRC Review Guidance

The NRC staff is preparing a revision to the standard review plan (SRP) in NUREG-0800. It is understood that one of the proposed changes is to move the following words from section 7.1 of the SRP to a new section 7.1-D that augments IEEE 7-4.3.2-2003, Annex E requirements:

"Annex G of IEEE Std 7-4.3.2 describes acceptable approaches to computer communication independence. The preferred approach to communication independence ensures that:

- (1) redundant safety-grade equipment communicate via one-way communications paths,
- (2) safety-grade systems do not receive information from non-safety-grade systems except when under test,
- (3) if two-way communications are used, failure of coordination or handshaking between sending and receiving systems does not prevent either system from functioning correctly, and
- (4) the control of communications links resides in the sending system.

SRP Appendix 7.1-C provides guidance for the review of communications independence."

In lieu of the NRC preferred approach described above, it is suggested that new SRP section 7.1-D:

- a) Incorporate the buffering circuit acceptance criteria described above.
- b) List and endorse the changes to Annex E of IEEE Std. 7-4.3.2-2003 as shown in Attachment 1 to this white paper.
- c) Incorporate the additional design practices described above.

Incorporating these items into the SRP is judged to provide a sufficient set of attributes to guide staff review of a licensee submittal.

Use of the buffering circuit acceptance criteria, the proposed changes to Annex E of IEEE Std. 7-4.3.2-2003, additional design practices suggested, and the other requirements of IEEE Std. 603-1998 and IEEE Std. 7-4.3.2-2003 ensures the following attributes are met for communication between redundant safety divisions and between safety and non-safety systems:

1. Electrical independence – Electrical faults in one electrical division cannot adversely affect performance of the safety function. Electrical faults in non-safety systems cannot adversely affect any safety function.
2. Communications independence – Erroneous data originating in one electrical division cannot adversely affect performance of the safety function. Erroneous data originating in a non-safety system cannot adversely affect any safety function.

DRAFT

12/11/2006

Long-Term Actions

The final resolution of the issues regarding communications between redundant safety divisions and between safety and non-safety systems should be in cooperation with IEEE Nuclear Power Engineering Committee (NPEC) working group SC 6.4. It is suggested that the proposed changes to Annex E of IEEE Std. 7-4.3.2-2003 be incorporated in the next revision of the standard. The buffering circuit acceptance criteria and the additional design considerations identified in this paper should be evaluated for inclusion in IEEE Std. 7-4.3.2. Once IEEE Std. 7-4.3.2 is revised consistent with these recommendations, the NRC should revise Regulatory Guide 1.152 to endorse the revised IEEE Std. 7-4.3.2.

Attachment 1 – Recommended changes to IEEE Std. 7-4.3.2

Annex E, Communication independence

E.1 Background

The use of computers in safety systems has provided an opportunity for a high level of data communication between computers within a single safety channel, between safety channels, and between safety and nonsafety computer systems (see also 5.6). Improper use of this communication ability could result in the loss of a computer's ability to perform its function or multiple functions and thereby inhibit the safety system from performing its function. This annex provides detailed methods that could be employed to allow the greatest use of communication without negatively affecting the safety system. Isolation should be considered in order to prevent fault propagation between safety channels and from a nonsafety computer to a safety computer.

E.2 Discussion

Whenever communication techniques are employed, the major concern relates to the need to eliminate the potential loss of safety functions as a result of communication activities. This includes transmission of data and any vehicle for acknowledging receipt of the data or indicating a failure in data transmission. The detection and correction of any communication failures should not be allowed to impede or interfere with the performance of safety functions.

For proper independence of the safety computer from nonsafety equipment, both electrical and communication isolation should be ensured. It should be noted that electrical and communication physical points of isolation may be different. Electrical isolation requirements are provided in IEEE Std 384-1992 [B5]. Recommendations for methods of communication isolation follow.

E.2.1 Communication between computers in different safety channels

Communication between computers in different safety channels may be desired for such purposes as voter logic or time stamp synchronization. Upon a failure of the communication, the preferred failure state **shall** be set if one has been identified. Figures E.1 and E.2 depict ways in which this can be accomplished.

Figure E.1 depicts broadcast communication between a safety computer in channel A and a safety computer in channel B. The one-way communication path provides a point of software isolation. The physical link(s) between the computers provide electrical isolation. This isolation may be accomplished optically (i.e., fiber optic cable or optical isolators). Communications isolation is provided through the broadcast communication.

The buffering circuit provides an interface allowing acknowledgment or no acknowledgment of data transfer between channels, collision avoidance, etc. It serves as a buffering feature between the communications link and the safety function to ensure integrity of the safety function. The buffering circuit should be separate (e.g., at a minimum on a different board) from the processor performing the safety function. The buffering circuit may be another processor, memory card(s), etc. V&V activities **shall** include the buffering circuit. The physical link between the buffering circuits **serves** as the point of electrical isolation.

DRAFT

12/11/2006

Figure E.2 depicts a method with two separate points of isolation, one electrical and one for communications. This method allows two-way communication between safety computers, as long as a buffering circuit is employed.

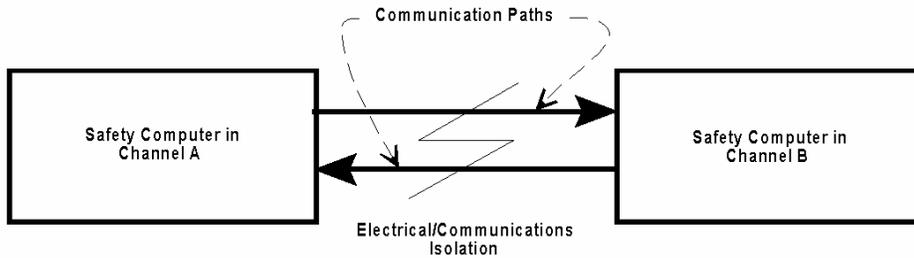


Figure E.1—Communication between safety channels (One-way communication)

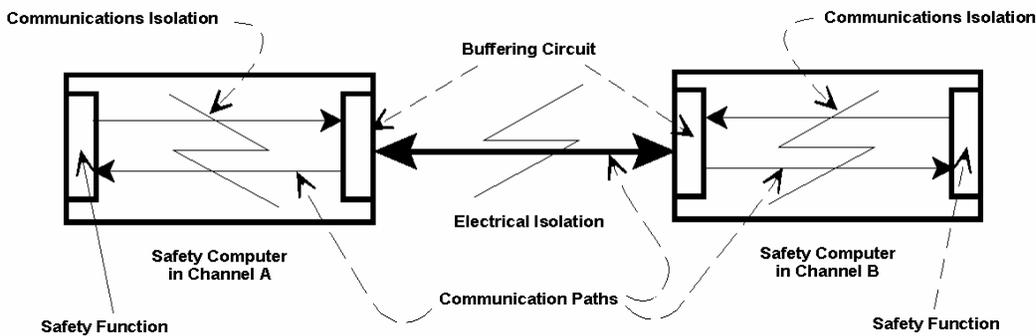


Figure E.2—Communication between safety channels (two-way communication)

The broadcast communication link between the safety function and the buffering circuit serves as a route for data to be sent out by the safety computer. The separate communication from the buffering circuit allows the safety function processor to receive data from another channel. The process of requesting and receiving data from another channel shall not result in loss of either of the safety functions.

E.2.2 Communication between safety and nonsafety computers

Communication between safety and nonsafety computers may be desired for purposes of time stamp synchronization and installation of approved setpoint changes. However, at no time should the safety computer require input from the nonsafety computer in order to perform its safety function. The following figures depict ways communication between safety and nonsafety computers can be accomplished.

Figure E.3 graphically shows a broadcast communication between the safety computer and the nonsafety computer. The one-way communication path provides for communication isolation. The physical link(s) between computers provides both electrical and communications isolation as required. Electrical isolation may be accomplished optically (i.e., fiber optic cable or optical isolators). Communications isolation is provided through the broadcast communication path.

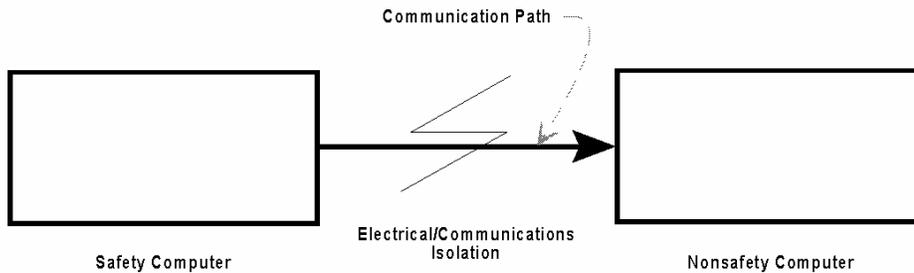


Figure E.3—Communication between safety and nonsafety computers (one-way communication)

Figure E.4 depicts a method with two separate points of isolation, one electrical and one communications. This method allows two-way communication between the safety computer and the nonsafety computer, as long as a buffering circuit is employed in the safety computer. Use of this method may be necessary when a separate computer is used for test and calibration purposes.

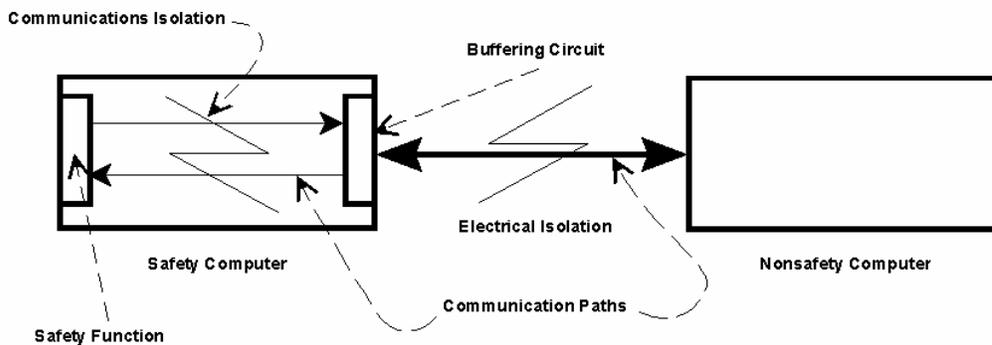


Figure E.4—Communication between safety and nonsafety computers (two-way communication)

The buffering circuit provides an interface allowing acknowledgment or no acknowledgment of data transfer between channels, collision avoidance, etc. It serves as a buffering feature between the communications link and safety function to assure the integrity of the safety function. The buffering circuit should be separate (i.e., at a minimum on a different board) from the processor performing the safety function. It may be another processor, memory card(s), etc. V&V activities **shall** include the buffering circuit. As required, the link between the buffering circuit and the nonsafety computer provides electrical isolation.

The broadcast communication link between the safety function and the buffering circuit serves as a route for data to be sent by the safety computer. The process of sending data **shall** not result in loss of the safety function. The broadcast communications link from the buffering circuit to the safety function is necessary when a separate test and calibration computer is employed.

DRAFT

12/11/2006

Figure E.5 is similar to figure E.4 except that an optional buffering circuit and communication path is employed in the nonsafety computer.

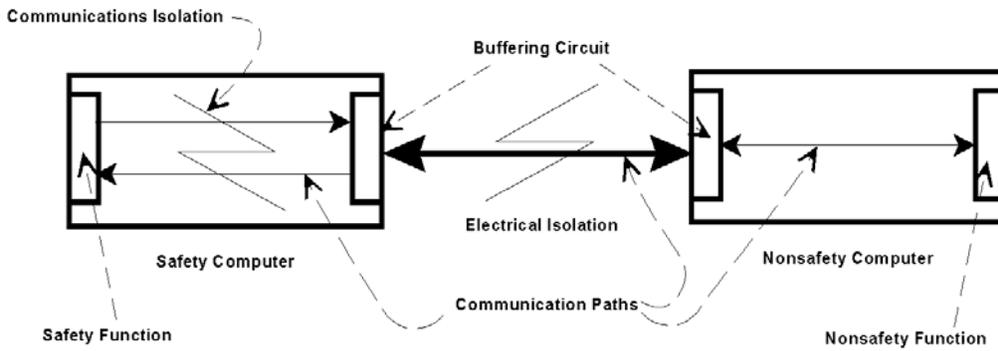


Figure E.5—Communication between safety and nonsafety computers