5.6 Independence

In addition to the requirements of IEEE Std 603-1998, data communication between safety divisions or between safety and non-safety systems shall not inhibit the performance of the safety function. Redundant Channels within the same division are not subject to the requirements of this section.

IEEE Std 603-1998 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 safety functions and software performing non-safety functions may reside on the same computer and use the same computer resources.

Safety systems shall be designed such that no input from non-safety systems is required for the system to perform its safety functions. Data input (e.g., setpoints, scaling, etc.) from a non-safety system that receives verification equivalent to the quality of the safety system such as independent reviews and configuration controls is an acceptable for use in a safety system (See section 5.6.4.3 for detail criteria).

5.6.1 Between redundant portions of a safety system

In addition to IEEE Std 603-1998 requirements, see section 5.6.4 for additional detailed criteria.

5.6.2 Between safety systems and effects of design basis event

No requirements beyond IEEE Std 603-1998 are necessary.

5.6.3 Between safety systems and other systems

In addition to IEEE Std 603-1998 requirements, see section 5.6.4 for additional detailed criteria.

5.6.3.1 Interconnected equipment

In addition to IEEE Std 603-1998 requirements, see section 5.6.4 for additional detailed criteria.

5.6.3.2 Equipment in proximity

a) ***Separation.***

No requirements beyond IEEE Std 603-1998 are necessary.

b) ***Barrier.***

Either of the following approaches is acceptable to address the previous issues:

a) Barrier requirements shall be identified to provide adequate confidence that the non-safety functions cannot interfere with performance of the safety functions of the software or firmware. The barriers shall be designed in accordance with the requirements of this standard. The non-safety software is not required to meet these requirements.

b) If barriers between the safety software and non-safety software are not implemented, the non-safety software functions shall be developed in accordance with the requirements of this standard.

5.6.3.3 Effects of a single random failure

No requirements beyond IEEE Std 603-1998 are necessary.

5.6.4 Detailed criteria

5.6.4.1 Buffering Function

A buffering function provides an interface allowing data transfer between channels. 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 from the processor performing the safety function. The following criteria shall be applied to the buffering function:

a) 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, separate logic in an FPGA, or located on a separate card).
b) The execution of the safety function shall be independent of the operation of the buffering function (e.g., increased data rate to the buffer shall not affect the safety function such as decreasing its response time.)
c) The buffering functions shall be subject to the same V&V processes as the safety system functions.
d) The buffering circuit may also provide electrical isolation if the physical link (e.g., fiber optic medium) is qualified for fault isolation.

5.6.4.2 Communications

The following criterion applies to digital communications between redundant safety divisions and between safety and non-safety systems to ensure high-quality:

a) The processor performing the safety function 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 safety 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 divisions shall be processed in a manner that does not adversely affect the safety function of other independent divisions.
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. (Does this cause Triconex a problem?)
e) Data communication shall not alter safety system software while the safety system's channel is in operation (e.g., interlocks that prevent on-line changes to safety system software).
f) Credible communication faults (e.g., sleeping/frozen interface communications, erroneous data sets, and spurious data sets) shall not prevent performance of required safety functions.

5.6.4.3 Data Exchange

The following criterion applies to data exchange between non-safety and safety systems to ensure high-quality:

a.) The safety system shall not be dependent on the non-safety related communication link or the data from the non-safety related system to perform its safety related function.
b.) Data can be received from non-safety related system/instrument if the safety related system is placed in a non-operable (Inop) state and data is confirmed by manual action (operator) to ensure that the correct data is downloaded or the information is buffered in a safety related device until such time when the safety related system can be placed in an Inop state. At this time the operator confirms the download, verifies that the safety function is functional/operable, and returns the safety related instrument to the operable state.

c.) Data that is not used for safety related functions, such as a time clock, which is used for time stamping events may be stored in a buffer where the safety related function/data is not affected by the non-safety related time stamping being buffered.

3.1 Definitions

Barrier: A component or feature of the design that prevents adverse interaction between two safety divisions or between a safety division and a non-safety system.

Guidance for establishing communication independence is provided in Annex E.