DRAFT DRAFT DRAFT

DIGITAL INSTRUMENTATION AND CONTROLS

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

Requirements and Acceptance Criteria:
Provisions for Interdivisional[1] Communications

As used in this document, interdivision communications includes communications involving entities in different 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. Interdivision communications may be bidirectional or unidirectional. Bidirectional communication among safety divisions and between safety and nonsafety equipment is acceptable provided certain restrictions are enforced. Bidirectional communications should be assumed in the following discussions, unless indicated otherwise.

1 GENERAL CRITERIA

Each safety division must be protected from undue influence from other safety divisions and from nonsafety divisions. In addition, the communication process itself should be carried out by a communications processor[2] [3] separate from the function processor that executes the division 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 by means of technology such as dual-ported memory or other shared memory or other technology that ensures there is no disruption to the deterministic execution of the function processor. Access to the shared memory must be controlled in such a manner that the function processor has sufficient access to the share memory to complete the safety function in a deterministic manner and within the required loop cycle time. Failure of the logic to meet this criterion must be detectable. The function processors shall be designed to perform the required safety function with a credible single failure that adversely affects the data in shared memory.

The following criteria apply to digital communications between redundant safety divisions and between safety and non-safety divisions while the system is operable (Note that these requirements do not apply to communications within a safety division):

[1] Based upon the IEEE 603 definition of division.

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

[3] The communication function and the safety logic function can be implemented in separate logic within a single FPGA or ASIC device. The interface between the two functions must meet these requirements for interdivisional communications.

Formatted: Font color: Auto

Formatted: Font color: Auto

Formatted: Font color: Auto

Deleted: July 25, 2007

Deleted: 10:54 AM

Inserted: July 25, 2007

Deleted: July 2, 2007

Inserted: 10:54 AM

Deleted: 11:52 AM

Deleted: NEI Markup of HICRcRequirements-Comm (3) rev1.doc

a) The function processor must perform no communication handshaking, and must not be subject to communications-related interrupts.

b) Only predefined data sets (pre-determined message format and protocol, with the same sort of information located in the same position of each message) may be accepted by the receiving system. Unrecognized messages and data must not be used within the safety function logic executed by the function processor.

c) Data exchanged between redundant safety system divisions must be processed in a manner that does not adversely affect the safety function of the sending division, the receiving division, or any other independent divisions.

d) Incoming message data must be stored in fixed, predetermined, locations in the shared memory and in the memory associated with the function processor. These memory locations must not be used for any other purpose. The function processor and shared memory locations must be allocated such that input data and output data are segregated (in separate areas) from each other.

e) Data communication must not be able to alter any memory locations that are not intended to be adjusted periodically by operations personnel. This includes base system software, application software and protected setpoints[4] and constants. On-line changes to these memory locations shall be blocked by interlocks (e.g. physical and/or software) that require physical actions. Examples of acceptable means of enabling the access to perform changes to these memory locations include keylock switches, memory chip partitions, or password enabling.

Formatted: Font color: Auto

Formatted: Font color: Auto

f) The progress of the function processor through its software loop shall not be adversely affected by any message from outside the division.

g) Credible communication faults shall not prevent performance of required safety functions. Credible communications faults to consider include:

1. Messages may be corrupted due to errors in communications processors, errors introduced in buffer interfaces, introduced in the transmission media, or from interference.
2. Messages may be repeated at an incorrect point in time.
3. Messages may be sent in the incorrect sequence.
4. Messages may be lost, which includes both failures to receive an uncorrupted message or to acknowledge receipt of a message.
5. Messages may be delayed beyond their permitted arrival time window, including errors in the transmission medium, congested transmission lines, interference, or by delay in sending buffered messages.

Deleted: July 25, 2007

Deleted: 10:54 AM

Inserted: July 25, 2007

Deleted: July 2, 2007

Inserted: 10:54 AM

Deleted: 11:52 AM

Deleted: NEI Markup of HICRcRequirements-Comm (3) rev1.doc

[4] In this context software includes addressable constants/setpoints that are not intended to be adjusted periodically by operations personnel.

6. Messages may be inserted into the communication medium, from unexpected or unknown sources.

7. Messages may be sent to the wrong destination, which could treat the message as a valid message.

8. Messages may be longer than the receiving buffer, resulting in buffer overflow and memory corruption.

9. Messages may contain data that is outside the expected range.

10. Messages may appear valid, but data may be placed in incorrect locations within the message.

11. Messages may occur at a high rate that degrades or causes the system to fail (i.e., broadcast storm).

h) Malfunctions of control system resources (e.g., workstations, application servers) shared between systems shall have an impact that is consistent with the assumptions made in the safety analysis of the plant. Design considerations include:

1. No single unit of software shall generate commands to multiple control processors that are assumed to malfunction independently by the safety analysis.

2. No single control action (e.g., mouse click) shall generate commands to multiple control processors that are assumed to malfunction independently by the safety analysis.

3. Each control processor or its associated communication processor shall detect and block commands from the shared resources that do not pass the communication error checks.

Delete Section 2 - Existing criteria addresses communication needs.

~~2 VITAL COMMUNICATIONS~~

~~(communications necessary for the successful execution of a safety functions)~~

Delete Section 3 - Existing criteria addresses communication needs and safety analysis topics should be address by D3 TWG and acceptance criteria.

~~3 GENERAL COMMUNICATIONS~~

~~(communications not supporting any safety function)~~

Deleted: July 25, 2007
Deleted: 10:54 AM
Inserted: July 25, 2007
Deleted: July 2, 2007
Inserted: 10:54 AM
Deleted: 11:52 AM
Deleted: NEI Markup of HICRcRequirements-Comm (3) rev1.doc