RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

8/22/2024

SAFETY SYSTEM DIGITAL PLATFORM
- MELTAC (MITSUBISHI ELECTRIC TOTAL ADVANCED CONTROLLER) -
TOPICAL REPORT

Mitsubishi Electric Corporation

EPID:	**L-2023-TOP-0036**
RAI NO.:	**RAI 6**
DATE OF RAI ISSUE:	**1/19/2024**

RAI 6

Regulatory Basis: 10 CFR 50.55a(h), “Protection and Safety Systems,” requires that protection systems must be consistent with their licensing basis or may meet the requirements of the IEEE Std 603-1991, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations,” and the correction sheet dated January 30, 1995. Clause 5.6.1, “Between Redundant Portions of a Safety System” states, in part, that 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 to accomplish the safety function during and following any design basis event requiring that safety function. Clause 5.6.3, “Between Safety Systems and Other Systems”, states, in part, that the safety system design shall be such that credible failures in and consequential actions by other systems, as documented in Section 4.8 of the design basis, shall not prevent the safety systems from meeting the requirements of this standard. MELTAC is a safety system digital platform which shall meet the requirements in the above Clauses 5.6.1 and 5.6.3.

Background and Issue: Section 4.3.2 of the MELTAC TR states that the Control Network can also be used to communicate non-safety data between different divisions. Staff Position 3 of Digital Instrumentation & Controls (DI&C)-Interim Staff Guidance (ISG)-04 says that “A safety channel should not receive any communication from outside its own safety division unless that communication supports or enhances the performance of the safety function”.

Request: Please clarify what non-safety data are communicated between safety divisions and provide justifications on how the revised Melco platform meets the above criterion of DI&C-ISG-04.

ANSWER:

There is no non-safety data communicated between safety divisions. Section 4.3.2 and

4.3.3 of MELTAC Topical Report (JEXU-1041-1008) will be revised to clarify the restrictions for inter-divisional communication below.

There is no non-safety data communicated between safety divisions via the Data Link. In addition, the Control Network can provide inter-divisional communication between the non-safety system and one or more safety divisions. However, there is no inter-divisional communication between safety divisions via the Control Network.

As stated in Section 3.1.3 of MELTAC Platform ISG-04 Conformance Analysis Report (JEXU-1041-1015), Staff Position 3 of Digital Instrumentation & Controls (DI&C)-Interim Staff Guidance (ISG)-04 is a functional independence requirement that is addressed at the application level.

The MELTAC Platform is capable of a Data Link which can be used for inter-divisional communication between safety divisions and a Control Network which can be used for inter-divisional communication between the non-safety system and one or more safety divisions. These capabilities can support human tasks via multi-divisional VDUs by reducing burden, reducing the likelihood of human errors, and the use of advanced graphical user interfaces. However, the signals to be communicated to the safety divisions from the non-safety division, and whether they support or enhance the performance of the safety function, are evaluated at the application level.

Impact on Topical Report and/or Support Documents.

Section 4.3.2 and 4.3.3 of MELTAC Topical Report (JEXU-1041-1008) will be revised (see Attachment-1).

Section 3.1.1 and 3.4.2 of MELTAC platform ISG-04 Conformance Analysis (JEXU-1051-1015) will be revised (see Attachment-2). Q8

Revision History

Revision	Date	Page (section)	Description
0	March 2024	All	Initial issue
1	August 2024	2 Attachment 2	Revised to reflect the result of NRC Observation meeting (ADAMS Accession No. ML24206A078 and ML24212A321). Q8 notation corresponds to the NRC question number for RAI responses. Added section 3.1.1 and 3.4.2 of ISG-04 Conformance Analysis (JEXU-1041-1015) as the impact on support documents. Added the markup of section 3.1.1 and 3.4.2 of ISG-04 Conformance Analysis (JEXU-1041-1015).

4.3 Communication System

4.3.1 General Description

The key design bases of the Control Network, Data Link and Maintenance Network are provided below. These are applicable to both the controller and the safety VDU processor.

a) Maintenance Network, Control Network and Data Link:

- Asynchronous communication is used. The CPU Module and the communication controller execute their tasks asynchronously. This is facilitated through shared 2-port memory, which allows data to be communicated between the two digital components with no synchronization.
- The CPU Module performs no communication handshaking that could disrupt deterministic logic processing. The digital components that execute the safety functions are separate from the digital components that execute the communications.
- Predefined data size and structure ensure deterministic communication.
- Electrical faults or communication processing faults in one electrical division (or controller) cannot adversely affect performance of the safety function in other divisions (or controllers).

b) Maintenance Network:

- Hardwired interlocks in the CPU Module ensure changes to basic software or application software cannot be made through the data communication interface while the controller or the safety VDU processor are operating, or while the CPU Module is installed in the on-line chassis.

4.3.2 Control Network

The Control Network communicates plant process data and control signal data with a deterministic periodic cycle.

The Control Network is used for the following applications:

a) The Control Network is used ~~mainly~~ to communicate safety-related data ~~between multiple~~ among controllers and safety VDU processors within any single safety division~~, and between controllers and the safety VDU processor(s), all in the same division~~.

b) The Control Network ~~can~~ is also ~~be~~ used to communicate non-safety data between ~~different divisions including~~ the non-safety system and one or more safety divisions. ~~This may be between multiple controllers in different divisions.~~ RAI 6, 9

The specific inter-divisional communication data is application specific. The typical types of inter-divisional communication between safety and non-safety are as follows:

- Process signals from non-safety controllers to manually control the safety components of each division.
- Alarm or Status information from the safety components or safety instrumentation to non-safety controllers.

Inter-divisional communication ~~for safety-related functions~~ between safety divisions is not implemented in the Control Network. For this application only Data Link communication is used, see Section 4.3.3. RAI 6, 8, 9

4.3.3 Data Link

4.3.3.1 Configuration

Data Link communication is used to transmit process signals between the controllers in different safety trains. In addition, there is no non-safety data communicated between safety divisions via the Data Link. The Data Link uses a broadcast protocol with a 1 Mbps throughput, with no communication handshaking. RAI 6

Figure 4.3-14 provides a graphical representation of typical Data Link connections between redundant safety trains. This figure shows all the Data Link components and an example of a connection configuration when CH1 of the controller for train A is the transmission port (T), CH1 of controllers for other trains is the reception port (R), CH4 of controller for train D is the transmission port (T), and CH4 of controllers for other trains is the reception port (R).

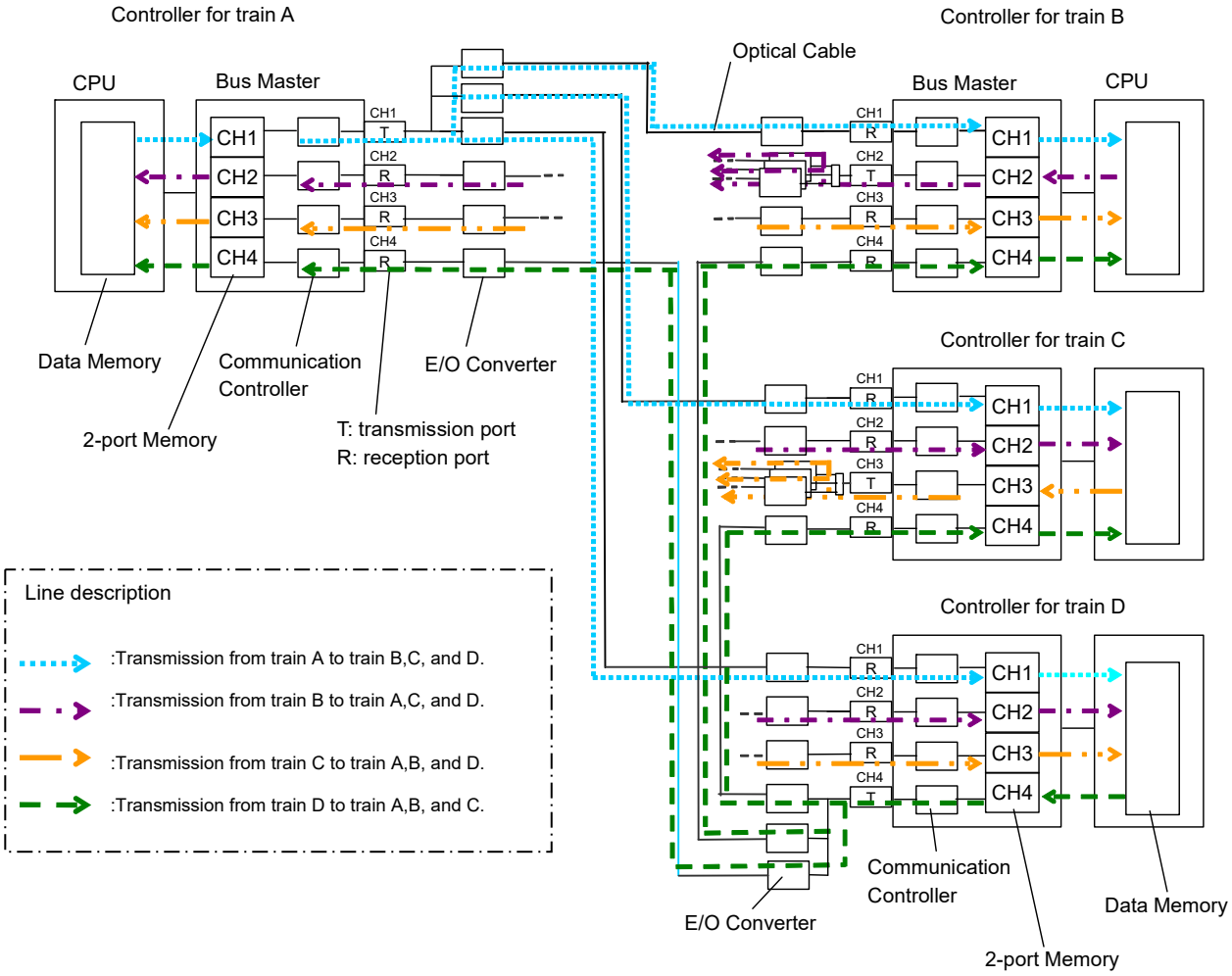

Figure 4.3-14 Example of Connection Configuration of Data Link Configuration

The Data Link is interfaced through Bus Master Modules. The Bus Master Module provides 4 communication ports (also referred to as channels). **[**

3.1.1 Staff Position 1

Requirement
A safety channel should not be dependent upon any information or resource originating or residing outside its own safety division to accomplish its safety function. This is a fundamental consequence of the independence requirements of IEEE603. It is recognized that division voting logic must receive inputs from multiple safety divisions.
Analysis

RAI-6
Rev.1
Q8

3.4 Analysis of Multidivisional Control and Display Stations (Section 3 of ISG-04)

This section describes the analysis of multidivisional control and display stations. Staff Position 3.1 in ISG-04 provides the criteria for this analysis.

3.4.1 Staff Position 3.1 - 1.

Requirement
Nonsafety stations receiving information from one or more safety divisions: All communications with safety-related equipment should conform to the guidelines for interdivisional communications.
Analysis

3.4.2 Staff Position 3.1 - 2.

Requirement
Safety-related stations receiving information from other divisions (safety or nonsafety): All communications with equipment outside the station's own safety division, whether that equipment is safety-related or not, should conform to the guidelines for interdivisional communications. Note that the guidelines for interdivisional communications refer to provisions relating to the nature and limitations concerning such communications, as well as guidelines relating to the communications process itself.
Analysis

RAI-6 Rev.1 Q8