MELTAC Platform ISG-04 Conformance Analysis

Non-Proprietary Version

September 2014

Prepared:	Kazufumi Yoshida	Sep. 4, 2014
	Kazufumi Yoshida, Manager Control & Protection Systems Section	Date
Reviewed:	Manabu Taniguchi	Sep. 5, 2014
	Manabu Taniguchi, Manager Control & Protection Systems Section	Date
Approved:	Hidetoshi Matsushita	Sep. 5, 2014
	Hidetoshi Matsushita, Section Manager Control & Protection Systems Section	Date

Signature History

	Rev.0			
Prepared	Kazufumi Yoshida			
Reviewed	Manabu Taniguchi			
Approved	Hidetoshi Matsushita			

Revision History

Revision	Date	Page (section)	Description
0	September 2014	All	Initial issue

This document has been prepared by Mitsubishi Electric Corporation, Ltd. ("MELCO") in connection with its request to the U.S. Nuclear Regulatory Commission ("NRC") licensing review of the MELTAC platform. No right to disclose, use or copy any of the information in this document, other than by the NRC and its contractors in support of the licensing review of the MELTAC platform, is authorized without the express written permission of MELCO.

This document contains technology information and intellectual property relating to the MELTAC platform and it is delivered to the NRC on the express condition that it not be disclosed, copied or reproduced in whole or in part, or used for the benefit of anyone other than MHI without the express written permission of MELCO, except as set forth in the previous paragraph.

This document is protected by the laws of Japan, U.S. copyright law, international treaties and conventions, and the applicable laws of any country where it is being used.

Mitsubishi Electric Corporation
7-3, Marunouchi 2-chome, Chiyoda-ku
Tokyo 100-8310 Japan

Abstract

This document contains the MELTAC platform conformance analysis against the applicable requirements of NRC DI&C Interim Staff Guidance (ISG)-04 "Highly-Integrated Control Rooms-Communications Issues (HICRc)" and NUREG/CR-6991 “Design Practices for Communications and Workstations in Highly Integrated Control Rooms”. This analysis also identifies requirements that are fulfilled at the application level, but does not address compliance to those requirements.

ISG-04 and NUREG/CR-6991 establish requirements for inter-division digital communication interfaces. The two digital inter-division communication interfaces used in the MELTAC platform are the Maintenance Network and the Data Link. The Maintenance Network is used only within a single division to allow communication between safety-related MELTAC controllers or safety VDU processors and the non-safety MELTAC engineering tool. The Data Link is typically used to send data from one safety division to another but may also be used to send data to a non-safety related MELTAC controller.

ISG-04 also establishes requirements for priority modules that combine diverse actuation signals with the actuation signals generated by the safety system. In the MELTAC platform these are referred to as Power Interface (PIF) Modules.

In addition, ISG-04 contains requirements for multidivisional control and display stations. The MELTAC platform includes a safety VDU. Control signals from a safety VDU and associated safety VDU processor could be interfaced to a different division using the Data Link; this would be configured at the application level. The MELTAC engineering tool can be temporarily connected to the MELTAC controller and safety VDU processor through the Maintenance Network and is not connected during normal operation.

This analysis demonstrates that the MELTAC platform complies with the applicable requirements.

Table of Contents

List of Tables

List of Figures

List of Acronyms

ASIC	Application Specific Integrated Circuit
ATWS	Anticipated Transients Without Scram
CCF	Common Cause Failure
CFR	Code of Federal Regulations
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CYC	Constant-Cycle
DAS	Diverse Actuation System
DCD	Design Control Document
DI	Digital Input
DP	Data Packet
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ESF	Engineered Safety Features
ESFAS	Engineered Safety Features Actuation System
FET	Field Effect Transistor
FMEA	Failure Modes and Effects Analysis
FPGA	Field Programmable Gate Array
F-ROM	Flash Electrically Erasable Programmable Read Only Memory
F/W	Firmware
I&C	Instrumentation and control
IEEE	Institute of Electrical and Electronics Engineers
I/F	Interface
I/O	Input/Output
IPL	Interposing Logic
ISG	Interim Staff Guidance
LSI	Large Scale Integration
MELTAC	Mitsubishi Electric Total Advanced Controller
NACK	Negative Acknowledgement
NaN	Not a Number
NMR	N-Modular Redundant
NRC	U.S. Nuclear Regulatory Commission
PIF	Power Interface
PLD	Programmable Logic Device
POL	Problem Oriented Language
PP	Protection Packet
PSS	Plant Safety System
PSS-CCP	Plant Safety System Component Control Processor
QAP	Quality Assurance Program
RAM	Random Access Memory
RFI	Radio Frequency Interface
RG	Regulatory Guide
RPP	Reactor Protection Processor
RPS	Reactor Protection System
RT	Reactor Trip
UDP/IP	User Datagram Protocol Internet Protocol

UV-ROM	Ultra-Violet Erasable Programmable Read Only Memory
VDU	Visual Display Unit
V&V	Verification and Validation

1.0 PURPOSE

This document analyzes the MELTAC platform against the applicable requirements of NRC DI&C Interim Staff Guidance (ISG)-04 "Highly-Integrated Control Rooms-Communications Issues (HICRc)". In addition the MELTAC platform is also analyzed against the communication errors defined in NUREG/CR-6991 “Design Practices for Communications and Workstations in Highly Integrated Control Rooms”, Section 2.3 “General Nature of Digital Communication Errors.“ NUREG/CR-6991 Section 2.3 covers the items provided in ISG-04 Section 1, staff position 12 “Communication faults” as well as some additional items.

The analysis identifies areas where the MELTAC platform does and does not comply with the requirements. Corrective actions are identified for areas where the MELTAC platform is not compliant with the requirements.

1.1 Definitions

No special definitions.

1.2 Applicable Standards

- Digital I&C Interim Staff Guidance-04 Highly-Integrated Control Rooms – Communications Issues (ISG-04), Revision 1
- NUREG/CR-6991 Design Practices for Communications and Workstations in Highly Integrated Control Rooms, September 2009

1.3 References

Document name	Document number	Revision
Safety System Digital Platform –MELTAC– Topical Report	JEXU-1041-1008	0

2.0 SCOPE

[

]

2.1 Methodology

[

]

3.0 ANALYSIS RESULTS

The following analyses demonstrate compliance of the MELTAC platform to the NRC staff positions given in DI&C-ISG-04 “Highly-Integrated Control Rooms-Communications Issues (HICRc)” (ISG-04).

The requirements from each staff position are shown along with an analysis of how the MELTAC platform complies with the requirements.

Compliance to some requirements can only be determined at the application level. For these requirements, the analysis may identify examples of compliant MELTAC platform system configurations.

3.1 Analysis of Interdivisional Communications (Section 1 of ISG-04)

This section contains the analysis of the MELTAC platform to the requirements given in ISG-04 Section 1 “Interdivisional Communications” staff positions 1-11 and 13-20. Staff position 12 of ISG-04 Section 1 is discussed in Section 3.2.

The analyses encompass the MELTAC platform Data Link (JEXU-1041-1008, section 4.3.3) and Maintenance Network (JEXU-1041-1008, section 4.3.4).

The MELTAC controller and safety VDU processor are only temporarily connected to the Maintenance Network and are not connected during normal operation (JEXU-1041-1008, Section 4.1.4); therefore the Maintenance Network has no impact on the execution of the safety function. This temporary connection allows for maintenance and trouble shooting. 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 (JEXU-1041-1008, Section 4.3).

As noted in Sections 2.0 and 2.1, communication fault detectability is addressed where applicable.

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

3.1.2 Staff Position 2

Requirement
The safety function of each safety channel should be protected from adverse influence from outside the division of which that channel is a member. Information and signals originating outside the division must not be able to inhibit or delay the safety function. This protection must be implemented within the affected division (rather than in the sources outside the division), and must not itself be affected by any condition or information from outside the affected division. This protection must be sustained despite any operation, malfunction, design error, communication error, or software error or corruption existing or originating outside the division.
Analysis

3.1.3 Staff Position 3

Requirement
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. Receipt of information that does not support or enhance the safety function would involve the performance of functions that are not directly related to the safety function. Safety systems should be as simple as possible. Functions that are not necessary for safety, even if they enhance reliability, should be executed outside the safety system. A safety system designed to perform functions not directly related to the safety function would be more complex than a system that performs the same safety function, but is not designed to perform other functions. The more complex system would increase the likelihood of failures and software errors. Such a complex design, therefore, should be avoided within the safety system. For example, comparison of readings from sensors in different divisions may provide useful information concerning the behavior of the sensors (for example, On-Line Monitoring). Such a function executed within a safety system, however, could also result in unacceptable influence of one division over another, or could involve functions not directly related to the safety functions, and should not be executed within the safety system. Receipt of information from outside the division, and the performance of functions not directly related to the safety function, if used, should be justified. It should be demonstrated that the added system/software complexity associated with the performance of functions not directly related to the safety function and with the receipt of information in support of those functions does not significantly increase the likelihood of software specification or coding errors, including errors that would affect more than one division. The applicant should justify the definition of “significantly” used in the demonstration.
Analysis

3.1.4 Staff Position 4

Requirement
The communication process itself should be carried out by a communications processor[ii] separate from the processor that executes the safety function, so that communications errors and malfunctions will not interfere with the execution of the safety function. The communication and function processors should operate asynchronously, sharing information only by means of dual-ported memory or some other shared memory resource that is dedicated exclusively to this exchange of information. The function processor, the communications processor, and the shared memory, along with all supporting circuits and software, are all considered to be safety-related, and must be designed, qualified, fabricated, etc., in accordance with 10 C.F.R. Part 50, Appendix A and B. Access to the shared memory should be controlled in such a manner that the function processor has priority access to the shared memory to complete the safety function in a deterministic manner. For example, if the communication processor is accessing the shared memory at a time when the function processor needs to access it, the function processor should gain access within a timeframe that does not impact the loop cycle time assumed in the plant safety analyses. If the shared memory cannot support unrestricted simultaneous access by both processors, then the access controls should be configured such that the function processor always has precedence. The safety function circuits and program logic should ensure that the safety function will be performed within the timeframe established in the safety analysis, and will be completed successfully without data from the shared memory in the event that the function processor is unable to gain access to the shared memory.
Analysis

[ii] “Processor” may be a CPU or other processing technology such as simple discrete logic, logic within an FPGA, an Application Specific Integrated Circuit (ASIC), etc.

3.1.5 Staff Position 5

Requirement
The cycle time for the safety function processor should be determined in consideration of the longest possible completion time for each access to the shared memory. This longest-possible completion time should include the response time of the memory itself and of the circuits associated with it, and should also include the longest possible delay in access to the memory by the function processor assuming worst-case conditions for the transfer of access from the communications processor to the function processor. Failure of the system to meet the limiting cycle time should be detected and alarmed.
Analysis

3.1.6 Staff Position 6

Requirement
The safety function processor should perform no communication handshaking and should not accept interrupts from outside its own safety division.
Analysis

3.1.7 Staff Position 7

Requirement
Only predefined data sets should be used by the receiving system. Unrecognized messages and data should be identified and dispositioned by the receiving system in accordance with the pre-specified design requirements. Data from unrecognized messages must not be used within the safety logic executed by the safety function processor. Message format and protocol should be pre-determined. Every message should have the same message field structure and sequence, including message identification, status information, data bits, etc. in the same locations in every message. Every datum should be included in every transmit cycle, whether it has changed since the previous transmission or not, to ensure deterministic system behavior.
Analysis

3.1.8 Staff Position 8

Requirement
Data exchanged between redundant safety divisions or between safety and non-safety divisions should be processed in a manner that does not adversely affect the safety function of the sending divisions, the receiving divisions, or any other independent divisions.
Analysis

3.1.9 Staff Position 9

Requirement
Incoming message data should be stored in fixed predetermined locations in the shared memory and in the memory associated with the function processor. These memory locations should not be used for any other purpose. The memory locations should be allocated such that input data and output data are segregated from each other in separate memory devices or in separate pre-specified physical areas within a memory device.
Analysis

3.1.10 Staff Position 10

Requirement
Safety division software should be protected from alteration while the safety division is in operation. On-line changes to safety system software should be prevented by hardwired interlocks or by physical disconnection of maintenance and monitoring equipment. A workstation (e.g. engineer or programmer station) may alter addressable constants, setpoints, parameters, and other settings associated with a safety function only by way of the dual-processor/shared-memory scheme described in this guidance, or when the associated channel is inoperable. Such a workstation should be physically restricted from making changes in more than one division at a time. The restriction should be by means of physical cable disconnect, or by means of keylock switch that either physically opens the data transmission circuit or interrupts the connection by means of hardwired logic. “Hardwired logic” as used here refers to circuitry that physically interrupts the flow of information, such as an electronic AND gate circuit (that does not use software or firmware) with one input controlled by the hardware switch and the other connected to the information source: the information appears at the output of the gate only when the switch is in a position that applies a “TRUE” or “1” at the input to which it is connected. Provisions that rely on software to effect the disconnection are not acceptable. It is noted that software may be used in the safety system or in the workstation to accommodate the effects of the open circuit or for status logging or other purposes.
Analysis

3.1.11 Staff Position 11

Requirement
Provisions for interdivisional communication should explicitly preclude the ability to send software instructions to a safety function processor unless all safety functions associated with that processor are either bypassed or otherwise not in service. The progress of a safety function processor through its instruction sequence should not be affected by any message from outside its division. For example, a received message should not be able to direct the processor to execute a subroutine or branch to a new instruction sequence.
Analysis

3.1.12 Staff Position 12

Refer to Section 3.2.

3.1.13 Staff Position 13

Requirement
Vital communications, such as the sharing of channel trip decisions for the purpose of voting, should include provisions for ensuring that received messages are correct and are correctly understood. Such communications should employ error-detecting or error-correcting coding along with means for dealing with corrupt, invalid, untimely or otherwise questionable data. The effectiveness of error detection/correction should be demonstrated in the design and proof testing of the associated codes, but once demonstrated is not subject to periodic testing. Error-correcting methods, if used, should be shown to always reconstruct the original message exactly or to designate the message as unrecoverable. None of this activity should affect the operation of the safety-function processor.
Analysis

3.1.14 Staff Position 14

Requirement
Vital communications should be point-to-point by means of a dedicated medium (copper or optical cable). In this context, “point-to-point” means that the message is passed directly from the sending node to the receiving node without the involvement of equipment outside the division of the sending or receiving node. Implementation of other communication strategies should provide the same reliability and should be justified.
Analysis

[iii] “Vital” communications as used herein are communications that are needed to support a safety function. Failure of vital communications could inhibit the performance of the safety function. The most common implementation of vital communications is the distribution of channel trip information to other divisions for the purpose of voting.

3.1.15 Staff Position 15

Requirement
Communication for safety functions should communicate a fixed set of data (called the "state") at regular intervals, whether data in the set has changed or not.
Analysis

3.1.16 Staff Position 16

Requirement
Network connectivity, liveness, and real-time properties essential to the safety application should be verified in the protocol. Liveness, in particular, is taken to mean that no connection to any network outside the division can cause an RPS/ESFAS communication protocol to stall, either deadlock or livelock. (Note: This is also required by the independence criteria of: (1) 10 C.F.R. Part 50, Appendix A, General Design Criteria ("GDC") 24, which states, "interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired."; and (2) IEEE 603-1991 IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations.) (Source: NUREG/CR-6082, 3.4.3)
Analysis

3.1.17 Staff Position 17

Requirement
Pursuant to 10 C.F.R. § 50.49, the medium used in a vital[iii] communications channel should be qualified for the anticipated normal and post-accident environments. For example, some optical fibers and components may be subject to gradual degradation as a result of prolonged exposure to radiation or to heat. In addition, new digital systems may need susceptibility testing for EMI/RFI and power surges, if the environments are significant to the equipment being qualified.
Analysis

[iii] "Vital" communications as used herein are communications that are needed to support a safety function. Failure of vital communications could inhibit the performance of the safety function. The most common implementation of vital communications is the distribution of channel trip information to other divisions for the purpose of voting.

3.1.18 Staff Position 18

Requirement
Provisions for communications should be analyzed for hazards and performance deficits posed by unneeded functionality and complication.
Analysis

3.1.19 Staff Position 19

Requirement
If data rates exceed the capacity of a communications link or the ability of nodes to handle traffic, the system will suffer congestion. All links and nodes should have sufficient capacity to support all functions. The applicant should identify the true data rate, including overhead, to ensure that communication bandwidth is sufficient to ensure proper performance of all safety functions. Communications throughput thresholds and safety system sensitivity to communications throughput issues should be confirmed by testing.
Analysis

3.1.20 Staff Position 20

Requirement
The safety system response time calculations should assume a data error rate that is greater than or equal to the design basis error rate and is supported by the error rate observed in design and qualification testing.
Analysis

3.2 Detectability of Communication Faults

This section describes the analysis of the communication faults identified in Staff Position 12 of ISG-04 Section 1. The analyses encompass the MELTAC platform Data Link (JEXU-1041-1008, section 4.3.3) and Maintenance Network (JEXU-1041-1008, section 4.3.4). These analyses address communication faults at the MELTAC platform level. Application level methods to prevent communication faults from affecting the performance of the safety functions are not described.

Table 3.2-1 Communication Faults Described in NRC Digital I&C ISG-04 Section 1, Staff Position 12

	Fault	Description
1	Message corruption	Messages may be corrupted due to errors in communications processors, errors introduced in buffer interfaces, errors introduced in the transmission media, or from interference or electrical noise.
2	Repeated message	Messages may be repeated at an incorrect point in time.
3	Incorrect message sequence	Messages may be sent in the incorrect sequence.
4	Message reception failure	Messages may be lost, which includes both failures to receive an uncorrupted message or to acknowledge receipt of a message.
5	Delayed message	Messages may be delayed beyond their permitted arrival time window for several reasons, including errors in the transmission medium, congested transmission lines, interference, or by delay in sending buffered messages.
6	Message from unexpected source	Messages may be inserted into the communication medium from unexpected or unknown sources.
7	Message sent to wrong destination	Messages may be sent to the wrong destination, which could treat the message as a valid message.
8	Over-length message	Messages may be longer than the receiving buffer, resulting in buffer overflow and memory corruption.
9	Out-of-range message	Messages may contain data that is outside the expected range.
10	Incorrect data location	Messages may appear valid, but data may be placed in incorrect locations within the message.
11	High rate message	Messages may occur at a high rate that degrades or causes the system to fail (i.e., broadcast storm).
12	Message header/address corruption	Message headers or addresses may be corrupted.

Because a Data Link fault may affect the safety function, additional analyses of communication faults described in Section 2.3 of NUREG/CR-6991 were made for the Data Link, as shown in the next table. Faults related to segmented networks are not analyzed because the Data Link network is not segmented. Fault 20 is not included in NUREG/CR-6991; however it was included because it is a credible communication fault. No additional analysis of Maintenance Network faults was performed because the MELTAC controller and safety VDU processor are only temporarily connected to the Maintenance Network and are not connected during normal operation (JEXU-1041-1008, Section 4.1.4); therefore the Maintenance Network has no impact on the execution of the safety function. 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 (JEXU-1041-1008, Section 4.3)

Table 3.2-2 NUREG/CR-6991 Section 2.3

	Fault	Description
13	Invalid data "masquerading" as valid	Correctly formatted messages are received from an incorrect source that disguises itself as a correct source.
14	Commission fault (babbling idiot)	Messages sent from other nodes are corrupted due to frequent message transmission at incorrect times by a malfunctioning node.
15	Inconsistency	A single failure propagates via the cooperative mechanisms that the N-Modular redundant (NMR) system uses and causes the failure of the entire NMR system.
16	Excessive jitter	Messages arrive at inconsistent times due to network jitter.
17	Data collision	In nondeterministic networks, such as Ethernet, multiple devices may attempt to transmit data at exactly the same time resulting in a collision.
18	Out of synchronization	Messages are missed by the receiver because messages are updated by the sender too early.
19	Incorrect encoding/decoding	Communication is impossible due to inconsistency between the sender (encoding) and receiver (decoding).
20	Interruption	Messages may be interrupted completely or in the middle of data transmission.

3.2.1 Data Link

3.2.2 Engineering (Maintenance) Network

The table below provides an analysis of communication faults from the perspective of the MELTAC controller and safety VDU processor.

The errors in the table are applicable when the MELTAC controller or safety VDU processor is connected to the MELTAC engineering tool (non-safety) via the Maintenance Network. The MELTAC controller and safety VDU processor are only temporarily connected to the Maintenance Network. This temporary connection is under administrative control to ensure that before a MELTAC controller or safety VDU processor are connected to the Maintenance Network it is formally taken out of service with appropriate management of the affected plant technical specifications. This analysis demonstrates how the MELTAC controller and safety VDU processor protect themselves from communications errors on the maintenance network should the maintenance network be inadvertently connected during normal operation.

3.2.3 Safety VDU (Touch Screen to Safety VDU Processor Communications)

The communication link used between the safety VDU touch screen and the safety VDU processor is used only within the same safety division. Therefore, it is not evaluated within the scope of ISG-04, which applies only to interdivisional data communications.

3.2.4 Interdivisional Communication Interface to Power Interface (PIF) Module

For some applications, the PIF Module may receive control inputs from outside its safety division. For example, the PIF Module may receive signals from the Diverse Actuation System (DAS). However, since these are conventional hardwired binary interdivisional signals, they are not subject to the digital communication errors defined in ISG-04. Other aspects of these signals regarding conformance to ISG-04 are analyzed in Section 3.3.5.

3.2.5 Interdivisional Communication Interface for Analog Inputs

For some applications, analog inputs to the safety division may be shared with a non-safety division. Typically, the analog inputs to the RPS are shared with the DAS. These analog signals are distributed prior to the analog to digital converters within the MELTAC Analog Input Modules. Since these are conventional hardwired analog interdivisional signals, they are not subject to the digital communication errors defined in ISG-04. Since the safety division only transmits these signals (i.e. there are no interdivisional analog signals received by the safety system), other ISG-04 requirements are not applicable.

3.3 Analysis of Command Prioritization (Section 2 of ISG-04)

This section provides an analysis of the MELTAC platform command prioritization features. The Staff Positions in ISG-04 Section 2 are used as criteria for this analysis.

The MELTAC platform includes a Power Interface (PIF) Module to implement priority logic. The PIF Module employs state-based priority logic to ensure that either the primary system (e.g. the safety system) or backup system (e.g. the Diverse Actuation System) can place the component in its preferred safety state. This state-based priority logic is implemented on an Interposing Logic (IPL) sub-board mounted on the PIF Module that controls the component in direct response to external contact inputs, independent of the MELTAC controller output commands. There are several types of IPL sub-boards for different types of plant components (e.g.: switchgears, solenoid valves, etc.). Each PIF Module is configured with the appropriate IPL sub-board for the component being controlled. The IPL is realized by discrete logic Integrated Circuits.

3.3.1 Staff Position 1

Requirement
A priority module is a safety-related device or software function. A priority module must meet all of the 10 C.F.R. Part 50, Appendix A and B requirements (design, qualification, quality, etc.) applicable to safety-related devices or software.
Analysis

3.3.2 Staff Position 2

Requirement
Priority modules used for diverse actuation signals should be independent of the remainder of the digital system, and should function properly regardless of the state or condition of the digital system. If these recommendations are not satisfied, the applicant should show how the diverse actuation requirements are met.
Analysis

3.3.3 Staff Position 3

Requirement
Safety-related commands that direct a component to a safe state must always have the highest priority and must override all other commands. Commands that originate in a safety-related channel but which only cancel or enable cancellation of the effect of the safe-state command (that is, a consequence of a Common-Cause Failure in the primary system that erroneously forces the plant equipment to a state that is different from the designated “safe state.”), and which do not directly support any safety function, have lower priority and may be overridden by other commands. In some cases, such as containment isolation valve in an auxiliary feedwater line, there is no universal “safe state”. The valve must be open under some circumstances and closed under others. The relative priority to be applied to commands from a diverse actuation system, for example, is not obvious in such a case. This is a system operation issue, and priorities should be assigned on the basis of considerations relating to plant system design or other criteria unrelated to the use of digital systems. This issue is outside the scope of this ISG. The reasoning behind the proposed priority ranking should be explained in detail. The reviewer should refer the proposed priority ranking and the explanation to appropriate systems experts for review. The priority module itself should be shown to apply the commands correctly in order of their priority rankings, and should meet all other applicable guidance. It should be shown that the unavailability or spurious operation of the actuated device is accounted for in, or bounded by, the plant safety analysis.
Analysis

3.3.4 Staff Position 4

Requirement
A priority module may control one or more components. If a priority module controls more than one component, then all of these provisions apply to each of the actuated components.
Analysis

3.3.5 Staff Position 5

Requirement
Communication isolation for each priority module should be as described in the guidance for interdivisional communications.
Analysis
See the table below for the interdivisional signals typically interfaced to the PIF Module. The numbers in the left column correspond to the Staff Position numbers in ISG-04 Section 1.
Evaluation
Conforms, see the table below.

3.3.6 Staff Position 6

Requirement
Software used in the design, testing, maintenance, etc. of a priority module is subject to all of the applicable guidance in Regulatory Guide 1.152, which endorses IEEE Std. 7-4.3.2-2003 (with comments). This includes software applicable to any programmable device used in support of the safety function of a prioritization module, such as programmable logic devices (PLDs), programmable gate arrays, or other such devices. Section 5.3.2 of IEEE 7-4.3.2-2003 is particularly applicable to this subject. Validation of design tools used for programming a priority module or a component of a priority module is not necessary if the device directly affected by those tools is 100% tested before being released for service. 100% testing means that every possible combination of inputs and every possible sequence of device states is tested, and all outputs are verified for every case. The testing should not involve the use of the design tool itself. Software-based prioritization must meet all requirements (quality requirements, V&V, documentation, etc.) applicable to safety-related software.
Analysis

3.3.7 Staff Position 7

Requirement
Any software program that is used in support of the safety function within a priority module is safety-related software. All requirements that apply to safety-related software also apply to prioritization module software. Nonvolatile memory (such as burned-in or reprogrammable gate arrays or random-access memory) should be changeable only through removal and replacement of the memory device. Design provisions should ensure that static memory and programmable logic cannot be altered while installed in the module. The contents and configuration of field programmable memory should be considered to be software, and should be developed, maintained, and controlled accordingly.
Analysis

3.3.8 Staff Position 8

Requirement
To minimize the probability of failures due to common software, the priority module design should be fully tested (This refers to proof-of-design testing, not to individual testing of each module and not to surveillance testing.). If the tests are generated by any automatic test generation program then all the test sequences and test results should be manually verified. Testing should include the application of every possible combination of inputs and the evaluation of all of the outputs that result from each combination of inputs. If a module includes state-based logic (that is, if the response to a particular set of inputs depends upon past conditions), then all possible sequences of input sets should also be tested. If testing of all possible sequences of input sets is not considered practical by an applicant, then the applicant should identify the testing that is excluded and justify that exclusion. The applicant should show that the testing planned or performed provides adequate assurance of proper operation under all conditions and sequences of conditions. Note that it is possible that logic devices within the priority module include unused inputs: assuming those inputs are forced by the module circuitry to a particular known state, those inputs can be excluded from the "all possible combinations" criterion. For example, a priority module may include logic executed in a gate array that has more inputs than are necessary. The unused inputs should be forced to either "TRUE" or "FALSE" and then can be ignored in the "all possible combinations" testing.
Analysis

3.3.9 Staff Position 9

Requirement
Automatic testing within a priority module, whether initiated from within the module or triggered from outside and including failure of automatic testing features, should not inhibit the safety function of the module in any way. Failure of automatic testing software could constitute common-cause failure if it were to result in the disabling of the module safety function.
Analysis

3.3.10 Staff Position 10

Requirement
The priority module must ensure that the completion of a protective action as required by IEEE Std. 603 is not interrupted by commands, conditions, or failures outside the module's own safety division.
Analysis

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

3.4.3 Staff Position 3.1 - 3.

Requirement
Nonsafety stations controlling the operation of safety-related equipment: Nonsafety stations may control the operation of safety-related equipment, provided the following restrictions are enforced.
Analysis

3.4.4 Staff Position 3.1 - 4.

Requirement

Safety-related stations controlling the operation of equipment in other safety-related divisions:

Safety-related stations controlling the operation of equipment in other divisions are subject to constraints similar to those described above for nonsafety stations that control the operation of safety-related equipment.

- A control station should access safety-related plant equipment outside its own division only by way of a priority module associated with that equipment. Priority modules should be designed and applied as described in the guidance on priority modules.
- A station must not influence the operation of safety-related equipment outside its own division when that equipment is performing its safety function. This provision should be implemented within the affected (target) safety-related system, and should be unaffected by any operation, malfunction, design error, software error, or communication error outside the division of which those controls are a member. In addition:
  - The extra-divisional (that is, “outside the division”) control station should be able to bypass a safety function only when the affected division itself determined that such action would be acceptable.
  - The extra-divisional station should not be able to suppress any safety function. (If the safety system itself determines that termination of a safety command is warranted as a result of the safety function having been achieved, and if the applicant demonstrates that the safety system has all information and logic needed to make such a determination, then the safety command may be reset from a source outside the safety division. If operator judgment is needed to establish the acceptability of resetting the safety command, then reset from outside the safety division is not acceptable because there would be no protection from inappropriate or accidental reset.)
  - The extra-divisional station should not be able to bring a safety function out of bypass condition unless the affected division has itself determined that such action would be acceptable.

Analysis

3.4.5 Staff Position 3.1 - 5

Requirement
Malfunctions and Spurious Actuations: The result of malfunctions of control system resources (e.g., workstations, application servers, protection/control processors) shared between systems must be consistent with the assumptions made in the safety analysis of the plant. Design and review criteria for complying with these requirements, as set forth in 10 C.F.R. § 50.34 and 50.59, include but are not limited to the following:
Analysis

No.	Requirement		
1	Control processors that are assumed to malfunction independently in the safety analysis should not be affected by failure of a multidivisional control and display station.		

No.	Requirement		
2	Control functions that are assumed to malfunction independently in the safety analysis should not be affected by failure of a single control processor.		
3	Safety and control processors should be configured and functionally distributed so that a single processor malfunction or software error will not result in spurious actuations that are not enveloped in the plant design bases, accident analyses, ATWS provisions, or other provisions for abnormal conditions. This includes spurious actuation of more than one plant device or system as a result of processor malfunction or software error. The possibility and consequences of malfunction of multiple processors as a result of common software error must be addressed.		

No.	Requirement		
4	No single control action (for example, mouse click or screen touch) should generate commands to plant equipment. Two positive operator actions should be required to generate a command. For example: When the operator requests any safety function or other important function, the system should respond “do you want to proceed?” The operator should then be required to respond “Yes” or “No” to cause the system to execute the function. Other question-and-confirm strategies may be used in place of the one described in the example. The second operation as described here is to provide protection from spurious actuations, not protection from operator error. Protection from operator error may involve similar but more restrictive provisions, as addressed in guidance related to Human Factors.		
5	Each control processor or its associated communication processor should detect and block commands that do not pass the communication error checks.		

No.	Requirement		
6	Multidivisional control and display stations should be qualified to withstand the effects of adverse environments, seismic conditions, EMI/RFI, power surges, and all other design basis conditions applicable to safety-related equipment at the same plant location. This qualification need not demonstrate complete functionality during or after the application of the design basis condition unless the station is safety-related. Stations which are not safety-related should be shown to produce no spurious actuations and to have no adverse effect upon any safety-related equipment or device as a result of a design basis condition, both during the condition and afterwards. If spurious or abnormal actuations or stoppages are possible as a result of a design basis condition, then the plant safety analyses must envelope those spurious and abnormal actuations and stoppages. Qualification should be supported by testing rather than by analysis alone. D3 considerations may warrant the inclusion of additional qualification criteria or measures in addition to those described herein.		
7	Loss of power, power surges, power interruption, and any other credible event to any operator workstation or controller should not result in spurious actuation or stoppage of any plant device or system unless that spurious actuation or stoppage is enveloped in the plant safety analyses.		

No.	Requirement		
8	The design should have provision for an “operator workstation disable” switch to be activated upon abandonment of the main control room, to preclude spurious actuations that might otherwise occur as a result of the condition causing the abandonment (such as control room fire or flooding). The means of disabling control room operator stations should be immune to short-circuits, environmental conditions in the control room, etc. that might restore functionality to the control room operator stations and result in spurious actuations.		
9	Failure or malfunction of any operator workstation must not result in a plant condition (including simultaneous conditions) that is not enveloped in the plant design bases, accident analyses, and anticipated transients without scram (ATWS) provisions, or in other unanticipated abnormal plant conditions.		

3.5 Analysis of Message Field Failures in the Data Link

This section describes the analysis of the communication fault "incorrect data location" identified in Staff Position 12 of ISG-04 Section 1 (see Section 3.2). The analysis encompasses the MELTAC platform Data Link (JEXU-1041-1008, section 4.3.3). This analysis addresses communication faults at the MELTAC platform level.

Figure 3.5-1 describes the message format used in the Data Link.

Table 3.5-1 describes the function of each field in the Data Link message. The first column gives the name of the message field, the second column gives the definition of the field value as set by the transmitter, the third column describes the action of the receiver for normal conditions and the fourth column give the values the message field may take.

Table 3.5-2 provides an analysis of possible errors for each field in the Data Link message. See Section 3.5.2 for a description of each column in the table.

3.5.1 Message Format

Figure 3.5-1 Message Format of Process Signal (Data Link)

Table 3.5-1 Message Field Explanation of Process Signal through the Data Link

3.5.2 Analysis of Message Feld Errors

An analysis was conducted, for each message field described in Section 3.5.1, to determine if possible invalid data patterns can be detected, and if not, how the controller would be affected.

This analysis covers the case where the content of each field in the outgoing message is corrupted before the CRC is added. (Any corruption of fields after the CRC is added is not covered because the message will be discarded by the receiving node due to a CRC error and will not affect the receiver.)

Table 3.5-2 below documents the analysis of the possible errors for each field in the Data Link message. The first column gives the name of the message field, the second column gives the possible message field error, the third column describes the check done at the receiver to detect the error, the fourth column gives the impact on the application when the possible error occurs and the fifth column provides an analysis of the impact of the error. In the cases where action is required as a result of the analysis, the action is described.

Table 3.5-2 Message Field Analysis Result of Process Signal through the Data Link

4.0 CONCLUSIONS

This analysis demonstrates that the MELTAC platform complies with the applicable requirements (see Section 2). The MELTAC platform compliance with each requirement is shown within the tables located in Section 3.

The analysis also identifies requirements that are fulfilled at the application level, but does not address compliance to these requirements.