MELTAC Platform Basic Software Safety Report

Non Proprietary Version

March 2010

© 2010 MITSUBISHI ELECTRIC CORPORATION
All Rights Reserved

Prepared:	Yasunobu Koga Yasunobu Koga, Manager DCS Development Section	03/26/2010 Date
Reviewed:	Makoto Ito Makoto Ito, Manager DCS Development Section	03/26/2010 Date
Approved:	Kentaro Sadayuki Kentaro Sadayuki, Section Manager Development Quality Control Section	03/29/2010 Date

Signature History

	Rev.0	Rev.1
Prepared	Tomonori Yamane	Yasunobu Koga
Reviewed	Makoto Ito	Makoto Ito
Approved	Shigeo Ueno	Masahiko Nambu

Revision History

Revision	Date	Page (section)	Description
0	February 2007	All	Original issued
1	October 2009	All	● MELCO reflected the result of NRC audit "Audit of MHI Documents in support of the MELTAC platform safety evaluation" in September 2008. NRC ISG-04 Sections 1, 2, and 3.1 on Digital I&C were added to the criteria for communication analysis. ● Self-Diagnosis Functions were added to the analysis. ● Post-Development Procedures were added to the analysis.
2	March 2010	All	The document title is modified to "MELTAC Platform Basic Software Safety Report".
		1 (Sec.1)	Description of purpose is modified for MELTAC Platform.
		(Sec.1.2)	"MELTAC Basic Platform Software Program" is added for reference document. "US-APWR Software Safety Plan" is deleted.
		2 (Sec.2.1)	Description of Potential Hazard is modified.
		3 (Sec.2.2)	Description of Acceptance Criteria is modified.
		9 (Sec.3.2.4)	Description of Evaluation is modified.
		35 (Sec.3.4.1)	Description of Evaluation is modified.
		39 (Sec.3.4.6)	Description of Evaluation is modified.
		(Sec.3.4.7)	Description of Analysis and Evaluation is modified.
		56 (Sec.3.6.2)	Description of EXM is added in Table3.6-2C.

Revision	Date	Page (section)	Description
2	March 2010	61 (Sec.3.6.4)	Description of ECC is added in Table 3.6-4B.
		63 (Sec.3.6.4)	PCI bus is changed into FutureBUS+ in Table 3.6-4D.
		65 (Sec.3.6..5)	PCI bus is changed into FutureBUS+ in Table 3.6-5A.
		66 (Sec 3.6.5)	Description of L bus is added in Table 3.5-5B.
		67 (Sec 3.6.6)	Numbering error is corrected. (Table 3.6-4A -> Table 3.6-6A)
		77 (Sec 3.6.12)	Numbering error is corrected. (Table 3.6.12A -> Table 3.6.12B)
		81 (Sec.3.7.2)	Description of Operation Phase is modified.

Table of Contents

1. Purpose 1
1.1. Definition 1
1.2. Reference Document-Applicable Standard 1
2. Scope 2
2.1. Analysis Target 2
2.2. Analysis Criteria 3
3. Software Safety Analysis Result 4
3.1. Detectability of Input, Operation, and Output hazards 4
3.2. Analysis of Inter-divisional Communications 6
3.2.1. ISG-04 1.1 6
3.2.2. ISG-04 1.2 6
3.2.3. ISG-04 1.3 7
3.2.4. ISG-04 1.4 8
3.2.5. ISG-04 1.5 9
3.2.6. ISG-04 1.6 9
3.2.7. ISG-04 1.7 10
3.2.8. ISG-04 1.8 10
3.2.9. ISG-04 1.9 11
3.2.10. ISG-04 1.10 11
3.2.11. ISG-04 1.11 12
3.2.12. ISG-04 1.12 13
3.2.13. ISG-04 1.13 13
3.2.14. ISG-04 1.14 13
3.2.15. ISG-04 1.15 13
3.2.16. ISG-04 1.16 13
3.2.17. ISG-04 1.17 13
3.2.18. ISG-04 1.18 15
3.2.19. ISG-04 1.19 15
3.2.20. ISG-04 1.20 16
3.3. Detectability of Communication Faults 17
3.3.1. Control Network 18
3.3.2. Data Link 23
3.3.3. Engineering (Maintenance) Network 27
3.3.4. Safety VDU (Touch screen to S-VDU processor communication) 32
3.4. Analysis of Command Prioritization 35
3.4.1. ISG-04 2.1 35
3.4.2. ISG-04 2.2 35
3.4.3. ISG-04 2.3 36
3.4.4. ISG-04 2.4 36
3.4.5. ISG-04 2.5 36
3.4.6. ISG-04 2.6 38
3.4.7. ISG-04 2.7 39
3.4.8. ISG-04 2.8 40
3.4.9. ISG-04 2.9 40
3.4.10. ISG-04 2.10 41
3.5. Analysis of Multi-divisional Control and Display Stations 42
3.5.1. ISG-04 3.1.1 42
3.5.2. ISG-04 3.1.2 42
3.5.3. ISG-04 3.1.3 42
3.5.4. ISG-04 3.1.4 44
3.5.5. ISG-04 3.1.5 44

3.6. Analysis of Self-Diagnosis Functions 49
3.6.1. CPU Module 49
3.6.2. System Management Module (SMM) 54
3.6.3. Bus Master Module 57
3.6.4. Control Network I/F Module 60
3.6.5. FMU Module 65
3.6.6. Touch Panel Interface Module 67
3.6.7. Safety VDU Panel 69
3.6.8. Analog Input Module 70
3.6.9. Analog Output Module 72
3.6.10. Digital Input Module 74
3.6.11. Digital Output Module 75
3.6.12. PIF Module 76
3.6.13. Repeater Module 78
3.6.14. Power Supply Module 79
3.6.15. Controller Cabinet 80
3.7. Analysis of Post-Development Procedures 81
3.7.1. Production phase 81
3.7.2. Operation phase 81
3.7.3. Maintenance phase 82
4. Analysis Summary 83
Appendix A. Thread Audit of the V&V activities 84
Appendix B. Referenced Documentation 88

1. Purpose

This document reports the results of a specific software safety analysis activity for the MELTAC Platform Basic Software according to the Software Safety Plan (SSP) in the [JEXU-1012-1132] “MELTAC Platform Basic Software Program Manual”.

The specific activity addressed in this software safety analysis is identification and analysis of potential hazards that may adversely affect critical platform functions. This analysis assesses the effectiveness of mitigating platform level design features which ensure the hazards are correctly detected and the platform responds as specified.

As defined in the “MELTAC Platform Basic Software Program Manual”, other platform level software safety analysis activities are within the scope of Verification and Validation (V&V). This includes review by the V&V Team of each of the principal design documents to ensure identification and traceability of critical platform functions from specification to testing.

The software safety analysis activities conducted for the MELTAC Platform Basic Software are supplemented by the software safety analysis activities conducted for critical application level functions, as defined by the applicable project Application Software Software Program Manual.

1.1. Definition

No special definitions.

1.2. Reference Document-Applicable Standard

- NPD Procedure **[ ]**
- [JEXU-1012-1132] “MELTAC Platform Basic Software Program Manual”
- Digital I&C Interim Staff Guidance-04 Highly-Integrated Control Rooms – Communications Issues (ISG-04)

2. Scope

2.1. Analysis Target

The following table identifies the major hazards for the MELTAC Basic Software, which have the possibility to interfere with correct system operation.

Table 2.1-1 Potential Hazards

2.2. Analysis Criteria

The potential hazards noted in Table 2.1-1 will be checked against the following criteria.

Table 2.2-1 Acceptance Criteria

[

]

3. Software Safety Analysis Result

We analyzed if faults can be detected at the architecture level.

If detection was done by software, its implementation was confirmed through verification of specification document and source code. The Analysis column in the tables below describes the method of tolerating the hazard, and the specific section(s) of the document(s) which identify this tolerance method.

Compliance to some requirements is determined through the application system configuration or application software. For these requirements, the analysis identifies example(s) of the compliance method(s), without identifying specific documentation. The documentation reference is application specific.

3.1. Detectability of Input, Operation, and Output hazards

The results of analyzing the detectability of input, operation, and output hazards are as follows.

For input from the network, refer to Sec.3.2 through 3.5.

3.2. Analysis of Inter-divisional Communications

The results of analyzing the interdivisional communication are as follows. This section is applicable to the Data Link, Control Network (ie. Unit Bus and Safety Bus in the PSMS/PCMS) and Maintenance Network. Inter-division communication for the PIF module is discussed in Sec. 3.4.5.

As noted in section 2.2, Staff Positions from ISG-04 Section 1 are used as criteria.

3.2.1. ISG-04 1.1

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.

3.2.2. ISG-04 1.2

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.

3.2.3. ISG-04 1.3

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.

3.2.4. ISG-04 1.4

Requirement
The communication process itself should be carried out by a communications processor 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.

3.2.5. ISG-04 1.5

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.

3.2.6. ISG-04 1.6

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

3.2.7. ISG-04 1.7

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.

3.2.8. ISG-04 1.8

Requirement
Data exchanged between redundant safety divisions or between safety and nonsafety 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.

3.2.9. ISG-04 1.9

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.

3.2.10. ISG-04 1.10

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.

3.2.11. ISG-04 1.11

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.

3.2.12. ISG-04 1.12

Refer to section 3.3.

3.2.13. ISG-04 1.13

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.

3.2.14. ISG-04 1.14

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.

3.2.15. ISG-04 1.15

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.

3.2.16. ISG-04 1.16

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)

3.2.17. ISG-04 1.17

Requirement
Pursuant to 10 C.F.R. § 50.49, the medium used in a Vital 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.

3.2.18. ISG-04 1.18

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

3.2.19. ISG-04 1.19

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.

3.2.20. ISG-04 1.20

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.

3.3. Detectability of Communication Faults

The results of analyzing the detectability of communication faults (network input hazards) using ISG-04 Staff position 1.12 as criteria are noted in this section. The subsections below analyze each communication type.

Table 3.3-1 Communication faults described in NRC Digital I&C ISG-04 Staff position 1.12

	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 messages	Messages may be repeated at an incorrect point in time.
3	Incorrect sequence of messages	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	Wrong destination message	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 data	Messages may contain data that is outside the expected range.
10	Incorrect location of data	Messages may appear valid, but data may be placed in incorrect locations within the message.
11	High rate message occurrence	Messages may occur at a high rate that degrades or causes the system to fail (i.e., broadcast storm).
12	Header / address corruption	Message headers or addresses may be corrupted.

3.3.1. Control Network

[

]

3.3.2. Data Link

3.3.3. Engineering (Maintenance) Network

The table below analyzes message errors only from the perspective of the safety controller, not the Engineering Tool.

3.3.4. Safety VDU (Touch screen to S-VDU processor communication)

[

]

3.4. Analysis of Command Prioritization

The results of analyzing the command prioritization are as follows. It is noted that in MELTAC there are two priority logic functions. One is in the function processor which prioritizes safety commands over non-safety commands received via the Unit Bus (eg. from the PCMS). The second is within the PIF module which employs state based priority logic to ensure that either the primary system or the backup system can put the component in its preferred safety state.

As noted in section 2.2, Staff Positions from ISG-04 Section 2 are used as criteria.

3.4.1. ISG-04 2.1

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.

3.4.2. ISG-04 2.2

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.

3.4.3. ISG-04 2.3

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. <abbreviated> 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.

3.4.4. ISG-04 2.4

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.

3.4.5. ISG-04 2.5

Requirement
Communication isolation for each priority module should be as described in the guidance for interdivisional communications.

3.4.6. ISG-04 2.6

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 Standard 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. <abbreviated> 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.

3.4.7. ISG-04 2.7

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.

3.4.8. ISG-04 2.8

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. <abbreviated>

3.4.9. ISG-04 2.9

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.

3.4.10. ISG-04 2.10

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

3.5. Analysis of Multi-divisional Control and Display Stations

The results of analyzing the command prioritization are as follows.
As noted in section 2.2, Staff Positions from ISG-04 Section 3.1 are used as criteria.

3.5.1. ISG-04 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.

3.5.2. ISG-04 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.

3.5.3. ISG-04 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.

No.	Requirement
1	The nonsafety station should access safety-related plant equipment 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.
2	A nonsafety station should not affect the operation of safety-related equipment when the safety-related equipment is performing its safety function. This provision should be implemented within the safety-related system, and must be unaffected by any operation, malfunction, design error, software error, or communication error in the nonsafety equipment.
3	The nonsafety station should be able to bypass a safety function only when the affected division has itself determined that such action would be acceptable.
4	The nonsafety station should not be able to suppress any safety function.
5	The nonsafety 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.

3.5.4. ISG-04 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. <Details abbreviated. See the ISG-04 document.>

3.5.5. ISG-04 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:

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.
2	Control functions that are assumed to malfunction independently in the safety analysis should not be affected by failure of a single control processor.

No.	Requirement
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.
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.
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.

No.	Requirement
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.

3.6. Analysis of Self-Diagnosis Functions

The results of analyzing the self-diagnosis functions are as follows.

3.6.1. CPU Module

3.6.2. System Management Module (SMM)

3.6.3. Bus Master Module

3.6.4. Control Network I/F Module

3.6.5. FMU Module

3.6.6. Touch Panel Interface Module

3.6.7. Safety VDU Panel

3.6.8. Analog Input Module

3.6.9. Analog Output Module

3.6.10. Digital Input Module

3.6.11. Digital Output Module

3.6.12. PIF Module

3.6.13. Repeater Module

3.6.14. Power Supply Module

3.6.15. Controller Cabinet

3.7. Analysis of Post-Development Procedures

[

]

3.7.1. Production phase

3.7.2. Operation phase

3.7.3. Maintenance phase

4. Analysis Summary

[

]

Appendix A. Thread Audit of the V&V activities

[

]

Appendix B. Referenced Documentation

The following table is a list of specification documentation referenced in this analysis.