US-APWR

Response Time of Safety I&C System

Non Proprietary Version

April 2011

Revision History

Revision	Date	Page (Section)	Description
0	October 2009	All	Original issued
1	April 2010	1, 4, 5, 7	Editorial correction.
		4 (3.2 (1))	Added "The response time of control rod drop is described in DCD Subsection 15.0.0.2.5." at the end of the paragraph. Added the description of T_5 (Rod Drop) in Figure 3.2-1.
		5 (3.3)	Corrected the scope of T_3 & H in Figure 3.3-1.
		7 (3.4)	Added the Assumption associated with Tables 4.2-1 and 4.2-2 in Section 3.4" Assumptions for Response Time of Safety I&C System".
		8 (4.0) (4.1)	Transferred Section 4.0 of revision 0 to section 4.1 "Response Time Requirement for RT and ESF System" and corrected figure number. Added Section 4.0 "ALLOCATED RESPONSE TIMES".
		9 (4.2)	Added new section 4.2 "Response Time Allocation and Basis" which represent response time allocation based on equipment specification and supplier and model of equipment.
		17 (5.0) (5.1) (5.2) (5.3)	Replaced section 5.0 "REFERENCES" with new section 5.0 "BASIS FOR ELIMINATION OF SURVEILLANCE TESTS" and followed subsections which represent justification of test elimination for transmitters, NIS and RCP speed.
		19 (6.0)	Transferred section 5.0 "REFERENCES" to section 6.0 and updated the description of the reference documents [1] & [2] to the latest version and added reference document [4] & [5].
2	April 2011	General	Editorial correction.

Revision	Date	Page (Section)	Description
2 (Continued)		7 (3.4)	Revised to follow the response to RAI 593-4565 Question 07-21 BTP-1. ・ Removed 5th bullet. ・ Revised 6th bullet. ・ Added 7th bullet.
		10 (4.2)	Revised to follow the response to RAI 593-4565 Question 07-21 BTP-1. ・ Revised the description of 3rd paragraph. ・ Added 4th paragraph.
		11-17 (4.2)	Removed column "Basis for Elimination of Surveillance" from Table 4.2-1 and 4.2-2.
		18 (4.2.1)	Added Section 4.2.1 to follow the response to RAI 593-4565 Question 07-21 BTP-1.
		18-27 (4.2.2)	Added Section 4.2.2 to follow the response to RAI 593-4565 Question 07-21 BTP-1 and BTP-2.
		28 (5.0)	Revised the description of 2nd paragraph, reflecting revision of Table 4.2-1 and 4.2-2.
		30 (6.0)	Updated reference document to latest version. Added JEXU-1015-1009 to reference document.
		33 (A.4)	Added 4th paragraph in "Conformance" to follow the response to RAI 593-4565 Question 07-21 BTP-3.
		35 (A.6)	Revised 1st paragraph in "Conformance" to follow the response to RAI 593-4565 Question 07-21 BTP-2.

Mitsubishi Heavy Industries, Ltd.
16-5, Konan 2-chome, Minato-ku
Tokyo 108-8215 Japan

Abstract

This technical report describes the response time for the safety instrumentation and control (I&C) system of the US-APWR. This report relates to performance requirements of the safety I&C system presented in US-APWR Design Control Document (DCD) (Reference 1) Section 7.9 "Data Communication Systems" and to describe the conformance to BTP 7-21.

In reactor trip (RT) system, which is categorized in the safety I&C system of the US-APWR, the response time of the I&C system is defined to be the time needed for a sensor to detect abnormal process value, control system to process the signal, reactor trip breaker (RTB) to open, and the release of control rods by control rod drive mechanism (CRDM). Similarly, in engineered safety features (ESF) actuation system, the response time of the I&C system is defined to be the time needed for a sensor to detect abnormal process value and an actuation signal to be sent out from I&C equipment to a component. The response times in RT and ESF systems are required to be within certain ranges determined by the safety analysis, and these I&C systems need to be designed to satisfy the response time requirements from the safety analysis.

In this document, the response times in RT system and ESF system of the US-APWR are defined, which are followed by their system configurations. Then, the response time of analytical limit from safety analysis is allocated to the individual component of I&C system (i.e., response time of sensor, digital controller). The allocated response time is the response time requirement of the safety I&C system. Then, response time analysis of the safety I&C system is conducted, verifying that the safety I&C system functions in real time and achieves its objectives within the analytical limit of the response time set forth in the safety analysis.

The digital I&C system of the US-APWR adopts the MELTAC platform. Since the MELTAC platform utilizes system modules that cyclically process data, the response times depend on the asynchronous timing of data input and module processing. The configuration and load of input/output (I/O) and central processing unit (CPU) Module of MELTAC platform is designed to meet the digital controller response time described in this document considering the asynchronous sequential processing within each module.

This document also describes conformance of the safety I&C system of US-APWR to BTP 7-21, which requires real-time performance, as presented in Appendix A.

Table of Contents

List of Tables
List of Figures
List of Acronyms

1.0 INTRODUCTION 1
1.1 Purpose 1
1.2 Scope 1
2.0 CODES AND STANDARDS 2
3.0 SYSTEM DESCRIPTION 3
3.1 Safety Functions Credited in Safety Analysis 3
3.2 Definitions of Response Time of Safety I&C System 3
3.3 Signal Pass of Safety I&C System for RT and ESF Actuation 5
3.4 Basis for Response Time of Safety I&C System 7
4.0 ALLOCATED RESPONSE TIMES 8
4.1 Response Time Requirement for RT and ESF System 8
4.2 Basis for Response Time Allocations 10
4.2.1 Basis for Response Time Allocations for Sensors, RTBs and CRDMs 18
4.2.2 Basis for Response Time Allocations for Digital Controller 18
5.0 BASIS FOR ELIMINATION OF SURVEILLANCE TESTS 28
5.1 Transmitters 28
5.2 NIS 29
5.3 RCP Speed 29
6.0 REFERENCES 30
Appendix A Conformance to BTP 7-21 31
A.1 Limiting Response Times 31
A.2 Digital Computer Timing Requirements 31
A.3 Architecture 32
A.4 Design Commitments 33
A.5 Performance Verification 34
A.6 Use of Cyclic Real-Time Executive 34
A.7 Use of Part-Scale Prototypes 35

List of Tables

Table 4.1-1	Allocated Response Time of Reactor Trip	…8
Table 4.1-2	Allocated Response Time of ESF Actuation	…9
Table 4.2-1	Response Time Allocation for Reactor Trip and Basis	…11
Table 4.2-2	Response Time Allocation for ESF Actuation and Basis	…15
Table 4.2-3	The System Scale Applied to The estimation of maximum response times	…23
Table 4.2-4	Response Time Calculation for Maximum, Minimum and Safety Evaluation in Each Component	…24

List of Figures

Figure 3.2-1	Breakdown Response Time for Reactor Trip	…4
Figure 3.2-2	Breakdown Response Time for ESF Actuation	…4
Figure 3.3-1	Signal Pass of Reactor Trip	…5
Figure 3.3-2	Signal Pass of ESF Actuation	…6
Figure 4.2-1	System Configuration of Case 1	…20
Figure 4.2-2	System Configuration of Case 2	…21
Figure 4.2-3	System Configuration of Case 3	…22

List of Acronyms

AI	analog input
BTP	Branch Technical Position
CPU	central processing unit
CRDM	control rod drive mechanism
DCD	Design Control Document
DI	digital input
DO	digital output
DSP	digital signal processer
ECCS	emergency core cooling system
ESF	engineered safety features
ESFAS	engineered safety features actuation system
FET	field effect transistor
FPGA	Field Programmable Gate Array
GDC	General Design Criteria
I&C	instrumentation and control
I/F	interface
I/O	input/output
IEEE	Institute of Electrical and Electronics Engineers
IR	intermediate range
ITAAC	inspections, tests, analyses, and acceptance criteria
MHI	Mitsubishi Heavy Industries, Ltd.
NIS	nuclear instrumentation system
NRC	U.S. Nuclear Regulatory Commission
NUREG	NRC Technical Report Designation (Nuclear Regulatory Commission)
PAM	post accident monitoring
PIF	power interface
PSMS	protection and safety monitoring system
RCP	reactor coolant pump
RPS	reactor protection system
RT	reactor trip
RTB	reactor trip breaker
SLS	safety logic system
SR	source range
SRP	Standard Review Plan

1.0 INTRODUCTION

1.1 Purpose

The purpose of this document is to demonstrate that the overall response time of the US-APWR safety I&C system functions can be implemented within the time delays assumed in the safety analysis of the US-APWR.

In order to show response times, system description and configuration of the safety I&C system is addressed first. Then the allocated response times of individual components and the total response time assumed in the safety analysis, in accordance with the system configuration of the safety I&C system are discussed.

In addition, conformance of the safety I&C system of US-APWR to BTP 7-21, which requires the realization of real-time performance of digital computers, is shown.

1.2 Scope

The scope of this document includes the response time of the safety I&C system of the US-APWR, which consists of the response times of reactor trip (RT) system and engineered safety features (ESF) system, and showing conformance to BTP 7-21.

The allocated response time of the I&C system in this document is the result of the basic design phase of I&C system. This is the response time requirement for the components that will be procured and designed during the detailed design phase. For RT system, the response time from the detection of process value by a sensor till the release of control rods by control rod drive mechanism (CRDM) is considered. Similarly, for ESF system the response time from the detection of process value by a sensor till the sending-out of an ESF actuation signal from the I&C system to a component is considered. The response time of the control equipment such as motor contactor or switchgear is excluded in the response time of I&C system of ESF system in this document. In this document, the response time of the I&C system is addressed against the safety requirement from safety functions credited in the safety analysis, which are RT functions and ESF functions mentioned in DCD (Reference 1) Table 7.2-3 and 7.3-4 in Section 7.2 and 7.3 and credited in safety analysis in Chapter 15 Table 15.0-4. Specific systems, components, or modules of the response time with respect to a signal for achieving each safety function will be explained in Section 3.3.

2.0 CODES AND STANDARDS

This section lists the applicable or reference codes, standards and guidance which establish the basis for the US-APWR response time of safety I&C system. The General Design Criterion (GDC) is listed in order to show the view of overall requirements for the response time while these criteria are also addressed in the US-APWR DCD and the Safety I&C Technical Report (Reference 2) as the compliance commitment for the response time:

(1) "GDC 10, Reactor Design", 10CFR50 appendix A.

(2) "GDC 13, Instrumentation and Control", 10CFR50 appendix A.

(3) "GDC 20, Protection System Functions", 10CFR50 appendix A.

(4) "GDC 29, Protection Against Anticipated Operational Occurrences", 10CFR50 appendix A.

(5) "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants", RG 1.152, Revision 2.

(6) "Data Communications", NUREG/CR-6082.

(7) "Reviewing Real-Time Performance and Its Application of Nuclear Reactor Safety Systems", NUREG/CR-6083.

(8) "Guidance on Digital Computer Real-Time Performance", SRP BTP 7-21.

(9) "IEEE Standard for Software Verification and Validation", IEEE Std. 1012-1998.

(10) "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations", IEEE Std. 7-4.3.2-2003.

3.0 SYSTEM DESCRIPTION

3.1 Safety Functions Credited in Safety Analysis

In this document, the response time of the I&C system is addressed against the safety requirement from safety functions credited in the safety analysis, which are RT functions and ESF functions mentioned in DCD (Reference 1) Table 7.2-3 and 7.3-4 in Section 7.2 and 7.3 and credited in safety analysis in Chapter 15 Table 15.0-4. RT signals and ESF actuation signals to be described are listed as follows.

(1) RT functions
- High Power Range Neutron Flux (low setpoint) RT
- High Power Range Neutron Flux (high setpoint) RT
- Over Temperature ΔT RT
- Over Power ΔT RT
- Low Reactor Coolant Flow RT
- Low Reactor Coolant Pump Speed RT
- High Pressurizer Pressure RT
- Low Pressurizer Pressure RT
- Low Steam Generator Water Level RT
- High-High Steam Generator Water Level RT
- High Pressurizer Water Level RT
- Emergency Core Cooling System (ECCS) Signal RT

(2) ESF actuation functions
- ECCS Signal
  - Low Main Steam Line Pressure
  - Low Pressurizer Pressure
  - High Containment Pressure
- Main Steam Line Isolation Signal
  - Low Main Steam Line Pressure
  - High-High Containment Pressure
- Containment Spray Signal
  - High-3 Containment Pressure
- Emergency Feedwater Actuation
  - Low Steam Generator Water Level
- Emergency Feedwater Isolation Signal
  - Low Main Steam Line Pressure
  - Coincidence of High Steam Generator Water Level and RT

3.2 Definitions of Response Time of Safety I&C System

Response time is defined as delay time caused by components in which the signal of I&C system is processed. The followings show breakdown response time of RT and ESF systems.

(1) Response time of RT

Response time of I&C system in RT is broken down to each delay time from process value reach setpoint until control rods are released by the CRDM. Refer to the Safety I&C Technical Report (Reference 2) Section 6.5.3 for the breakdown response time for RT. This document repeats the description of the Safety I&C Technical Report (Reference 2) for better understanding of the response time. It is noted that the response time of control rod drop is excluded from this report, because that response time is outside the scope of the I&C system discussed in this document. The response time of control rod drop is described in DCD (Reference 1) Subsection 15.0.0.2.5.

Figure 3.2-1 Breakdown Response Time for Reactor Trip

(2) Response time of ESF actuation
Response time of ESF actuation is broken down to delay time as the following in each process from process value reach setpoint until ESF actuation signal is generated.

Figure 3.2-2 Breakdown Response Time for ESF Actuation

3.3 Signal Pass of Safety I&C System for RT and ESF Actuation

This section describes signal pass in the safety I&C systems which are required to consider response time of RT and ESF actuation based on system configuration. For the overall I&C system, system configuration of RT system and ESF system, refer to DCD (Reference 1) 7.1, 7.2, 7.3 for more detail.

(1) Signal pass of RT and associated configuration of equipment

Figure 3.3-1 Signal Pass of Reactor Trip

A signal from the sensor, which has detected a variation of the process parameter, is sent to the processing part of reactor protection system (RPS) through the input part of RPS and is subjected to the bistable. Then, the signal from the bistable is sent to the processing part of RPS of other train via data links and is subjected to the 2-out-of-4 voting logic with signals of other three trains. Then, the signal from the 2-out-of-4 voting logic is subjected to the logical addition with signals for other trip conditions and is sent as a RT signal from the output part of the RPS. Then, the RT signal from the output part of RPS is sent to RTB. Finally, when RTB opens, CRDM release the control rods.

(2) Signal pass of ESF actuation and associated configuration of equipment

Figure 3.3-2 Signal Pass of ESF Actuation

A signal from the sensor, which has detected a variation of the process parameter, is sent out to the processing part of RPS through the input part and is subjected to the bistable. Then, the signal from the bistable is sent out to the processing module of RPS of other train via data links and is subjected to the 2-out-of-4 voting logic with signals of other three trains. Then, the signal from the 2-out-of-4 voting logic is sent out to engineered safety features actuation system (ESFAS) via data links and is again subjected to the 2-out-of-4 voting logic in ESFAS. Then, the signal from the 2-out-of-4 voting logic is sent out as an ESF actuation signal from ESFAS. The ESF actuation signal sent out from ESFAS then enters safety logic system (SLS) through the safety bus. This signal is subjected to the logical addition with signals sent out under other ESF actuation conditions and is sent out from the Power Interface (PIF) Module of SLS to the component.

3.4 Basis for Response Time of Safety I&C System

In this document, the following bases are made for the response time evaluation.

4.0 ALLOCATED RESPONSE TIMES

4.1 Response Time Requirement for RT and ESF System

The allocated response times for the RT signal and the ESF actuation signal are shown in Tables 4.1-1 and 4.1-2, respectively. These allocations establish the response time requirement for each component. It can be seen that the total response times for the safety I&C system is equivalent to the analytical limits shown in Table 7.2-3 and 7.3-4 of DCD (Reference 1) Section 7.2 and 7.3 and credited in safety analysis in DCD (Reference 1) Section 15.0.0.3.

Table 4.1-1 Allocated Response Time of Reactor Trip

Table 4.1-2 Allocated Response Time of ESF Actuation

4.2 Basis for Response Time Allocations

The US-APWR Technical Specifications (US-APWR DCD (Reference 1) chapter 16) requires verification that the response times for all RT system and ESF system functions are less than or equal to the maximum values assumed in the accident analysis. Response time may be verified by actual periodic surveillance response time tests in any series of sequential, overlapping or total channel measurements, or by the summation of allocated sensor, signal processing and actuation logic response times with actual response time tests on the remainder of the channel. Allocations for sensor, signal conditioning, and actuation logic response times may be obtained from: (1) historical records based on acceptable response time tests (hydraulic, noise, or power interrupt tests), (2) in place, onsite, or offsite (e.g., vendor) test measurements, or (3) utilizing vendor engineering specifications. This section provides the basis and methodology for allocating response times for the sensors, digital controllers, RTB, and CRDM in the RT system, and the sensors and digital controllers in the ESF systems.

The supplier and model of sensor, controller, RTB and CRDM assumed to be applied in US-APWR, and the response times based on the specifications of these equipments are provided in Tables 4.2-1 and 4.2-2 respectively for the RT and ESF actuation systems. The expected response times for non-MELTAC components listed in Tables 4.2-1 and 4.2-2 are based on typical equipment procured for use in the US nuclear power industry. The expected response times will be specified in the applicable procurement documents prior to making the final determination of equipment, and response times will be verified prior to commercial operation.

Allocated response times from T1 to T4 in Tables 4.1-1, 4.1-2 are determined as values which envelop the values based on the specifications of the individual equipments that applied to US-APWR. The values based on specifications are addressed in a column “Expected Response Times Based on Specification” in Tables 4.2-1 and 4.2-2. Tables 4.2-1 and 4.2-2 show there is margin between the expected response times and the allocated response times or the expected response time is equal to the allocated response time. Therefore, the allocated response times for RT and ESF actuation components are to be met by the installed equipment in the actual plant.

The model numbers shown in Table 4.2-1 are only to establish credibility for the response time allocations, based on the actual performance specifications of known components. The actual US-APWR model numbers may be different.

Table 4.2-1 Response Time Allocation for Reactor Trip and Basis
(Sheet 1 of 4)

Table 4.2-1 Response Time Allocation for Reactor Trip and Basis
(Sheet 2 of 4)

Table 4.2-1 Response Time Allocation for Reactor Trip and Basis
(Sheet 3 of 4)

Table 4.2-1 Response Time Allocation for Reactor Trip and Basis
(Sheet 4 of 4)

Table 4.2-2 Response Time Allocation for ESF Actuation and Basis
(Sheet 1 of 3)

Table 4.2-2 Response Time Allocation for ESF Actuation and Basis
(Sheet 2 of 3)

Table 4.2-2 Response Time Allocation for ESF Actuation and Basis
(Sheet 3 of 3)

4.2.1 Basis for Response Time Allocations for Sensors, RTBs and CRDMs

Equipments assigned to sensor part in Tables 4.2-1 and 4.2-2 of this document are transmitters and RTDs of the general vendors in U.S. The response times of these sensors are addressed in the vender specifications and we can find the vender specifications in each vendor web site. The response times T1 of NIS and RCP Speed are negligible and the bases are described in Sections 5.2 and 5.3 respectively. Response time T3 (0.1 sec) is in accordance with the specification of RTBs. The response time of RTBs applied to Japanese Pressurized Water Reactor (PWR) is less than 0.1 sec. RTBs of the same specification will be applied to US-APWR. Also, response time T4 (0.15 sec) is in accordance with the specification of CRDMs as addressed in DCD (Reference 1) Section 3.9.4.2.1.

4.2.2 Basis for Response Time Allocations for Digital Controller

Maximum response times are calculated by the method provided in Table 4.4-1 of the MELTAC Platform Technical Report (Reference 3). The system scale of digital controller is considered for estimating some of response times. To estimate the maximum response times, the system scale is determined by adding some margins to the system scale based on the DCD (Reference 1). The system scale applied to the estimation of maximum response times are shown in Table 4.2-3.

All estimated values above are less than 80% of response time requirement addressed in the column of allocated response times in Tables 4.2-1 and 4.2-2. Therefore, allocated response times T2 in Table 4.2-1, 4.2-2 are appropriate.

●Case 1

Figure 4.2-1 System Configuration of Case 1

●Case 2

Figure 4.2-2 System Configuration of Case 2

●Case 3

Figure 4.2-3 System Configuration of Case 3

Table 4.2-3 The System Scale Applied to the Estimation of Maximum Response Times

Table 4.2-4 Response Time Calculation for Maximum, Minimum and Safety Evaluation in Each Component (Sheet 1 of 4)

Table 4.2-4 Response Time Calculation for Maximum, Minimum and Safety Evaluation in Each Component (Sheet 2 of 4)

Table 4.2-4 Response Time Calculation for Maximum, Minimum and Safety Evaluation in Each Component (Sheet 3 of 4)

Table 4.2-4 Response Time Calculation for Maximum, Minimum and Safety Evaluation in Each Component (Sheet 4 of 4)

5.0 BASIS FOR ELIMINATION OF SURVEILLANCE TESTS

The US-APWR Technical Specifications (US-APWR DCD (Reference 1) chapter 16) describe that the response time may be measured by means of any series of sequential, overlapping, or total steps so that the entire response time is measured. In lieu of measurement, an allocated response time may be applied for selected components provided that the components and the allocation methodology have been previously reviewed and approved by the NRC. This section provides the basis and methodology for allocating response times, and therefore eliminating response time testing for the sensors and digital controllers in the RT and ESF actuation system.

The subject components for elimination of response time tests are transmitters, NIS detector, RCP speed detector and MELTAC platform. The methodology of the response time test elimination is provided in this section and Section 4.6 of the MELTAC Platform Technical Report (Reference 3).

IEEE 338-1987 endorsed by RG1.118 describes about the elimination of response time test that response time testing of all safety-related equipment is not required if, in lieu of response time testing, the response time of safety system equipment is verified by functional testing calibration checks or other tests, or both. This is acceptable if it can be demonstrated that changes in response time beyond acceptable limits are accompanied by changes in performance characteristics that are detectable during routine periodic tests.

MHI applies the description for the response time elimination in IEEE 338-1987 for the safety I&C system. The periodic response time tests of sensors and digital controllers in the RT and ESF actuation system are eliminated by using allocated response times. The failure modes of these components that can affect their response times will also be detected by periodic channel calibration and channel check surveillance tests.

The next subsections provide the detailed methodology of elimination or relaxation of periodic response time tests for sensors including transmitter, nuclear detector and RCP speed sensor.

5.1 Transmitters

5.2 NIS

5.3 RCP Speed

6.0 REFERENCES

References are enumerated in this section, except for codes and standard described in Section 2.

[1] “Design Control Document for the US-APWR”, Revision 3, Mitsubishi Heavy Industries. Ltd., March 2011.

[2] “Safety I&C Description and Design Process”, MUAP-07004, Revision 5, Mitsubishi Heavy Industries. Ltd., October 2010.

[3] “Safety System Digital Platform –MELTAC-”, MUAP-07005, Revision 6, Mitsubishi Heavy Industries. Ltd., October 2010.

[4] “MELTAC Platform Basic Software Safety Report”, JEXU-1015-1009, Revision 3, Mitsubishi Electric Corporation, October 2010.

[5] “Investigation of Response Time Testing Requirements”, EPRI NP-7243, Electric Power Research Institute, May 1991.

[6] “Technical Guidance for Detection for Oil-Loss Failure of Rosemount Pressure Transmitters”, EPRI NP-7121, Electric Power Research Institute, December 1990.

Appendix A Conformance to BTP 7-21

The purpose of this Appendix is to show that MHI's I&C system and its real-time performance conform to the seven acceptance criteria in Section B.3 of BTP 7-21. Excerpts of acceptance criteria from Section B.3 of BTP 7-21 are indicated in *italics*.

A.1 Limiting Response Times

Criteria: Limiting response times should be shown to be consistent with safety requirements (e.g., suppress power oscillations, prevent fuel design limits from being exceeded, prevent a non-coolable core geometry). Setpoint analyses and limiting response times should also be shown to be consistent. The reviewer should verify that limiting response times are acceptable to the organizations responsible for reactor systems, electrical systems, and plant systems before accepting the limiting response times as a basis for timing requirements.

Conformance: The response times of the safety I&C system shown in Tables 4.0-1 and 4.0-2, meets the analytical limits for the response times shown in Tables 7.2-3 and 7.3-4 of DCD Sections 7.2 and 7.3 and credited in safety analysis in DCD Chapter 15. The safety I&C system including the digital controller is designed to meet the response time, which are addressed in this document. Since the processes are asynchronous, there is variation in the response time in the digital controller, but since each process is deterministic there is no uncertainty in the worst case calculated response time. For this reason, both the limiting response times and the setpoint analyses satisfy the safety requirements.

Hence, the safety I&C system of US-APWR conforms to the acceptance criterion “limiting response times” of BTP 7-21.

A.2 Digital Computer Timing Requirements

Criteria: Digital computer timing should be shown to be consistent with the limiting response times and characteristics of the computer hardware, software, and data communications systems. Computer system timing requirements that should be addressed in a software requirements specifications are described in SRP BTP 7-14.

Conformance: A timing problem of digital controllers along the signal pass shown in Section 3.3 are related to the response times of the processing part of the digital controller. The digital controllers adopt the MELTAC platform, and details of the response time are described in Section 4.4 of the MELTAC Platform Topical Report (Reference 3). Since the MELTAC platform having cyclic processing sequence, the response time varies. The maximum response time results when all asynchronous processes pass their data to the next process just after the next process is initiated. In the detailed design phase, conformance to the response time allocations described in this document are demonstrated through response time calculations or analysis for the MELTAC platform which are based on the maximum response time. Therefore, the digital computer timing is consistent with the limiting response times and with the characteristics of computer hardware, software, and data communications systems. In addition, conformance of computer system timing requirements to BTP 7-21 is described in the software requirements specifications.

Hence, the safety I&C system of US-APWR conforms to the acceptance criterion "Digital Computer Timing Requirements" of BTP 7-21.

A.3 Architecture

Criteria: The level of detail in the architectural description should be sufficient that the Staff can determine the number of message delays and computational delays interposed between the sensor and the actuator. An allocation of time delays to elements of the system and software architecture should be available. In initial design phases (e.g., at the point of design certification application), an estimated allocation of time delays to elements of the proposed architecture should be available. Subsequent detailed design and implementation should develop refined timing allocations down to unit levels in the software architecture.

A design should be feasible with currently known methods and representative equipment. Design timing feasibility may be demonstrated by allocating a timing budget to components of the system architecture so that the entire system meets its timing requirements. See NUREG/CR-6083, Sections 2.2, 2.3.1, and 2.3.2, and NUREG/CR-6082. The timing budget should include internal and external communication delays, with adequate margins.

Any non-deterministic delays should be noted and a basis provided that such delays are not part of any safety functions, nor can the delays impede any protective action.

Software architectural timing requirements should be addressed in a software architectural description as described in SRP BTP 7-14. Databases, disk drives, printers, or other equipment or architectural elements subject to halting or failure should not be able to impede protective system action.

Conformance: For RT system, details of the response time allocation and architecture present between the sensor and the component are shown in Figure 3.3-1 in Section 3.3. For ESF system, details of the response time allocation and architecture present between the sensor and the component are shown in Figure 3.3-2 in Section 3.3. Details of the response time of the each component in MELTAC platform are shown in Figure 4.4-2 and Table 4.4-1 of the MELTAC Platform Technical Report (Reference 3) Section 4.4.2. Descriptions for allocating response times to elements of software architecture are described in Section 4.4.1 of the MELTAC Platform Technical Report (Reference 3). An estimated allocation of response times to equipments of the proposed architecture in initial design phases is considered in this document. With these initial requirements of this document being treated as the design basic requirements, more refined timing allocations down to module levels in the software architecture are developed in subsequent detailed design and implementation phase.

RT and ESF systems of the US-APWR are configured with the MELTAC platform which has sufficient proven reliability and performance in nuclear plant applications as described in Section 7 of the MELTAC Platform Technical Report (Reference 3). The MELTAC platform allocates a response time budget to components of the system architecture so that the system is to be designed to meet this response time allocation. The system has sufficient feasibility. Since I/O modules and communication buses are considered as elements for the response time delays, adequate margins are considered for connection or communication delays between equipment. In addition, these response time delays are all deterministic.

Software architectural timing features are clearly addressed in the MELTAC Platform Technical Report (Reference 3) Section 4.4.1. The system is designed such that databases, disk drives, or other equipment or architectural elements subject to halting or failure do not disturb the protective action.

Hence, the safety I&C system of US-APWR conforms to the acceptance criterion "Architecture" of BTP 7-21.

A.4 Design Commitments

Criteria: Design basis documents should describe system timing goals.

Timing requirements should be satisfied by design commitments.

A design should consider data rates, data bandwidths, and data precision requirements for normal and off-normal operation, including the impact of environmental extremes. There should be sufficient excess capacity margins to accommodate likely future increases in demands or software or hardware changes to equipment.

Design basis documents should identify design practices that the applicant/licensee will use to avoid timing problems. Risky design practices such as non-deterministic data communications, non-deterministic computation, use of interrupts, multitasking, dynamic scheduling, and event-driven design should be avoided. When such practices are allowed, the applicant/licensee should describe methods for control of the associated risk. NUREG/CR-6082 and NUREG/CR-6083 describe risky design practices in more detail.

Conformance: Timing requirements required by the data communication system of the US-APWR are analytical limits of the response times shown in Table 15.0-4 of DCD Chapter 15. Tables 4.0-1 and 4.0-2 in this document, which are the response time allocation, satisfy these timing requirements.

Since the MELTAC platform processes analog inputs with 16-bit resolution, the numeric precision are in the order of 10^{-5}, which is considered to be negligible compared with total uncertainty. Therefore, data precision requirements are assumed to be satisfied. In addition, data rates and data bandwidths are taken into consideration in the design as shown in the materials that are referred to in DCD Section 7.9.2.3.4. Initial design for the US-APWR is carried out with sufficient excess capacity margins to accommodate likely future increases in hardware or software functions.

The MELTAC platform adopts deterministic data communications to avoid timing problems. Risky design practices such as non-deterministic data communications, non-deterministic computation, use of interrupts, multitasking, dynamic scheduling, and event-driven design are not adopted.

Hence, the safety I&C system of US-APWR conforms to the acceptance criterion "Design Commitments" of BTP 7-21.

A.5 Performance Verification

Criteria: The means proposed, or used, for verifying a system's timing should be consistent with the design.

Testing and/or analytic justification should show that the system meets limiting response times for a reasonable, randomly selected subset of system loads, conditions, and design basis events. The subset should include some limiting load conditions and be chosen by persons independent of the persons who designed the system.

Both analytical and test techniques of timing analysis have drawbacks. It is difficult to demonstrate completeness of timing tests. Completeness is easier to demonstrate for analyses, but analyses predict extreme times that are not actually possible. Therefore, analysis and testing are often combined in a complementary manner to confirm that a system can meet the limiting response times.

Measurement methods should be appropriate to the resolution and detail required.

Timing measurements should meet projections or the anomalies should be satisfactorily explained (NUREG/CR-6083, Sections 2.1, 2.3.3, and 2.3.4).

Conformance: The response time of the safety I&C system is designed and verified in water fall design process during basic design and detail design phase. In addition, within the scope of software V&V activities for the digital safety system these design process including response time design is verified. IEEE Std 7-4.3.2-2003 endorsed by RG1.152 refers IEEE Std 1012-1998. IEEE Std 1012-1998 provides the standard for software verification and validation (V&V).

Response time testing shows that the system meets limiting response times for a reasonable and randomly selected subset of system loads, conditions, and design basis events. The subset includes some limiting load conditions and is chosen by persons independent of the persons who designed the system. Verifying that the system meets the limiting response times is conducted by a combination of analysis and testing. The analysis is conducted according to the method described in the Safety I&C Technical Report (Reference 2) Section 6.5.3 and the MELTAC Platform Technical Report (Reference 3) Section 4.4.

Hence, the safety I&C system of US-APWR conforms to the acceptance criterion "Performance Verification" of BTP 7-21.

A.6 Use of Cyclic Real-Time Executive

Criteria: In systems that include a cyclic real-time executive (operating system), a typical cycle includes application modules, diagnostic modules, and other support modules. A watch-dog timer is normally set at the beginning of each cycle and reset at the end. If the cycle is not completed before the watch-dog timer period is complete, an error is generated.

A basis should be provided that describes the cycle and demonstrates that the watch-dog timer is correctly implemented, the time required for the application modules does not exceed the allotted time given in the architecture timing budget, and diagnostic and other support modules will not cause the allotted time to be exceeded.

Examples of solutions acceptable to the Staff may be found in the Safety Evaluation Reports for the Palo Verde Nuclear Generating Station, Units 1, 2, and 3, "Issuance of Amendments on the Core Protection Calculator System Upgrade," dated October 24, 2003, and the Siemens Power Corporation, Topical Report EMF-2110(NP), "Teleperm XS: A Digital Reactor Protection System," dated May 5, 2000.

Conformance: The I&C system of the US-APWR adopts the MELTAC platform which system technology includes a cyclic real-time executive. As explained in the MELTAC Platform Technical Report (Reference 3), the MELTAC platform includes processing modules (application modules) and support modules such as I/O modules and Bus Master Modules, and these modules have self-diagnostic function. It is designed such that the self-diagnostic does not hinder the achievements of the response time requirements. In addition, the MELTAC platform adopts a watch-dog timer. As Section 4.4.1 of the MELTAC Platform Technical Report (Reference 3) provides an explanation for processing time cycles.

Therefore, the watch-dog timer is correctly implemented. As mentioned in Section A.3 "Architecture" in this document, the MELTAC platform allocates a response time budget to components of the system architecture so that the system is to be designed to meet this response time allocation. Therefore, the response time required for the application module, the support module, and the self-diagnostic module does not exceed the allotted time given in the architecture timing allocation.

Hence, the safety I&C system of US-APWR conforms to the acceptance criterion "Use of Cyclic Real-Time Executive" of BTP 7-21.

A.7 Use of Part-Scale Prototypes

Criteria: In systems that have not been implemented and tested on a full scale, expected system delays on scale-up should be calculated and shown to be less than limiting system response times (NUREG/CR-6083, Sections 2.1.3 and 2.1.4).

A basis should be provided that describes the effects of adding sensors, divisions, communication links, controllers, computer nodes, or actuation devices required to scale the test system to full scale.

Test data should confirm scaling as well as performance projections. Exceptions are considered anomalies or abnormal events.

Prototypes designed to demonstrate scaling should include all significant architectural elements plus enough additional elements to show the scaling effects to be measured.

Conformance: The MELTAC platform is conducted to perform full scale testing of response time in the factory acceptance test. A basis described the effects of adding sensors and actuation devices required to scale the test system to full US-APWR scale is prepared. Test data confirms scaling as well as performance projections. When anomalies or abnormal events are observed in the testing, they will be treated as exceptions. Prototypes designed to demonstrate scaling include all significant architectural elements plus enough additional elements to show the scaling effects to be measured.

Hence, the safety I&C system of US-APWR conforms to the acceptance criterion "Use of Part-Scale Prototypes" of BTP 7-21.