Safety I&C System

Revision 1

Non-Proprietary

May 2017

REVISION HISTORY

Revision	Date	Page	Description
0	November 2014	All	First Issue
1	May 2017	(Sections)	Revised based on RAI response or editorial correction. (RAI Numbers)
		xx (Acronyms)	master transfer switch (MTS) added
		xx (Acronyms)	quality assurance manual → APR1400 quality assurance manual (RAI 261-8253, Question 07.01-30)
		xxii (Acronyms)	transient and accident analysis (TAA) added
		3 (3.1)	Description for Type A variable added (RAI 38-7878, Question 07.05-1)
		3-4 (3.1)	Quality Standards (item f) deleted (RAI 43-7887, Question 07.01-10)
		4 (3.1)	Editorial correction (item k, QAPD)
		4 (3.2)	Editorial correction (QAM → APR1400 DC QAM)
		5 (3.2)	Description for Type A variable added (RAI 38-7878, Question 07.05-1)
		6 (3.2)	Editorial correction (RAI 50-7911, Question 07.02-9)
		8 (3.3.1)	SECY-93-087 II.Q → SRM on SECY-93-087 Item II.Q (RAI 43-7887, Question 07.01-16)
		8 (3.3.2)	SECY-93-087 II.T → SRM on SECY-93-087 Item II.T (RAI 43-7887, Question 07.01-17)
		10 (3.4.5)	Editorial correction (Protection → Protective)
		10 (3.4.7)	Description for Type A variable added (RAI 38-7878, Question 07.07-1)

Revision	Date	Page	Description
		11 (3.4.7)	Description for software class modified (RAI 38-7878, Question 07.07-1)
		12 (3.4.12)	Editorial correction (Digital → Use of)
		12 (3.4.16)	Editorial correction (“Software” deleted)
		13 (3.4.18)	Editorial correction (“and Complex Electronics” added)
		18 (4.1)	Description of safety system interfaces added. (RAI 45-7883, Question 07.09-2)
		18 (4.1)	Description for figures identical for all channels or divisions added. (RAI 50-7911, Question 07.02-1)
		18 (4.1)	Table 4-1 added to list interface signals between redundant portions of safety system. (RAI 45-7883, Question 07.09-2)
		18 (4.1)	Description of “All figures identical for all channels or divisions” added (RAI 50-7911, Question 07.02-1)
		19 (4.1)	Table 4-2 added to list interface signals between safety and non-safety system (RAI 45-7883, Question 07.09-2)
		20 (4.1.1.3)	safety limit → setpoints
		20 (4.1.1.4)	Description for Type A variable added (RAI 38-7878, Question 07.05-1)
		21 (4.1.1.5)	APC-S not susceptible to software CCF added (RAI 342-8291, Question 07.08-11)
		21 (4.1.1.5)	APC-S not susceptible to software CCF added (RAI 33-7880, Question 07.08-5)
		22 (4.1.2.5)	Description for Type A variable added (RAI 38-7878, Question 07.05-1)
		23 (4.1.2.7)	Description for IFPD failure added (RAI 323-8281, Question 07.03-19)
		25 (4.1.4)	Description for system status display added (RAI 323-8281, Question 07.03-19)

Revision	Date	Page	Description
		26 (4.1)	Fig. 4-1 modified as follows: - TSC, RCC, EOF and ERDS added - System/Component-Level MI revised - Signal from CPM to CCG added
		29 (Table 4-3)	Editorial corrections to be consistent with the related description (Transmitter → APC-S, CSAS → CIAS)
		30 (4.2.1.1)	Hardwired connection (PPS → TCS) added. (RAI 274-8277, Question 07.01-35)
		33 (4.2.2.1)	Editorial correction (RAI 50-7911, Question 07.02-9)
		34 (4.2.2.1)	PPS WDT description added. (RAI 356-7881, Question 07-14)
		34 (4.2.2.1)	Description for software diversity modified. (RAI 50-7911, Question 07.02-2)
		38 (4.2.3.4)	Description for MTP connection for software loading added (RAI 317-8271, Question 14.03.05-18)
		38 (4.2.3.6)	Status of RTSG latched trip state added (RAI 272-8313, Question 07.02-13)
		40 (4.2.2.1)	Fig. 4-5 modified to revise the configuration of LCL processor (RAI 50-7911, Question 07.02-5)
		42 (4.2.2.1)	Fig.4-7 modified to add Note 2 and Note 4.. (RAI 356-7881, Question 07-14) (RAI 272-8313, Question 07.02-13)
		43, 44 (4.2.4)	Descriptions of signal interfaces added. (RAI 45-7883, Question 07.09-2)
		45 (4.3.1.1)	Description for auxiliary trip added. (RAI 488-8617, Question 07.02-17)
		47 (4.3.1.5)	Description for unidirectional interface form MTP to DCS gateway server added (RAI 348-8279, Question 07.09-11)
		50,51 (4.3.2.3)	Description of response time requirements added. Figure 4-9 added. (RAI 50-7911, Question 07.02-4)
		55,58 (4.3.3.2)	Fig.4-11 (CEA positions and PF movement) added (RAI 274-8277, Question 07.01-40)

Revision	Date	Page	Description
		56 (4.3.3.3)	Description for CEAC1 and CEAC2 inoperable added (RAI 274-8277, Question 07.01-37)
		56, 57 (4.3.4.1, 4.3.4.2, 4.3.4.3 4.3.4.4, 4.3.4.6, 4.3.4.8)	Descriptions of signal interfaces added (RAI 45-7883, Question 07.09-2)
		64 (4.4.2)	ESF-2 signal and manual reset for ESF control description added (RAI 300-8297, Question 07.03-5)
		64 (4.4.2)	Description for IFPD to ESCM interface modified (RAI 317-8271, Question 14.03.05-32)
		65 (4.4.2)	Component control logic input description added (RAI 323-8281, Question 07.03-16)
		66 ~ 81 (4.4.2)	Table 4-4 added to add list of ESF-1 and 2 safety command signals (RAI 323-8281, Question 07.03-20)
		83 (4.4.3.1)	ESF-CCS WDT description added (RAI 33-7880, Question 07.08-14)
		86 (4.4.3.4)	Fig 4-15 modified to revise Minimum inventory switch term and connection between CPM and CCG (RAI 323-8281, Question 07.03-17)
		86 (4.4.3.4)	Fig 4-15 modified to add modulating control functions (RAI 323-8281, Question07.03-14)
		88 (4.2.2)	Editorial corrections (Fig. 4-17) EFS → ESF, AUTO START → AUTO STOP
		89 (4.4.3.4)	Fig.4-18 modified to show WDT initiation for ESF-CCS component (RAI 356-7881, Question 07-14)
		90 (4.4.4)	Editorial correction (PAMI → P)
		91 (4.4.4.7)	Editorial correction (PAMI → P)
		91 (4.4.4.12)	Descriptions of signal interfaces added (RAI 45-7883, Question 07.09-2)

Revision	Date	Page	Description
		91 ~ 99 (4.4.4.13)	Section 4.4.4.13 and Tab. 4-5 added to add interdivisional ESF-CCS signal (RAI 348-8279, Question 07.09-9)
		100 (4.5.1)	Description for Type A variable added saturation margins → subcooling margins (RAI 38-7878, 07.05-1)
		100 (4.5.2.1)	Description for Type A variable added saturation margins → subcooling margins, reactor vessel coolant water level → reactor vessel level (RAI 38-7878, Question 07.05-1)
		102,103 (4.5.2.5)	saturation margins → subcooling margins, upper head → RV upper head (RAI 38-7878, Question 07.05-1)
		103 (4.5.2.6)	Description for Type A variable added (RAI 38-7878, Question 07.05-1)
		103 (4.5.3)	Interface with “CPCS” deleted (RAI 38-7878, Question 07.05-1)
		104 (4.5.3)	Descriptions of signal interfaces added. (RAI 45-7883, Question 07.09-2)
		105 (4.5.3)	Table 4-6 modified to add I/O signals and description for Type A, and CPCS deleted (RAI 38-7878, Question 07.05-1)
		107 (4.6.1.3)	Description for message transfer modified. (RAI 348-8279, Question 07.09-17)
		107 (4.6.1.3)	Description for SDN network added (RAI 68-7892, Question 07.07-6)
		116 (4.7.1.3)	Description for “setpoint reset switches” added. (RAI 301-8280, Question 07.01-52)
		116 (4.7.1.4)	Description for control steps modified (RAI 45-7883, Question 07.09-7)
		117 (4.7.1.4)	ESCM Modulating control description added (RAI 323-8281, Question 07.03-14)
		121 (4.7.1.5)	New section for task timing analysis for IFPD to ESCM interface added (RAI 348-8279, Question 07.09-13)
		122 (4.7.4)	Description for “setpoint reset switches” added (RAI 301-8280, Question 07.01-52)

Revision	Date	Page	Description
		123 (4.7.5)	Editorial correction (then then → then)
		124 (4.7.5)	Fig 4-30 modified to Minimum inventory switch term and connection between CPM and CCG (RAI 323-8281, Question 07.03-17)
		125-128 (4.7.6)	Section 4.7.6 added to add MCR/RSR master transfer switch description and Fig. 4-31 and Fig. 4-32 (RAI 44-7877, Question 07.04-1R)
		129 (4.7.6)	P-CCS and PCS master transfer switch description and Fig. 4-33 added (RAI 44-7877, Question 07.04-6)
		130 (4.8.2)	Descriptions of signal interfaces added. (RAI 45-7883, Question 07.09-2)
		132 (5.1)	Editorial correction (QAM → APR1400 DC QAM)
		133 (6.0)	IEEE 323-1983 → IEEE323-2003 List of testing/analysis added. (RAI 43-7887, Question 07.01-24)
		133 (6.1)	Editorial correction Table 6.1-1 → Table 6-1
		134 (6.1)	Description for I&C cabinet protection design added (RAI 356-7881, Question 07-13)
		137 (7.1)	Editorial correction (RAI 50-7911, Question 07.02-9)
		137 (7.)	“Section 7.2 Unavailability Analysis” deleted. (RAI 356-7881, Question 07-20)
		138 (8)	Description for safety-related display panels added (RAI 323-8281, Question 07.03-8)
		139 (9)	References 19,20, and 21 added (RAI 348-8279, Question 07.09-14) TeRs revision date updated
		A8, A9 (A.4)	Equipment protective functions for safety-related plant equipment description added (RAI 301-8280, Question 07.01-47)
		A11 (A.5.3)	Editorial correction (NQAI → NQA-1)

Revision	Date	Page	Description
		A12 (A.5.4)	IEEE 323-1983 → IEEE323-2003 (RAI 43-7887, Question 07.01-24)
		A14 (A.5.6)	Analysis for Clause 5.6.3 added (RAI 45-7883, Question 07.09-1)
		A14 (A.5.6)	Signal interfaces (PPS → TCS, ENFMS → NIMS) added (RAI 274-8277, Question 07.01-35)
		A17 (A.5.8)	Description for Type A variable added (RAI 38-7878, Question 07.05-1)
		A18 (A.5.9)	Editorial correction (assess → access)
		A20 (A.5.11)	Identification requirements (IEEE 384 endorsed by RG 1.75) added (RAI 43-7887, Question 07.01-20)
		A20,A21 (A.5.12)	List of auxiliary features added (RAI 43-7887, Question 07.01-21)
		A23 (A.6.2)	Editorial correction (“.” deleted)
		A26 (A.6.7)	Editorial correction (RAI 50-7911, Question 07.02-9)
		C3 (C.3)	Fig. C.3-1 modified based on ACRS presentation
		C19 (C.5.1.3.2)	“CEA number 1” → “CEA01” (RAI 50-7911, Question 07.02-7)
		C20 (C.5.1.3.2)	Channel assignment for CPCS CEA01 modified. (RAI 50-7911, Question 07.02-7)
		C22 (C.5.1.3.5)	Editorial correction (PVGNS → PVNGS)
		C25 (C.5.1.3.7)	Description for plant trip due to PF modified. (RAI 274-8277, Question 07.01-37)
		C25 (C.5.1.3.7)	“CEA number 1” → “CEA01” (RAI 50-7911, Question 07.02-7)
		C26,C27 (C.5.1.3.7)	Safety enhancement of CPP and CEAC/CPP interdivisional communication added. (RAI 348-8279, Question 07.09-18)

Revision	Date	Page	Description
		C27,C29, C30 (C.5.1.3.7)	CPCS software comparison (Table C.5.1-2) and design conformance to CPU load restriction (Table C.5.1-3) added. (RAI 43-7887, Question 07.01-25)
		C35 (C.5.1.4)	Safety enhancement of interdivisional communications of CIV positions added (RAI 45-7883, Question 07.09-4)
		C39 ~ C79 (C.5.1.5)	Ethernet Compliance → IFPD-ESCM Network Compliance (RAI 45-7883, Question 07.09-7)
		C40 ~ C61 (C.5.1.5)	Description for compliance to DI&C-ISG-04, Section 1, Position 3 modified, Tab. C.5.1-4 and C.5.1-5 added, and Fig. C.5-1 and C.5-2 added (RAI 348-8279, Question07.09-13)
		C63 ~ C64 (C.5.1.5)	Description for compliance to DI&C-ISG-04, Section 1, Position 4 modified (RAI 348-8279, Question07.09-12)
		C68 ~ C75 (C.5.1.5)	Description for compliance to DI&C-ISG-04, Section 1, Position 12 modified (RAI 348-8279, Question07.09-12)
		C75 ~ C77 (C.5.1.5)	Description for compliance to DI&C-ISG-04, Section 1, Position 13,14,15, and 17 modified (RAI 348-8279, Question07.09-15)
		C78, C79 (C.5.1.5)	Description for compliance to DI&C-ISG-04, Section 1, Position 19 modified (RAI 348-8279, Question07.09-12)
		C79 (C.5.1.5)	Description for compliance to DI&C-ISG-04, Section 1, Position 20 modified (RAI 348-8279, Question07.09-14)
		C80 (C.5.2.1)	Description for “the diagnosis section of CIM output signals” added (RAI 37-7882, Question 07.03-2)
		C85 ~ C98 (C.5.3.1)	Description for compliance to DI&C-ISG-04, Section 3 modified and Fig. C.5-4 and C.5-5 added (RAI 45-7883, Question 07.09-3)
		E1 ~E7 (E.1)	Appendix for safety components controlled by ESCM and Tab. E.1-1 added (RAI 45-7883, Question 07.09-3)
			Note 1. Figure and Table numbers are renumbered by adding or deleting a figure or table accordingly.

This document was prepared for the design certification application to the U.S. Nuclear Regulatory Commission and contains technological information that constitutes intellectual property of Korea Hydro & Nuclear Power Co., Ltd. Copying, using, or distributing the information in this document in whole or in part is permitted only to the U.S. Nuclear Regulatory Commission and its contractors for the purpose of reviewing design certification application materials. Other uses are strictly prohibited without the written permission of Korea Electric Power Corporation and Korea Hydro & Nuclear Power Co., Ltd.

ABSTRACT

This Technical Report provides the system description and the design features of the digital computer-based safety I&C system which is intended to be used for the application of the APR1400 Design Certification to the Nuclear Regulatory Commission (NRC).

This report is focused on the system description, design features and software design process for the plant protection system (PPS), core protection calculator system (CPCS), engineered safety features – component control system (ESF-CCS) and qualified indication and alarm system – P (QIAS-P). The report includes the system's compliance with codes and standards, I&C system overview, safety I&C system configuration and description, data communication network, software reliability, equipment qualification plan and equipment reliability analysis methodology.

This report also includes four appendices; Conformance to IEEE Std. 603-1991, Conformance to IEEE Std. 7-4.3.2-2003, Conformance to DI&C-ISG-04, and Alternative to Independence Requirements of IEEE Std. 603-1991.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ACRONYMS AND ABBREVIATIONS

AC160	ABB Advant Controller Series160
AF100	Advant Fieldbus 100
AFAS	auxiliary feedwater actuation signal
AI	analog input
ALMS	acoustic leak monitoring system
AMI	accident monitoring instrumentation
ANS	American Nuclear Society
ANSI	American National Standards Institute
AO	analog output
AOO	anticipated operational occurrence
APC-S	auxiliary process cabinet – safety
APR1400	Advanced Power Reactor 1400
ASME	American Society of Mechanical Engineers
ATWS	anticipated transients without scram
BISI	bypassed and inoperable status indication
BOP	balance of plant
BP	bistable processor
BTP	Branch Technical Position
CCF	common cause failure
CCG	control channel gateway
CCS	component control system
CEA	control element assembly
CEAC	CEA calculator
CEDM	control element drive mechanism
CET	core exit thermocouple
CFR	Code of Federal Regulations
CI	communication interface
CIAS	containment isolation actuation signal
CIM	component interface module
CIV	containment isolation valve
CMOS	complementary metal oxide semiconductor
COLSS	core operating limit supervisory system
CP	communication processor
CPC-CWP	CPC CEA withdrawal prohibit

CPC(S)	core protection calculator (system)
CPIAS	containment purge isolation actuation signal
CPM	control panel multiplexer
CPP	CEA position processor
CPU	central processing unit
CRC	cyclic redundancy checksum
CREVAS	control room emergency ventilation actuation signal
CS	communication section
CSAS	containment spray actuation signal
CVCS	chemical volume control system
CWP	CEA withdrawal prohibit
D3	diversity and defense-in-depth
DAS	diverse actuation system
DB	database
DBE	design basis event
DCD	design control document
DCN-I	data communication network - information
DCS	distributed control system
DI	digital input
DIS	diverse indication system
DMA	diverse manual ESF actuation
DNBR	departure from nucleate boiling ratio
DO	digital output
DPS	diverse protection system
DPRAM	dual-ported random access memory
DRCS	digital rod control system
EDG	emergency diesel generator
EMC	electromagnetic compatibility
EMI	electromagnetic interference
ENFMS	ex-core neutron flux monitoring system
EOP	emergency operating procedure
EP	Ethernet processor
EPRI	Electric Power Research Institute
ESCM	ESF-CCS soft control module
ESF	engineered safety features
ESFAS	engineered safety features actuation system

ESF-CCS	engineered safety features - component control system
FE	function enable
FHEVAS	fuel handling area emergency ventilation actuation signal
FIDAS	fixed in-core detector amplifier system
FMEA	failure modes and effects analysis
FP	function processor
FPD	flat panel display
FPGA	field programmable gate array
FWCS	feedwater control system
GC	group controller
GDC	General Design Criteria
HDLC	high level data link control
HFE	human factors engineering
HJTC	heated junction thermocouple
HRA	human reliability analysis
HSI	human - system interface
HSL	high speed link
HVAC	heating, ventilation, and air conditioning
I&C	instrumentation and control
ICC	inadequate core cooling
ICIS	in-core instrumentation system
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IFPD	information flat panel display
I/O	input and output
IPS	information processing system
IRWST	in - containment refueling water storage tank
ITAAC	inspections, tests, analyses, and acceptance criteria
ITP	interface and test processor
ITS	important-to-safety
IVMS	internal vibration monitoring system
KHNP	Korea Hydro & Nuclear Power Co., Ltd.
LC	loop controller
LCL	local coincidence logic
LCO	limiting conditions for operation
LDP	large display panel

LOCA	loss of coolant accident
LPD	local power density
LPMS	loose parts monitoring system
L-R	latch-reset
MCC	motor control center
MCR	main control room
MI	minimum inventory
MIL Std.	Military Standard
MSIS	main steam isolation signal
MSIV	main steam isolation valve
MTC	MTP/ITP cabinet
MTP	maintenance and test panel
MTS	master transfer switch
NR	narrow range
NIMS	NSSS integrity monitoring system
NPCS	NSSS process control system
NRC	Nuclear Regulatory Commission
NSSS	nuclear steam supply system
O&M	operation & maintenance
OM	operator module
P-CCS	process - component control system
PCS	power control system
PF	penalty factor
PI	process instrumentation
PM	processor module
PLC	programmable logic controller (AC160)
PLCS	pressurizer level control system
PLD	programmable logic device
PPCS	pressurizer pressure control system
PPS	plant protection system
PRA	probabilistic risk analysis
PS	processing section
PVNGS	Palo Verde Nuclear Generating Station
PZR	pressurizer
QAM	APR1400 DC quality assurance manual
QAPD	quality assurance program description

QIAS-P	qualified indication and alarm system - p
QIAS-N	qualified indication and alarm system - non-safety
RAM	random access memory
RCP	reactor coolant pump
RCPSSSS	reactor coolant pump shaft speed sensing system
RCPVMS	reactor coolant pump vibration monitoring system
RCS	reactor coolant system
RFI	radio frequency interference
RG	Regulatory Guide
RH	relative humidity
RMS	radiation monitoring system
ROM	read only memory
RPCS	reactor power cutback system
RPS	reactor protection system
RRS	reactor regulating system
RSC	remote shutdown console
RSR	remote shutdown room
RSPT	reed switch position transmitter
RT	reactor trip
RTD	resistance temperature detector
RTM	requirement traceability matrix
RTSG	reactor trip switchgear
RTSS	reactor trip switchgear system
SAFDL	specified acceptable fuel design limit
SBCS	steam bypass control system
SC	safety console
SDL (HSL)	serial data link (common q high speed link)
SDN (AF100)	safety system data network (Advant Fieldbus 100)
SDOE	secure development and operational environment
SFC	single failure criterion
SG	steam generator
SHA	software hazard analysis
SIAS	safety injection actuation signal
SODP	shutdown overview display panel
SPADES+	safety parameter display and evaluation system plus
SPDS	safety parameter display system

SPM	software program manual
S-R	set-reset
SRDC	safety-related divisionalized cabinet
SRM	Staff Requirements Memorandum
SRP	Standard Review Plan
SSE	safe shutdown earthquake
ST	shunt trip
STD	standard
SW	software
TAA	transient and accident analysis
TCB	trip circuit breaker
TCS	turbine control system
TeR	technical report
TID	total integrated dose
TMI	Three Mile Island
TS	technical specification
TTL	transistor-transistor logic
UV	undervoltage
Vac	volts-alternating current
V&V	verification and validation
VBPSS	vital bus power supply system
Vdc	volts-direct current
VOPT	variable over power trip
WDT	watchdog timer
WR	wide range

Page intentionally blank

1 PURPOSE

This Technical Report (TeR) provides the system description and the design process of the digital computer-based safety I&C system, which is intended to be used for the application of the Advanced Power Reactor 1400 Design Certification (APR1400 DC).

2 SCOPE

This report provides the system description, design features and software design process of the following safety I&C system: the plant protection system (PPS), the core protection calculator system (CPCS), the engineered safety features – component control system (ESF-CCS), and the qualified indication and alarm system-P (QIAS-P).

It includes the system's compliance with codes and standards, I&C system overview, safety I&C system configuration and design description, data communication network, software reliability, equipment qualification plan, equipment reliability analysis methodology, and safety I&C system platform.

This report also includes three appendices; Conformance to IEEE Std. 603-1991, Conformance to IEEE Std. 7-4.3.2-2003, Conformance to DI&C-ISG-04, and Alternative to Independence Requirements to IEEE Std. 603-1991.

This report does not cover sensors and associated cables, ancillary trip systems or other safety I&C system and equipment.

The diversity and defense-in-depth (D3) analysis is addressed in the Diversity and Defense-in-Depth TeR (Reference 1) and software common cause failure (CCF) analysis coincident with design basis events (DBEs) for the safety I&C system is addressed in the CCF Coping Analysis TeR (Reference 2). In addition, priority logic design to cope with a CCF is addressed in the Component Interface Module TeR (Reference 3).

3 APPLICABLE CODES AND REGULATIONS

This section describes the compliance of the safety I&C system with the applicable codes and regulations. The system's compliance with IEEE Std. 603-1991, IEEE Std. 7-4.3.2-2003, NRC Interim Staff Guidance (ISG) DI&C-ISG-04, "Highly-Integrated Control Rooms – Communications Issues" (Reference 4), and alternative to independence requirements of IEEE Std. 603-1991 are addressed in Appendices A, B, C, and D of this report, respectively.

3.1 10 CFR Part 50 and 52

a. 10 CFR 50.34(f)(2)(v), "Bypass and Inoperable Status Indication"

The indications of bypasses and inoperable status of the safety I&C system are available on the operator module (OM), maintenance and test panel (MTP), qualified indication and alarm system - non-safety (QIAS-N) and information processing system (IPS) displays.

See compliance with Regulatory Guide (RG) 1.47 in Section 3.4.3.

b. 10 CFR 50.34(f)(2)(xii), "Auxiliary Feedwater System Automatic Initiation and Flow Indication"

The low steam generator (SG) water level trip signal initiates a reactor trip when the measured water level in a SG's downcomer region falls to a low preset value. Separate initiations are provided for the reactor protection system (RPS) and auxiliary feedwater actuation system (AFAS) to allow different setpoints for reactor trips and auxiliary feedwater actuations.

The AFAS continues to deliver auxiliary feedwater to the SG until a preset water level has been reestablished. Manual actuation is provided to permit the operator to actuate the AFAS.

Auxiliary feedwater flow rate is displayed on the QIAS-N, IPS, and diverse indication system (DIS).

c. 10 CFR 50.34(f)(2)(xiv), "Containment Isolation Systems"

The containment isolation actuation system (CIAS) is provided to mitigate the release of radioactive material during an accident by actuating the containment isolation valves (CIVs) which close the process lines penetrating the containment.

d. 10 CFR 50.34(f)(2)(xi), "Direct Indication of Relief and Safety Valve Position"
10 CFR 50.34(f)(2)(xvii), "Instrumentation to Measure, Record and Readout in the Control Room"
10 CFR 50.34(f)(2)(xviii), "Unambiguous Indication of Inadequate Core Cooling"
10 CFR 50.34(f)(2)(xix), "Instrumentation for Monitoring Plant Conditions Following an Accident"
10 CFR 50.34(f)(2)(xx), "Power Supplies for Pressurizer Relief Valves, Block Valves, and Level Indicators"

Types A, B and C accident monitoring instrumentation are displayed on the QIAS-P, QIAS-N, and IPS. The QIAS-N displays selected variables of Types D and E to support plant safe shutdown and Emergency Operating Procedure (EOP). All variables of Types D and E are displayed on the IPS.

e. 10 CFR 50.49, "Environmental Qualification of Electric Equipment Important to Safety for Nuclear Power Plants"

The safety I&C system is installed in a mild environment and therefore this criterion is not applicable. This criterion is applicable to instrumentation that interfaces to this system.

f. (Deleted)

g. 10 CFR 50.55a(h), “Protection and Safety Systems”

The safety I&C system is designed to meet the requirements of the requirements of IEEE Std. 603-1991 and the correction sheet dated January 30, 1995. Compliance to IEEE Std. 603-1991 is described in Appendix A of this report.

IEEE Std. 603-1991, Clause 6.7 states, “Capability of a safety system to accomplish its safety functions shall be retained while sense and command features equipment is in maintenance bypass”. The Balance of Plant (BOP) ESFAS functions are 1-out-of-2 logic taken twice except the fuel handling area emergency ventilation actuation signal (FHEVAS) initiation signal that performs 1-out-of-2 logic taken once. The detailed compliance with IEEE Std. 603-1991 is described in Appendix A.

The CPCS has two channels of reed switch position transmitter (RSPT) for each control element assembly (CEA). The alternative to Clause 5.6 of IEEE Std. 603-1991 to satisfy the independence requirement is described in Appendix D.

h. 10 CFR 50.62, “Requirements for Reduction of Risk from ATWS”

The diverse protection system (DPS) is designed to satisfy Anticipated Transients Without Scram (ATWS) requirements and is described in the Diversity and Defense-in-Depth TeR. The DPS is diverse from the safety I&C system.

The details of the diversity of the scram system are described in Section 4.8 and the conformance to 10 CFR 50.62 is described in Appendix B of the Diversity and Defense-in-Depth TeR.

i. 10 CFR 52.47(b)(1), “ITAAC for Standard Design Certification”

The Inspections, Tests, Analyses, and Acceptance Criteria (ITAAC) are described in Section 2.5 of the Design Control Document (DCD).

j. 10 CFR 50 Appendix A, “General Design Criteria for Nuclear Power Plants”

The safety I&C system is designed to meet the requirements of 10 CFR 50 Appendix A as described in Section 3.2.

k. 10 CFR 50 Appendix B. “Quality Assurance Criteria for Nuclear Power Plants and Fuel Processing Plants”

The safety I&C system is designed to meet the requirements of 10 CFR 50 Appendix B as described in the Quality Assurance Program Description (QAPD) (Reference 5).

l. 10 CFR 52.47(a)(2)(iv), “Release of Radioactive Material”

The CCF coping analysis is performed to meet the guideline values of radiation dose. The results of the offsite radiological consequences obtained from the CCF Coping Analysis TeR meet the acceptance criteria required by 10 CFR 52.47.

3.2 10 CFR Part 50 Appendix A, General Design Criteria

a. GDC 1, “Quality Standards and Records”

The QAPD and APR1400 DC Quality Assurance Manual (QAM) (Reference 6) comply with the requirements of 10 CFR 50, Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Processing Plants ".

b. GDC 2, “Design Bases for Protection Against Natural Phenomena”

The safety I&C system is designated as seismic Category I. The safety I&C system is installed in the I&C equipment rooms or main control room (MCR) that provide protection against other natural phenomena, such as wind, tornado, and flood.

c. GDC 4, “Environmental and Dynamic Effects Design Bases”

The safety I&C system is located in mild environments (MCR, I&C equipment rooms or mux rooms). The MCR, I&C equipment rooms, and mux rooms are designed to withstand the dynamic effects of missiles, pipe whipping or discharging fluids.

d. GDC 10, “Reactor Design”

The safety I&C system contributes to reactor design margin by providing conservatism in setpoint calculations and fault-tolerant features. Uncertainty methodology is described in the Uncertainty Methodology and Application for Instrumentation TeR (Reference 7) and setpoint methodology is described in the Setpoint Methodology for Plant Protection System TeR (Reference 8) and the CPC Setpoint Analysis Methodology for APR1400 (Reference 9).

e. GDC 13, “Instrumentation and Control”

The PPS consists of the RPS and the engineered safety features actuation system (ESFAS). The RPS is designed to monitor nuclear steam supply system (NSSS) operating conditions and to initiate reliable and rapid reactor shutdown if monitored variables or combinations of monitored variables deviate from the permissible operating range to a degree where a safety limit may be reached. The ESFAS is designed to monitor plant variables and to actuate engineered safety features (ESF) systems during a DBE.

The ESF-CCS performs the ESF actuation functions and executes component control through interfacing ESFAS portion of the PPS. It performs 2-out-of-4 voting logic for four division ESFAS initiation signals derived from the PPS and component control logic of ESF components.

The CPCS generates low departure from nucleate boiling ratio (DNBR) and high local power density (LPD) trip signals and sends them to the PPS.

The QIAS-P provides a continuous display of Type A, B and C accident monitoring variables.

f. GDC 15, “Reactor Coolant System Design”

The PPS functions to mitigate the consequences in the event of an accident. Safety analyses show that the design limits for the reactor coolant pressure boundary are not exceeded in the event of any conditions stated in ANSI/ANS 51.1-1983, “Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactor Plants”.

g. GDC 16, “Containment Design”

The PPS functions to mitigate the release of radioactive materials during an accident by actuating the CIVs which close the process lines penetrating the containment.

The PPS functions to actuate the containment spray actuation system (CSAS) which removes heat from the containment atmosphere. The heat removal process results in reduction of containment temperature and pressure below the design values during and following an accident.

h. GDC 19, “Control Room”

The MCR safety console (SC) is equipped with hardwired minimum inventory (MI) switches including manual reactor trip switches and manual ESF system-level actuation switches, and OMs shared by the PPS, CPCS, and ESF-CCS. The MCR also has operator consoles and large display panel (LDP). Monitoring for safe operation is implemented with the QIAS-P, QIAS-N and IPS displays. Also, the DPS, DIS, and diverse manual ESF actuation (DMA) switches are provided as protection against CCFs in the safety I&C system coincident with DBEs.

i. GDC 20, “Protection System Functions”

The safety I&C system functions are described in Section 4.

j. GDC 21, “Protection System Reliability and Testability”

The safety I&C system is designed to provide high functional reliability and in-service testability. The protection system is designed to comply with the requirements of IEEE Std. 603-1991 and other standards endorsed by RGs. No credible single failure will result in loss of the protection function. The protection divisions are independent from each other with respect to wire routing, sensor mounting and power supply.

Each division of the protection system, including the sensors, up to the reactor trip switchgear system (RTSS) and ESF actuation devices, is capable of being checked during reactor operation. Process sensors of each channel in the protection systems are checked in the IPS through comparison of the redundant process sensor values using the discrete indications and alarms in the MCR.

To minimize inadvertent actuation of an ESF system or an inadvertent reactor trip, the protection systems utilize a 2-out-of-4 coincidence voting logic. In addition, the channel under testing is bypassed so that the resulting voting logic becomes a 2-out-of-3 logic. This allows periodic testing without loss of the protective functions during power operation.

k. GDC 22, “Protection System Independence”

The safety I&C system complies with the independence requirements of IEEE Std. 603-1991. Four independent measurement channels with sensors, sensor power supplies, signal conditioning units, and bistable trip functions are provided for each protective parameter monitored by the protection systems except for the CEA position sensors which are two-fold redundant.

Power to the protection system divisions is provided by independent vital power supply buses.

l. GDC 23, “Protection System Failure Modes”

The PPS trip channels are designed to fall into a safe state in the event of loss of power supply. A failure is assumed to occur in only one channel (i.e., a single failure). This channel is placed into bypass mode which places the RPS/ESFAS local coincidence logic into a 2-out-of-3 configuration which retains the coincidence of two for trip initiation.

Failure modes and effects analysis (FMEA) for the safety I&C system is described in the DCD Chapter 7.

m. GDC 24, “Separation of Protection and Control System”

Complete electrical, physical and communication isolations are maintained between redundant safety divisions, and between the safety system and non-safety system as described in Section A.5.6.

n. GDC 25, “Protection System Requirements for Reactivity Control Malfunctions”

Shutdown of the reactor is accomplished by opening of the RTSS circuit breakers which interrupt power to the control element drive mechanism (CEDM) coils. Actuation of the circuit breakers is independent of any existing control signals. The safety I&C system is designed such that specified acceptable fuel design limits (SAFDLs) are not exceeded for any single malfunction of the reactivity control systems, including the withdrawal of a single full-strength or part-strength CEA.

o. GDC 28, “Reactivity Limits”

The power control system (PCS) integrates control systems that are designed to control the reactor power level, which includes the reactor regulating system (RRS), reactor power cutback system (RPCS) and digital rod control system (DRCS). The PCS is designed to limit the potential amount and rate of reactivity increase to assure that the effects of postulated reactivity accidents are bounded.

p. GDC 29, ‘Protection Against Anticipated Operational Occurrences”

Plant events, designated in ANSI/ANS 51.1-1983, have been considered in the design of the protection and reactivity control systems.

Consideration of redundancy, independence and testability in the design, coupled with careful component selection, overall system testing, and adherence to detailed quality assurance requirements assure that safety functions are accomplished in the event of anticipated operational occurrences (AOOs).

q. GDC 33, “Reactor Coolant Makeup”

The ESF-CCS performs the ESF safety injection function and executes component control through the interfacing ESFAS portion of the PPS. The ESF-CCS performs selective 2-out-of-4 coincidence logic for the four-division ESFAS initiation signals derived from the PPS and component control logic of ESF components.

r. GDC 34, “Residual Heat Removal”

The ESF-CCS performs the ESF shutdown cooling function and executes component control through the interfacing ESFAS portion of the PPS. The ESF-CCS performs selective 2-out-of-4 coincidence logic for the four-division ESFAS initiation signals derived from the PPS and component control logic of ESF components.

s. GDC 35, “Emergency Core Cooling”

The ESF-CCS performs the ESF shutdown cooling function and executes component control through the interfacing ESFAS portion of the PPS. The ESF-CCS performs selective 2-out-of-4 coincidence logic for the four-division ESFAS initiation signals derived from the PPS and component control logic of ESF components.

t. GDC 38, “Containment Heat Removal”

The ESF-CCS performs the ESF containment spray function and executes component control through the interfacing ESFAS portion of the PPS. The ESF-CCS performs selective 2-out-of-4 coincidence logic for the four-division ESFAS initiation signals derived from the PPS and component control logic of ESF components.

u. GDC 41, “Containment Atmosphere Cleanup”

The ESF-CCS performs the ESF containment spray function and executes component control through the interfacing ESFAS portion of the PPS. The ESF-CCS performs selective 2-out-of-4 coincidence logic for the four-division ESFAS initiation signals derived from the PPS and component control logic of ESF components.

v. GDC 44 “Cooling Water”

The ESF-CCS performs the ESF component cooling water and essential service water functions and executes component control through the interfacing ESFAS portion of the PPS. The ESF-CCS performs selective 2-out-of-4 coincidence logic for the four-division ESFAS initiation signals derived from the PPS and component control logic of ESF components.

3.3 Staff Requirements Memorandum and NUREG Reports

3.3.1 SRM on SECY 93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactors", Item II.Q, "Defense Against Common-Mode Failures in Digital Instrumentation and Control Systems"

Analyses and design features for D3 for the safety I&C system are provided in accordance with SECY 93-087, II.Q, as referenced by NUREG-0800.

The DPS automatically initiates a reactor trip on high containment pressure to assist the mitigation of the effects of a postulated CCF of the safety I&C system, concurrent with a main steam line break inside containment. The DPS also automatically initiates a safety injection actuation signal (SIAS) on low pressurizer (PZR) pressure in case of loss of coolant accident with CCF of the safety I&C system.

The DMA switches are provided to allow manual control capability to support ESF actuation in the event of a postulated CCF of the safety I&C system.

The DIS displays position 4 variables defined in Staff Requirements Memorandum (SRM) on SECY 93-087 in the event of a postulated CCF of the safety I&C system.

Compliance with SRM to SECY 93-087 and the diverse I&C system design features are addressed in the Diversity and Defense-in-Depth TeR.

The detailed CCF analysis methodology and the results are described in the CCF Coping Analysis TeR.

3.3.2 SRM on SECY 93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactors", Item II.T, "Control Room Annunciator (Alarm) Reliability"

The alarm systems are designed to meet the requirements of the SRM to SECY 93-087, Item II.T and are implemented in both the IPS and QIAS-N, and are designed as independent and diverse from each other. Therefore, the implemented alarm functions have redundancy and diversity features in the alarm system as specified in SRM on SECY-93-087, Item II.T.

The alarm systems are implemented in the software driven IPS and QIAS-N. The alarm functions in the IPS and QIAS-N are non-safety grade. The QIAS-N processors also provide redundant processing in a hot standby configuration. Multi-division information displayed by the QIAS-N is independently processed and displayed by the IPS. The QIAS-N receives the processed information from each division of four interface and test processors (ITPs) and alarms any discrepancies from its own corresponding multi-division information calculators. Therefore, the implemented alarm function complies with SRM on SECY 93-087, Item II.T redundancy requirement.

The IPS and QIAS-N in which the alarm function is implemented are designed as independent and diverse from each other. The IPS receives alarm signals through fiber optic data link using unidirectional Ethernet via MTP from the PPS and ESF-CCS. The QIAS-N also receives alarm signals through unidirectional SDL via each division of ITP from the PPS and ESF-CCS. Therefore, the alarm functions by the IPS and QIAS-N would not impact the safety systems such as the PPS or ESF-CCS as well as the performance of the QIAS-N functions.

3.3.3 NUREG-0737, "Clarification of TMI Action Plan Requirements," 1980

The QIAS-P displays variables indicating inadequate core cooling (ICC) to meet the requirements of Item II.F.2 "Instrumentation for Detection of Inadequate Core Cooling" of NUREG-0737.

3.3.4 NUREG-0737, Supplement No. 1, "Clarification of TMI Action Plan Requirements: Requirements for Emergency Response Capability", 1982.

The safety parameter display and evaluation system plus (SPADES+) displays variables and information on the IPS to comply with the requirements of Item I.D.2 "Plant Safety Parameter Display Console" of NUREG-0737 Supplement No. 1.

3.4 Regulatory Guides

3.4.1 Regulatory Guide 1.22, "Periodic Testing of Protection System Actuation Functions", Rev.0

The safety I&C system complies with the guidance of RG 1.22 as follows:

a. Provisions are made to permit periodic testing of the complete safety I&C system with the reactor operating at power or when shutdown.

b. The provisions are incorporated in the testing of the PPS, from sensor to actuation device, including the RTSS and the ESF-CCS.

c. The manual testing is administratively controlled to prevent a simultaneous trip in more than one redundant division.

d. When a division is bypassed for manual testing, the bypass status is indicated in the MCR.

e. ESF actuation devices which cannot be tested during reactor operation are tested during reactor shutdown.

3.4.2 Regulatory Guide 1.29, "Seismic Design Classification," Rev. 4

The seismic design classification is designated as seismic Category I or non-seismic Category I depending on the functional and/or physical integrity requirements of the plant I&C systems.

3.4.3 Regulatory Guide 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems", Rev. 1

The bypassed and inoperable status indication (BISI) is processed by the IPS and displayed on the LDP and information flat panel display (IFPD). The BISI provides system-level indication of deliberately introduced inoperability of the protection system which is required for safe operation of the plant. The system-level alarms are actuated when a component actuated by a protection system is bypassed or deliberately rendered inoperable.

3.4.4 Regulatory Guide 1.53, "Application of the Single Failure Criterion to Nuclear Power Plant Protection Systems", Rev. 2 - endorses IEEE Std. 379-2000 (Reaffirmed 2008)

The safety I&C system complies with the guidance of IEEE Std. 379-2000 "IEEE Standard Application of the Single Failure Criterion to Nuclear Power Generating Station Safety Systems", as endorsed by RG 1.53.

The safety I&C system is designed to assure both the reactor safety and prevention of a spurious reactor trip. Safety is assured by design meeting the requirements of IEEE Std. 603-1991. The prevention of a spurious trip due to a single failure is assured by 2-out-of-3 voting logic in conjunction with a channel bypass function designed complying with the guidance of IEEE Std. 379-2000.

3.4.5 Regulatory Guide 1.62, “Manual Initiation of Protective Action”, Rev. 1

Compliance with RG 1.62 is as follows:

a. Each of the RPS and ESFAS functions can be manually actuated.

b. Manual initiation of a protective action is provided at the system-level.

c. Manual switches are located on the MCR SC and RTSS. The reactor trip signal and main steam isolation signal (MSIS) are manually actuated at the remote shutdown console (RSC).

d. The amount of equipment common to the manual and automatic initiation paths is kept to a minimum, that is usually limited to the actuation devices. No single credible failure in the manual, automatic, or common portions of the protective system prevents initiation of a protective action by manual or automatic means.

e. Manual initiation requires a minimum of equipment consistent with the needs of a, b, c, and d above.

3.4.6 Regulatory Guide 1.75, “Criteria for Independence of Electrical Safety Systems”, Rev. 3 - endorses IEEE Std. 384-1992

The instrumentation for the safety-related electrical systems complies with the guidance of IEEE Std. 384-1992, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits”, as endorsed by RG 1.75.

The PPS and ESF-CCS is divided into four divisions which are physically located in different geographic fire zones in order to provide the physical separation and electrical independence.

The independence and separation of redundant Class 1E circuits within and between the PPS divisions or ESF-CCS divisions are accomplished primarily through the use of fiber optic technology and barriers or conduits. The optical technology ensures that no single credible electrical fault in the PPS or ESF-CCS division can prevent the circuitry in any other redundant division from performing its safety function.

The ESF-CCS cabinets provide separation and independence for the 2-out-of-4 actuation and component control logic of the redundant ESF system divisions. The component control logic of each division is contained in a separate cabinet. The redundant cabinets are physically separated from each other by locating them in separated zones.

The analog and digital signals of the protection system sent to non-Class 1E systems for status monitoring, alarm and display (e.g., IPS, QIAS-N) are isolated. Fiber optic isolation and other techniques are used to ensure no credible failures on the non-Class 1E side of the isolation device will affect the Class 1E side and that independence of the protection system is not jeopardized.

3.4.7 Regulatory Guide 1.97, “Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants,” Rev. 4 - endorses IEEE Std. 497-2002

The QIAS-P processes and displays Types A, B and C variables. Selection of these variables complies with the guidance identified in Clause 4.0 of IEEE Std. 497-2002, "IEEE Standard Criteria for Accident

Monitoring Instrumentation for Nuclear Power Generating Stations", as endorsed by RG 1.97 Rev.4. The QIAS-N also processes and displays variables for Types B and C. The QIAS-N displays selected variables of Types D and E to support plant safe shutdown and EOPs.

QIAS-P software for Types A, B and C variables is assigned to important-to-safety (ITS) class defined in the Software Program Manual (SPM) TeR (Reference 10), and meets the requirements of IEEE Std. 7-4.3.2-2003 and ASME NQA-1-2008 with 2009 addenda which are specified in Clause 9, Quality Assurance, of IEEE Std. 497-2002.

3.4.8 Regulatory Guide 1.100, "Seismic Qualification of Electrical and Active Mechanical Equipment and Functional Qualification of Active Mechanical Equipment for Nuclear Power Plants," Rev. 3 – endorses IEEE Std. 344-2004 (Reaffirmed 2009)

The safety I&C system is designated as seismic Category I to withstand the cumulative effects of five 1/2 safe shutdown earthquakes (SSEs) followed by one SSE without loss of safety functions or physical integrity.

3.4.9 Regulatory Guide 1.105, "Setpoints for Safety-Related Instrumentation", Rev. 3 - endorses Part 1 of ISA-S67.04-1994

The generation of safety system setpoints complies with ISA-S67.04-1994, "Setpoints for Nuclear Safety Related Instrumentation Used in Nuclear Power Plants".

The environment considered when determining errors is the most detrimental realistic environment calculated or postulated to exist until the worst case time of the required reactor trip or ESF system actuation. This environment may be different for different events analyzed. For the setpoint calculation, the accident environment error calculation for process equipment uses the environmental conditions up to the longest required time of trip or actuation that results in the largest errors, thus providing additional conservatism to the resulting setpoints.

For all temperature and pressure setpoints, the trip is initiated at a point that is not at saturation for the equipment. For level setpoints, no analysis setpoint is within 5% of the ends of the level span.

The uncertainty and setpoint methodologies are described in the Uncertainty Methodology and Application for Instrumentation TeR and Setpoint Methodology for Plant Protection System TeR, respectively.

3.4.10 Regulatory Guide 1.118, "Periodic Testing of Electric Power and Protection Systems", Rev. 3 - endorses IEEE Std. 338-1987

The safety I&C system is designed so that they can be periodically tested as prescribed by the criteria of IEEE Std. 338-1987, "IEEE Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems", as endorsed by RG 1.118.

The system is periodically and routinely tested to verify its operability. A complete division is tested without causing a reactor trip or ESF system actuation, and without affecting system operability or availability. Overlap in the RPS and ESFAS division tests is provided to assure that the entire division is functional. The testing scheme is described in Section 4.2.2.

When any one division is being tested, the remaining three divisions still provide the RPS and ESFAS function.

3.4.11 Regulatory Guide 1.151, “Instrument Sensing Lines,” Rev.1

The instrument sensing lines used to actuate or monitor safety-related systems are appropriately classified and are capable of withstanding the effects of the SSE to comply with the guidance of RG 1.151.

3.4.12 Regulatory Guide 1.152, “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants”, Rev. 3 - endorses IEEE Std. 7-4.3.2-2003

The methods for specifying, designing, implementing, verifying, validating and maintaining the safety I&C system software comply with the guidance of IEEE Std. 7-4.3.2-2003, as endorsed by RG 1.152. The life cycle process for the safety I&C system application software is described in the SPM TeR.

The compliance with RG 1.152 including secure development and operational environment (SDOE) is described in the SPM TeR.

A deviation is taken to the last paragraph of Clause 5.3.3 of IEEE Std. 7-4.3.2 which states the “V&V requirements for the highest integrity level (level 4) apply to systems developed using this standard”. This deviation applies to the software qualification of the OM, MTP, ITP, ESF-CCS soft control module (ESCM), and QIAS-P. The description and justification for this deviation is provided in the SPM TeR.

3.4.13 Regulatory Guide 1.153, “Criteria for Safety Systems”, Rev. 1 – endorses IEEE Std. 603-1991

The RG 1.153 endorses IEEE Std. 603. The compliance with the requirements of IEEE Std. 603-1991 is described in Appendix A.

3.4.14 Regulatory Guide 1.168, “Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants”, Rev. 2 - endorses IEEE Std. 1012-2004 and IEEE Std. 1028-2008

The software verification, validation, reviews and audits process for the safety I&C system complies with the guidance of IEEE Std. 1012-2004 and IEEE Std. 1028-2008 as endorsed by RG 1.168. The verification & validation (V&V) plan, process and activities are described in the SPM TeR.

The software hazard analysis (SHA) for ITS class software, which does not perform safety functions such as reactor trip and ESF actuation, is not performed. However, ITS class software which could impact safety-critical class software is analyzed in the system-level SHA of concept phase for the safety-critical class software.

3.4.15 Regulatory Guide 1.169, “Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants”, Rev. 1 - endorses IEEE Std. 828-2005

The software configuration management process for the safety I&C system complies with the guidance of IEEE Std. 828-2005 as endorsed by RG 1.169. The configuration plan and methods are described in the SPM TeR.

3.4.16 Regulatory Guide 1.170, “Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants”, Rev. 1 - endorses IEEE Std. 829-2008

The software test documentation for the safety I&C system complies with the guidance of IEEE Std. 829-2008 as endorsed by RG 1.170. The test documentation is described in the SPM TeR.

3.4.17 Regulatory Guide 1.171, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants", Rev. 1 - endorses IEEE Std. 1008-1987 (Reaffirmed 2002)

The software unit testing process for the safety I&C system complies with the guidance of IEEE Std. 1008-1987 as endorsed by RG 1.171. The unit testing approaches are described in the SPM TeR.

For ITS class software, the unit testing is performed for every software feature, but module testing is not performed. The unit level testing verifies the functionality of the software as described in the SPM TeR.

3.4.18 Regulatory Guide 1.172, "Software Requirements Specifications for Digital Computer Software and Complex Electronics Used in Safety Systems of Nuclear Power Plants", Rev. 1 - endorses IEEE Std. 830-1998 (Reaffirmed 2009)

The software requirements specifications for the safety I&C system are developed in compliance with the guidance of IEEE Std. 830-1998 as endorsed by RG 1.172.

3.4.19 Regulatory Guide 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants", Rev. 1 - endorses IEEE Std. 1074-2006

The software life cycle model for the safety I&C system is consistent with the guidance of IEEE Std. 1074-2006 as endorsed by RG 1.173. The software life cycle activities are described in the SPM TeR.

3.4.20 Regulatory Guide 1.180, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems", Rev. 1-endorses MIL Std. 461E-1999, IEEE Std. 1050-1996, IEC 61000-Parts 3, 4 and 6, IEEE Std. C37.90.1-2002, IEEE Std. 62.36-2000, IEEE Std. C62.41.1-2002, IEEE Std. C62.41.2-1991, IEEE Std. C62.45-1992

The safety I&C system equipment are qualified in compliance with the EMI/RFI guidance of RG 1.180 and the endorsed standards. The equipment qualification is described in Section 6.

3.4.21 Regulatory Guide 1.189, "Fire Protection for Nuclear Power Plants," Rev. 2

The safety I&C system equipment are designed to comply with the guidance of RG 1.189. Details of the compliance with RG 1.189 are described in the DCD Chapter 9.

3.4.22 Regulatory Guide 1.204, "Guidelines for Lightning Protection of Nuclear Power Plants," Rev. 0

The safety I&C system equipment are designed to comply with the guidance of RG 1.204. Details of the compliance with RG 1.204 are described in the DCD Chapter 8.

3.4.23 Regulatory Guide 1.206, "Combined License Applications for Nuclear Power Plants (LWR Edition)", Rev. 0

The DCD (Reference 11) including this report is prepared to comply with the guidance described in RG 1.206 together with NUREG-0800 Standard Review Plan (SRP) in order for NRC to evaluate and confirm the safety determination.

3.4.24 Regulatory Guide 1.209, "Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants", Rev. 0 - endorses IEEE Std. 323-2003 (Reaffirmed 2008)

The safety I&C system equipment is qualified to the guidance of IEEE Std. 323-2003, as endorsed by RG 1.209. Since the equipment is located in the MCR and/or I&C equipment rooms, there is no change in the environment due to plant accidents. The safety I&C system equipment are tested and analyzed to meet the mild environmental qualification requirements.

3.5 Branch Technical Positions

3.5.1 BTP 7-1 Guidance on Isolation of Low-Pressure Systems from the High-Pressure Reactor Coolant System

The I&C systems are designed to meet the guidance of BTP 7-1. The interlock systems are described in Section 7.6 of the DCD.

3.5.2 BTP 7-2 Guidance on Requirements of Motor-Operated Valves in the Emergency Core Cooling System Accumulator Lines

The I&C systems are designed to meet the guidance of BTP 7-2. The interlocks associated with the safety injection tank isolation valve are described in Section 7.6 of the DCD.

3.5.3 BTP 7-3 Guidance on Protection System Trip Point Changes for Operation with Reactor Coolant Pumps out of Service

The reactor is not permitted to operate with a reactor coolant pump out of service. The PPS trips the reactor by low reactor coolant flow. Therefore, BTP 7-3 is not applicable.

3.5.4 BTP 7-4 Guidance on Design Criteria for Auxiliary Feedwater Systems

The I&C systems are designed to meet the guidance of BTP 7-4. Section 7.3 of the DCD describes the actuation of the auxiliary feedwater system and the FMEA of the ESF-CCS.

3.5.5 BTP 7-5 Guidance on Spurious Withdrawals of Single Control Rods in Pressurized Water Reactors

The I&C systems are designed to meet the guidance of BTP 7-5. Section 7.7 of the DCD describes the reactivity control system. Section 15.4 of the DCD describes the safety analysis results of reactivity anomalies.

3.5.6 BTP 7-6 Guidance on Design of Instrumentation and Controls Provided to Accomplish Changeover from Injection to Recirculation Mode

The APR1400 has no recirculation mode, therefore BTP 7-6 is not applicable.

3.5.7 BTP 7-8 Guidance for Application of Regulatory Guide 1.22

Provisions are made to permit periodic testing of the complete safety I&C system for all functions with the reactor operating at power or when shutdown.

3.5.8 BTP 7-9 Guidance on Requirements for Reactor Protection System Anticipatory Trips

All reactor trip functions of the PPS from the sensor to the final actuated devices are designed to meet the requirements of IEEE Std. 603-1991.

3.5.9 BTP 7-10 Guidance on Application of Regulatory Guide 1.97

The QIAS-P complies with the guidance of RG 1.97 Rev. 4 with a deviation described in Section 3.4.7.

3.5.10 BTP 7-11 Guidance on Application and Qualifications of Isolation Devices

The isolation devices to protect the safety I&C system are qualified to comply with the guidance of IEEE Std. 384-1992 as endorsed by RG 1.75. Isolation devices are designed to comply with the guidance of IEEE Std. C37.90.1-2002, IEEE Std. C62.23-1995, IEEE Std. C62.36-2000, IEEE Std. C62.41-1-2002, IEEE Std. C62.41-2-2002, and IEEE Std. C62.45-2002.

3.5.11 BTP 7-12 Guidance on Establishing and Maintaining Instrument Setpoints

Setpoint calculations are described in the Setpoint Methodology for Plant Protection System TeR.

3.5.12 BTP 7-13 Guidance on Cross-Calibration of Protection System Resistance Temperature Detectors

The cross-calibration techniques used for periodically verifying the performance (accuracy and response time) of resistance temperature detectors (RTDs) comply with this guidance.

3.5.13 BTP 7-14 Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems

The compliances to this guidance are described in Sections 3.4.14 through 3.4.19.

3.5.14 BTP 7-17 Guidance on Self-Test and Surveillance Test Provisions

The compliances to this guidance are described in Sections 3.2.j, 3.4.1, and 3.4.10.

BTP 7-17 states, “The safety classification and quality of the hardware and software used to perform periodic testing should be equivalent to that of the tested system. The design should maintain channel independence, maintain system integrity, and meet single failure criterion (SFC) during testing”.

The MTP and ITP are used to perform the periodic testing of the safety I&C system. Hence, the MTP, ITP, and associated communication path software should be qualified to comply with the guidance of IEEE Std. 7-4.3.2-2003, as endorsed by RG 1.152, and be classified as safety-critical class.

The MTP and ITP software is classified as ITS class as defined in the SPM TeR. The ITS class software does not meet the integrity level 4 V&V guidance of IEEE Std. 1012-2004. Testing of ITS class software is not the same as that of safety-critical class software. The testing for the safety-critical class and ITS class software is described in the SPM TeR.

3.5.15 BTP 7-18 Guidance on the Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems

The safety I&C system is implemented on a common programmable logic controller (PLC) platform which is qualified and dedicated for nuclear application as described in Section 8 and the Common Qualified Platform Topical Report (Reference 12).

3.5.16 BTP 7-19 Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems

Compliance with this criterion is addressed in the Diversity and Defense-in-Depth TeR.

3.5.17 BTP 7-21 Guidance on Digital Computer Real-Time Performance

Real-time performance is determined by performing response time analysis for all safety functions. An analysis for each function is performed, which demonstrates the actual system response time is less than the response time requirements. The response time analyses are described in the Response Time Analysis TeR (Reference 13).

3.6 Interim Staff Guidance

3.6.1 DI&C-ISG-04, Digital Instrumentation and Control, Highly-Integrated Control Rooms – Communication Issues

The compliance with DI&C-ISG-04 is addressed in Appendix C of this report.

4 I&C System Description

4.1 Overall I&C System

As shown in Figure 4-1, the I&C system consists of the safety I&C system, non-safety control system, diverse actuation system, and human-system interfaces (HSI) in the MCR and remote shutdown room (RSR).

The I&C system uses full digital technology, however the limited hardware switches are used to meet the safety system design criteria in IEEE Std. 603-1991 and results of the D3 analysis.

The safety I&C system is based on a common PLC platform which has been dedicated for nuclear safety systems as described in Section 8. The safety I&C system software is designed, verified and validated with industry standard software development and V&V process endorsed by the NRC. The safety I&C systems implemented on the common PLC platform consist of the PPS, ESF-CCS, CPCS and QIAS-P. The QIAS–N is also implemented on the common PLC platform even though it is a non-safety system, because it displays the plant’s important parameters and maintains diversity from the IPS. Also the control panel multiplexer (CPM), control channel gateway (CCG), and ITP use the common PLC platform.

Many non-safety I&C systems are implemented in a distributed control system (DCS) based common platform which has been proven by operating experience from the nuclear industry as well as other industries. The DCS supports component-level control, automatic process control, and high-level group control. The DCS is designed in a redundant and fault-tolerant architecture to achieve high reliability and prohibit the failure of a single component to cause a spurious plant trip. The non-safety systems implemented in the DCS are the PCS, NSSS process control system (NPCS), and process–component control system (P-CCS). However, the DPS and DIS use a non-software based field programmable gate array (FPGA) platform which is diverse from PLC and DCS.

There are systems which are not installed on a common I&C platform. They have their unique hardwares and fulfill the specific system design requirements. These non-standard systems typically include the ex-core neutron flux monitoring system (ENFMS), NSSS integrity monitoring system (NIMS), auxiliary process cabinet – safety (APC-S), and component interface module (CIM).

The IPS is implemented in the DCS platform and consists of networking equipment, computer servers, flat panel displays (FPDs) and peripherals to provide the operator with the plant information and soft control for the non-safety components.

The plant-wide data networks are composed of safety system data networks (SDNs, i.e., AF100) and non-safety data communication network-information (DCN-I). The SDN is independent and diverse from the DCN-I. The DCN-I utilizes different communication hardware, software and communication protocol from the SDN.

The I&C architecture exhibits the following independence, separation and diversity features:

- Each of the safety systems includes four divisions which are physically and electrically independent from each other to meet the SFC.
- A safety division does not receive any information or signals originating from another safety division or non-safety division to perform its safety function except the voting logic.
- The data communication networks for the safety system and the non-safety system are independent and diverse from each other. There is no potential for the deterministic cyclic processing of the safety function to be disrupted by any data communication. One way

communication via the serial data link (SDL, i.e., HSL) from safety systems to non-safety systems (i.e., QIAS-N) and buffering circuit using dual-ported memory are commonly used to prevent endangering the safety function. The other means from safety to non-safety data communication is via the plant computer datalink using the unidirectional protocol from the MTP.

- The DPS is diverse from the safety I&C system in aspects of trip mechanism, hardware and software.

- In addition to the DPS, the hardwired DMA switches and the DIS are provided on the MCR SC to cope with CCF of the safety I&C system.

The safety I&C system has the interface with redundant portions of the safety system and with non-safety system. Table 4-1 and Table 4-2 provide the specific interface information.

All figures provided in Section 4 are identical for all channels or divisions. If a figure provided is not identical for all channels or divisions, a note is provided in the figure to indicate the difference.

Table 4-1 Interface between Redundant Portions of the Safety System

No	From	To	Signal Description	Interface Type	Reference Section
1	PPS BP	PPS LCL	Partial trip	SDL	4.2.2.1
2	PPS	ESF-CCS GC	ESFAS initiation	SDL	4.1.1.2, 4.2.3.2, 4.2.3.3, 4.2.4
3-1	ITP Division A	ITP Division B	CIV signals (74 signals)	SDL	4.5.2
3-2	ITP Division C	ITP Division B	CIV signals (10 signals)	SDL	4.5.2
3-3	ITP Division D	ITP Division B	CIV signals (9 signals)	SDL	4.5.2
3-4	ITP Division B	ITP Division A	CIV signals (69 signals)	SDL	4.5.2
3-5	ITP Division C	ITP Division A	CIV signals (10 signals)	SDL	4.5.2
3-6	ITP Division D	ITP Division A	CIV signals (9 signals)	SDL	4.5.2
4	CPP in CPCS	CPC/CEAC in CPCS	Digitized RSPT values	SDL	4.3.2.1

Table 4-2 Interface between Safety and Non-safety system

No.	From	To	Signal Description	Interface Type	Reference Section
1	PPS	DRCS Remote I/O Cabinet	CWP contact	Hardwired	4.2.4
2	DIS	QIAS-P	Transfer command, HJTC heater power control	Hardwired	Figure 4-19, Table 4-6
3	QIAS-P	DIS	CETs, HJTCs, control status	Hardwired	Figure 4-19, Table 4-6
4	P-CCS	ESF-CCS	Non-safety control signals for CVCS, steam generator blowdown system, condenser vacuum system, fuel handling area HVAC system, fire protection system, process sampling system, and class 1E 4.16kV system	Hardwired	4.4.4.12
5	DMA Switches	CIM	Actuation signals for ESF components	Hardwired	4.1.1.7
6	DPS	CIM	Component control signals	Hardwired	4.1.1.7
7	ITP	QIAS-N	PPS status alarm, CPC data, Type A,B,C variables, ICC-related variables, operating ESF-CCS status for EOP, plant safe shutdown, cabinet trouble alarm, system in test	SDL	3.3.2, 4.1.1.4, 4.2.2.1, 4.2.3.5, 4.3.1.6,
8	MTP	DCS Gateway Server of IPS	PPS status alarm, CPC data, Type A,B,C variables, ICC-related calculation variables, control cabinet alarms, system in test	Ethernet Data Link	3.3.2, 4.3.1.5
9	IFPD (on each operator console)	ESCM (on each operator console)	Safety component selection information	Ethernet Data Link	4.1.2.7
10	PPS	TCS	Turbine trip signal	Hardwired	4.2.1.1
11	ENFMS	NIMS	Sub-channel neutron flux signal	SDL	A.5.6

4.1.1 Safety I&C Systems

4.1.1.1 Plant Protection System

The PPS consists of four redundant divisions that perform the necessary bistable, coincidence, initiation logic, maintenance and test function.

The PPS initiates reactor trip and system-level ESF actuation functions when a safety limit is exceeded by the plant conditions. To detect such conditions, the system utilizes measurements of the reactor core, reactor coolant system, main steam supply system, and containment building parameters.

Each PPS redundant division receives the process and discrete signals directly from field sensors or via the APC-S, ENFMS, and CPCS. The PPS provides the reactor trip signals to the RTSS using hardwired cables and ESFAS initiation signals to the ESF-CCS via fiber optic SDLs.

4.1.1.2 Engineered Safety Features - Component Control System

The ESF-CCS consists of four independent divisions that perform additional 2-out-of-4 voting logic, component control logic, and priority logic function.

The group controller (GC) of each ESF-CCS division receives four division ESFAS initiation signals derived from the ESFAS portion of the PPS and performs additional selective 2-out-of-4 coincidence logic to generate the ESF actuation signal. The GC also receives two division ESFAS initiation signals derived from the radiation monitoring system (RMS) and performs 1-out-of-2 logic to generate the ESF actuation signal. The ESF actuation signals are transmitted to the loop controller (LC) of the ESF-CCS. The LC executes the component control logic and outputs the component control signal to the CIM. The component control logic includes the priority logic for the operator’s manual control signal and ESF actuation signal. The ESF-CCS soft control module (ESCM) on the operator console generates a component control signal of safety components by manual operator actions.

4.1.1.3 Core Protection Calculator System

The CPCS has four redundant channels that compute the DNBR and LPD values using process values, reactor coolant pump (RCP) speed, CEA position and ex-core neutron flux.

The CPCS compares the DNBR and LPD values against setpoints to determine if fuel design limits are exceeded. When these values exceed setpoints, a trip signal is transmitted to the PPS using hardwired cables.

4.1.1.4 Qualified Indication and Alarm System - P

The QIAS-P, which has two independent divisions A and B, is implemented on the common PLC platform for the safety system. The QIAS-P processes the plant parameters that are input from the safety I&C system via SDN, APC-S via hardwired interface, and process instrumentation directly. The safety FPDs for the QIAS-P are installed on the MCR SC.

The QIAS-P transmits data to the QIAS-P safety FPD via the SDN for RG 1.97, Rev. 4, Types A, B and C variables.

The QIAS-P also transmits the sensor signals and their calculated variables to the IPS and QIAS-N through the MTP and ITP, respectively. In the case of the IPS, this data communication is a unidirectional protocol from the MTP. In the case of the ITP, the SDL data communication is used to transmit data to the QIAS-N.

4.1.1.5 Auxiliary Process Cabinet - Safety

The APC-S consists of four redundant channels designated as Class 1E. It receives safety-related sensor signals and distributes them to the PPS, CPCS, ESF-CCS, QIAS-P, and DIS via hardwired interfaces.

It includes signal conditioning/splitting equipment and the associated power supplies for sensor input. Qualified isolation devices are provided within the APC-S to interface safety signals to the non-safety systems.

The APC-S does not include any functional programmable unit. Therefore, the APC-S is not susceptible to software CCF. A functional programmable unit is a computer that consists of one or more associated processing units and peripheral equipment.

The signal conditioning/splitting and isolating devices of the APC-S are conventional analog circuits which are not developed from software-based development systems. Therefore, the APC-S is not susceptible to a postulated software CCF.

4.1.1.6 Ex-core Neutron Flux Monitoring System

The ENFMS provides a means to measure reactor power level by monitoring the neutron flux leakage from the reactor vessel for reactor control, protection and information display.

The ENFMS consists of four redundant safety channels.

4.1.1.7 Component Interface Module

The CIM is a hardware based safety module for ESF component control (i.e., there is no software). The CIM is implemented using simple hardware-based non-digital technology, so that there is no potential for a software design defect that could result in a CCF of the CIM. The CIM receives component control signals from the ESF-CCS, DPS, DMA switches, and front panel control switch. The CIM prioritizes between input signals according to prioritization and transmits an output signal to the plant component according to the priority mode.

4.1.1.8 Reactor Trip Switchgear System

The RTSS consists of four divisions. The RTSS is designed as Class 1E. The RTSS receives the reactor trip signals from the PPS, manual reactor trip switches, and the DPS through hardwired cables. The PPS interfaces with the undervoltage trip device of RTSS breakers. The DPS interfaces with the shunt trip device of the RTSS breakers. The RTSS disconnects the power to the DRCS for dropping CEAs into the reactor core by RPS signals from the PPS or manual reactor trip signals from the MCR or RSR.

4.1.2 Non-safety Control and Monitoring System

4.1.2.1 Power Control System

The PCS integrates control systems that are designed to control the reactor power level, which includes the RRS, RPCS and DRCS.

The RRS/RPCS logic and DRCS cabinets include the redundant DCS controllers with associated input and output (I/O).

The PCS is distributed to separate controller groups to ensure that a single failure does not cause plant conditions more severe than those considered in the safety analysis.

4.1.2.2 NSSS Process Control System

The NPCS consists of the pressurizer pressure control system (PPCS), pressurizer level control system (PLCS), feedwater control system (FWCS), steam bypass control system (SBCS), boron dilution alarm system, and single control loops of the chemical and volume control system (CVCS).

The NPCS is implemented as a part of the P-CCS.

The NPCS is distributed to separate controller groups to ensure that a single failure does not cause plant conditions more severe than those considered in the safety analysis.

4.1.2.3 Process - Component Control System

The P-CCS is designed to control non-safety components such as pumps, valves, heaters, and fans. The P-CCS performs data acquisition from field instruments and discrete/continuous controls, and provides process variables and their status information to the IPS and QIAS-N for plant monitoring.

Standardized component control logic and I/O interfaces are provided for the various types of components to be controlled. Manual operator controls for the P-CCS are performed through the soft control display on the IFPD driven by the IPS.

The P-CCS is distributed to separate controller groups to ensure that a single failure does not cause plant conditions more severe than those considered in the safety analysis.

4.1.2.4 Fixed In-core Detector Amplifier System

The fixed in-core detector amplifier system (FIDAS) monitors the fixed in-core neutron detector current signals, performs the necessary signal conversion to engineering unit values and transmits them to the IPS. The IPS uses these signals for the core operating limit supervisory system (COLSS) to estimate the gross power distribution and thermal margin in the core, and fuel burn-up in each fuel assembly.

Neutron flux in the reactor core is measured by the fixed in-core neutron detectors. Detectors are spaced radially and axially to permit representative flux mapping of the entire core.

4.1.2.5 Qualified Indication and Alarm System - Non-safety

The QIAS-N is a single division indication and alarm system that supports alternative plant operation if the IPS is unavailable. It provides the information required for EOP execution, safe shutdown, and important human actions under unavailable conditions of the operator consoles. The QIAS-N also provides a display of all RG 1.97, Rev.4, Types A, B and C variables. The QIAS-N displays selected variables of RG 1.97, Rev. 4, Types D and E variables to support the performing plant safe shutdown and EOPs.

The QIAS-N receives divisionalized information from the four safety divisions via their ITPs for safety variables and from the QIAS-N MTP for non-safety variables.

The QIAS-N is implemented on the common PLC platform for as the safety system. The QIAS-N HSI is provided by the FPDs on the SC.

4.1.2.6 NSSS Integrity Monitoring System

The NIMS detects selected conditions which indicate a deterioration or which could lead to a deterioration of the RCS pressure boundary.

The system consists of internal vibration monitoring system (IVMS), acoustic leak monitoring system (ALMS), loose parts monitoring system (LPMS), and RCP vibration monitoring system (RCPVMS).

4.1.2.7 Information Processing System

The IPS is the DCS based data processing system and HSI system that serve to provide operational means for control and monitoring of the plant. It consists of networking equipment, along with an alarm server, application program server, data base (DB) server, data link server and the IFPD installed on the operator consoles. The information is derived from other I&C systems and self-contained algorithms called application programs.

The IFPD provides the operator with the HSI resources including process mimic displays, alarms, and historical data access. It is designed to enhance overall plant operation, availability and efficiency. Also it provides the soft control templates for manual component controls. The soft control of the IFPD is used for control associated with the P-CCS controllers directly attached to the non-safety DCS platform network. The IFPD also interfaces to the ESCM to send safety component selection information through Ethernet network. The communication independence compliance with DI&C-ISG-04 is described in Appendix C.5.1.5.

When there is an IFPD failure, operators can use other IFPDs that are not malfunctioning. Due to the importance of IFPDs, operators are alerted to following IFPD malfunctions.

- Failure of network interface card
- Failure of hard disk drive
- Failure of display adapter
- Failure of keyboard video mouse
- Failure of keyboard/mouse
- Failure of FPD
- Failure of RAM
- Failure of disk controller
- Failure of CPU

The CCF of the non-safety control systems implemented on DCS platform is analyzed and the results are described in the Control System CCF Analysis TeR (Reference 14).

4.1.3 Diverse Actuation System

A detailed design description for the diverse actuation system (DAS) is described in the Diversity and Defense-in-Depth TeR. The DAS is implemented as a non-safety system.

4.1.3.1 Diverse Protection System

The DPS is designed to mitigate the effects of an ATWS event characterized by an AOO followed by a failure of the reactor trip portion of the protection system. In addition, the DPS is designed to include functions to assist in the mitigation of the effects of a postulated software CCF of the digital safety I&C system coincident with the DBEs analyzed in the DCD Chapter 15.

Pressurizer pressure and containment pressure are respectively monitored by a bistable comparator to generate a reactor trip signal to each channel whenever a pressure exceeds a predetermined setpoint. The DPS reactor trip signal is hardwired to the shunt trip device of the RTSS breakers.

The DPS AFAS automatically initiates auxiliary feedwater when the SG level falls below a predetermined value. The DPS SIAS also initiates safety injection actuation when pressurizer pressure decreases below a predetermined value. These DPS ESF actuation signals are hardwired to the CIM through the isolation device.

The DPS also automatically initiates a turbine trip signal to the turbine control system (TCS). The turbine trip signal is generated from the DPS when the DPS generates a reactor trip signal.

The DPS setpoints are specified so that the PPS automatic trip/actuation signals occur before the DPS automatic trip/actuation signals.

Figure 4-2 shows the design concept of diversity between the protection system and the DPS.

4.1.3.2 Diverse Indication System

The DIS is a single channel of non-safety equipment to meet the display requirements for BTP 7-19 Point 4 on D3 for the safety I&C system. The DIS is diverse from the safety I&C system.

The DIS provides plant operators with the following information that are not subject to a postulated software CCF in the common PLC platform because the displays are independent and diverse from the safety I&C system.

- Inadequate core cooling monitoring information
- Subset of AMI parameter information
- Subset of emergency operation-related variables

4.1.3.3 Diverse Manual ESF Actuation Switches

The DMA switches consist of conventional hardwired switches on the MCR SC for manual actuation of the ESF components, which are required for coping with postulated software CCFs in the safety I&C system. The DMA switches actuate components to manage critical safety functions and to actuate components that bring the plant in safe shutdown condition.

The DMA switches are independent and diverse from the manual actuation function within the safety I&C system. The DMA switches signals are hardwired to the CIM through the isolation device.

4.1.4 Human-System Interfaces

The HSI is designed in accordance with the advanced control design approach based on compact workstation-based operator consoles using the soft control and distributed digital control system. The compact workstation-based operator console HSI provides a convenient operating environment to facilitate display of plant status information for the operator such that the operability can be improved by reducing human error. And the HSI has sufficient diversity to demonstrate defense-in-depth protection against CCF of the safety I&C system.

The HSI comprises the following operating facilities to support the operating staff for efficient and safe plant operation.

- Compact workstation-based operator consoles
- A LDP for display of overall plant operational and safety assessment data
- A SC for maintaining the plant in safe condition, which is functionally independent of the operator consoles

The operator console design uses multiple identical and redundant compact workstations. Each console allows access to all information and controls necessary for one operator to monitor and control all processes associated with nuclear plant operation and safety. Each compact operator console comprises four IFPDs, four ESCMs, and pointing devices respectively. The IFPDs provide plant operating status information to the operator via graphical flow diagrams, alarm displays, plant summary displays, computerized procedures and non-safety soft control.

Also, the IFPDs inform operators of the status of the safety I&C system via system status displays which are a top level heath displays on the IFPDs. When IFPDs are inoperable, the QIAS-N FPDs and the OMs on the safety console provide required system status and plant operating status information sent from the PPS, ESF-CCS, QIAS-P, and CPCS.

The IFPDs only send identification data of component to the ESCMs to support operator's manual action. This identification data is used for bringing up the control template on the ESCM. It is unidirectional communication from the IFPD to the ESCM.

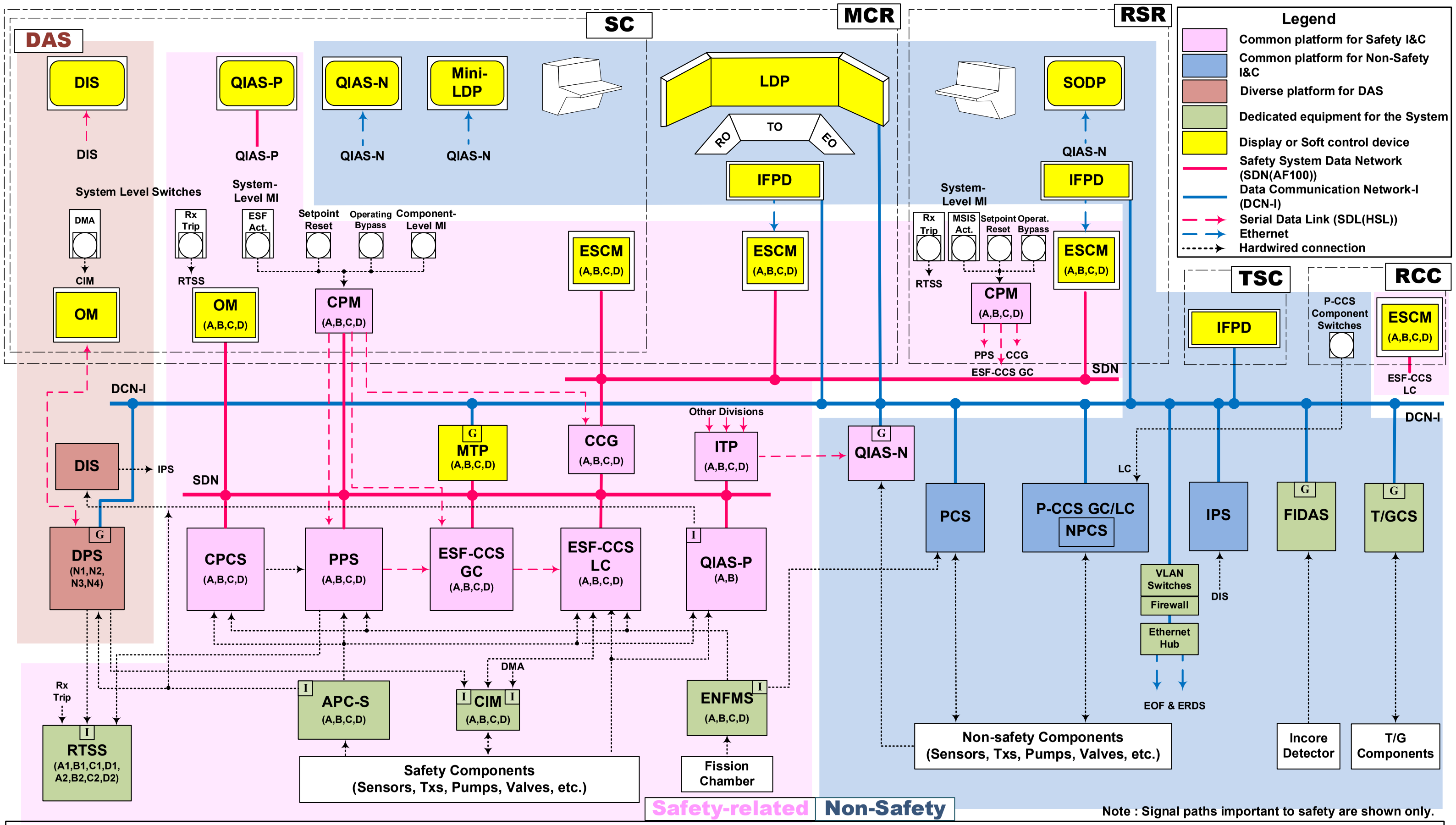
One set (one per division) of four ESCM FPDs also is installed on each operator console to provide manual control capability for controlling of safety component.

The LDP continuously displays spatially dedicated information that provides the status of the plant critical safety functions, plant operation mode, key operating parameters and status, and trend displays, etc. In addition to providing an overview and safety information, the LDP provides fixed indication of high priority alarms via alarm tiles and incorporates a variable display section to support operating goals in progress.

A SC is located in the left side of the MCR. Class 1E hardwired switches are provided as fixed position controls on the SC for manual actuation of the safety systems and components. Hence the MCR operators can still mitigate the accident and maintain the plant in safe condition using the SC in the unlikely event that all operator consoles are postulated to fail.

The OMs for PPS/CPCS/ESF-CCS, FPDs for QIAS-P and QIAS-N displays are also provided on the SC.

The DPS-OM, DMA switches and FPD for DIS are installed on the SC to provide diverse manual control and indication.



Note : Signal paths important to safety are shown only.

APC-S: Auxiliary Process Cabinet - Safety
CCG: Control Channel Gateway
CIM: Component Interface Module
CPCS: Core Protection Calculator System
CPM: Control Panel Multiplexer
DAS: Diverse Actuation System
DIS: Diverse Indication System
DCN-I: Data Communication Network-Information
DMA: Diverse Manual ESF
DPS: Diverse Protection System
ENFMS: Ex-core Neutron Flux Monitoring System
EOF: Emergency Operation Facility
ERDS: Emergency Response Data System
ESCM: ESF-CCS Soft Control Module
ESF-CCS: Engineered Safety Features - Component Control System
FIDAS: Fixed In-core Detector Amplifier System
G: Gateway
GC: Group Controller
I : Isolator
IFPD: Information Flat Panel Display
IPS: Information Processing System
ITP: Interface and Test Processor
LC: Loop Controller
LDP: Large Display Panel
MCR: Main Control Room
MI: Minimum Inventory
MTP: Maintenance and Test Panel
NPCS: NSSS Process Control System
MSIS: Main Steam Isolation System
OM: Operator Module
P-CCS: Process-Component Control System
PCS: Power Control System
PPS: Plant Protection System
QIAS-P/N: Qualified Indication & Alarm System – P / Non-safety
RCC: Remote Control Center
RSR: Remote Shutdown Room
RTSS: Reactor Trip Switchgear System
Rx: Reactor
SC: Safety Console
SODP: Shutdown Overview Display Panel
T/GCS: Turbine/Generator Control System
TSC: Technical Support Center, Txs: Transmitter

Rev.1

Figure 4-1 APR1400 I&C System Overview Architecture

TS

Figure 4-2 Diversity Design Concept between Protection System and Diverse Protection System

4.2 Plant Protection System

4.2.1 Functions

The PPS generates reactor trip (RT) and ESFAS initiation signals automatically whenever monitored process variables exceed safety limits. It is also equipped with means for manual initiation of each protective action.

The PPS provides outputs for operator monitoring of the status of the PPS and receives manually entered inputs for limited operator intervention in the automatic RT and ESF actuation such as an operating bypass and setpoint reset.

The PPS provides alarms and, in some cases limiting signals to control systems, whenever the selected plant process parameters approach the predetermined levels where plant protection would be required.

The PPS has a test capability for determining system operability and hardware diagnostic testing.

The PPS comprises two subsystems, the RPS and ESFAS, as shown in Figure 4-3.

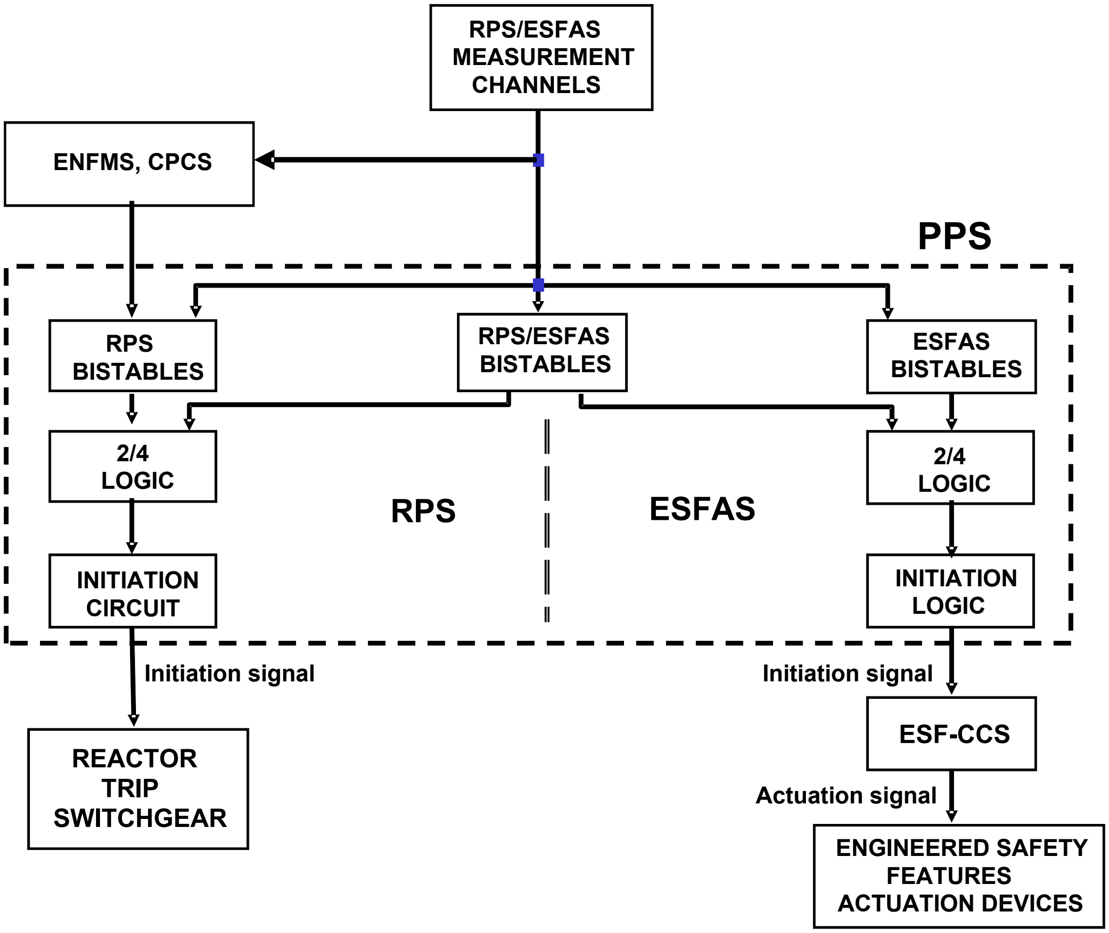


Figure 4-3 PPS Functional Block Diagram

Table 4-3 Summary of RPS and ESFAS Initiation Function

Reactor Trip/ESFAS Initiation Parameter	RPS	ESFAS	Input from
Variable Over Power	RT		ENFMS
High Logarithmic Power Level	RT		ENFMS
High Local Power Density (LPD)	RT		CPCS
Low Departure from Nucleate Boiling Ratio (DNBR)	RT		CPCS
High PZR Pressure	RT		APC-S
Low PZR Pressure	RT	SIAS, CIAS	APC-S
High SG1&2 Level	RT	MSIS	APC-S
Low SG1&2 Level	RT	AFAS	APC-S
Low SG1&2 Pressure	RT	MSIS	APC-S
Low Reactor Coolant Flow	RT		APC-S
High Containment Pressure	RT	MSIS, CIAS	APC-S
High High Containment Pressure		CSAS	APC-S

4.2.1.1 RPS Function

The RPS initiates a reactor trip to prevent fuel damage during AOOs in compliance with the requirements of GDC 20 of 10 CFR 50, Appendix A. The PPS also provides a reactor trip to assist the ESFAS in limiting fuel damage and the release of significant amounts of radioactivity during accidents.

The RPS initiates a reactor trip for the conditions listed below.

- Variable over power (rate limited setpoint)
- High logarithmic power level (fixed setpoint)
- High local power density (LPD) (contact)
- Low departure from nucleate boiling ratio (DNBR) (contact)
- High pressurizer pressure (fixed setpoint)
- Low pressurizer pressure (manual reset setpoint)
- High SG water level (fixed setpoint)

- Low SG water level (fixed setpoint)
- Low SG pressure (manual reset setpoint)
- Low reactor coolant flow (high decreasing rate, minimum value) (rate limited setpoint)
- High containment pressure (fixed setpoint)

Pre-trip alarms are also transmitted to the QIAS-N and IPS to provide audible and visual indication of an approach to a trip condition.

The PPS also automatically initiates a turbine trip signal to the TCS, which is unidirectional from the PPS to the TCS via a hardwired connection. The turbine trip signal is generated from the PPS when the PPS generates a reactor trip signal.

4.2.1.2 ESFAS Function

The ESFAS actuates system-level ESF functions that transmit signals to ESF components necessary to mitigate the consequences of the design basis accidents. This includes minimizing fuel damage and subsequent release of fission products to the environment.

There is an actuation signal for each ESFAS function. Each actuation function is similar except that specific inputs (and bypasses where provided) and the actuated devices are different.

There are ESFAS initiation signals associated with each of the following six NSSS ESF functions:

- Safety injection actuation signal
- Main steam isolation actuation signal
- Containment spray actuation signal
- Containment isolation actuation signal
- Auxiliary feedwater for SG1 actuation signal
- Auxiliary feedwater for SG2 actuation signal

4.2.1.3 Control Function

A CEA withdrawal prohibit (CWP) signal is generated when a CPC-CWP signal is input from the CPCS or high pressurizer pressure pre-trip condition is present.

The CWP signal is sent to the DRCS where it blocks CEA withdrawal.

4.2.1.4 Alarm Function

The PPS provides status alarm signals to the QIAS-N and IPS for the following types of conditions:

- Bistable trips
- Bistable pre-trips

- Operating bypasses
- Trip channel bypasses
- Operating bypass permissive
- PPS in test
- PPS trouble
- RPS initiation
- ESFAS initiation

4.2.1.5 Test Function

A capability is provided to permit manual periodic testing of the complete PPS and ESF-CCS with the reactor operating at power or when shutdown. These tests cover the trip path from sensor to the RTSS or ESF actuation device. The system test does not interfere with the protective function of the system.

4.2.1.6 Bypass Function

a. Trip Channel Bypass

Trip channel bypasses are provided to remove a trip channel from service for purpose of maintenance or testing. Any number of system parameters may be bypassed, but each parameter can be bypassed on only one channel at any given time by administrative procedure. A trip channel bypass results in the system performing 2-out-of-3 coincidence logic (i.e., ignoring the bypassed parameter).

Trip channel bypass is activated by a hardwired trip channel bypass switch on the MTP switch panel. Trip channel bypass switches on the MTP switch panel in the MTP/ITP cabinet (MTC) are connected to the bistable processor (BP) digital input (DI) module.

The all-bypass function is provided to bypass all parameters in one channel. The all-bypass switch is connected to the local coincidence logic (LCL) DI module.

b. Operating Bypass

Operating bypasses are provided to permit orderly startup and shutdown of the plant and to allow low power testing. The following operating bypasses are provided:

- High logarithmic power level bypass
- High LPD and low DNBR bypass
- Low pressurizer pressure bypass
- CPC-CWP bypass

4.2.1.7 Interlock Function

a. Trip Channel Bypass Interlock

Administrative procedures are used to prevent the operator from bypassing the same parameter in more than one channel. The all-bypass function, bypassing all parameters in the channel, is interlocked in the

LCL algorithm to prevent simultaneous bypass of more than one channel. The all-bypass interlock is implemented using a hardwired cable between the LCLs in all divisions. The purpose of the all-bypass function is to support testing and maintenance of the BP whereas the trip channel bypass is used against sensor failure.

b. Manual Test Interlock

Manual testing requires a permissive from a function enable (FE) keyswitch. The switch is controlled administratively to allow only one division test function to be operated at any one time.

c. CPCS Test Interlock

The low DNBR and high LPD channel trips are interlocked such that they must be bypassed in the PPS in order to test the CPCS. This ensures that only one CPCS channel is tested at a time.

4.2.1.8 Operator Module Function

An OM is provided for each of the four PPS safety divisions. The OMs are located on the MCR SC to provide the operator with such information as trip, pre-trip and bypass status, initiation circuit status, breaker position, and phase current status. The manual switches for operating bypass and setpoint reset control are provided on the MCR SC and RSC.

4.2.1.9 ITP Function

The ITP monitors the PPS division status. It transfers the PPS status to the QIAS-N and supports the testing function.

4.2.1.10 MTP Function

The MTP is the local HSI for maintenance and testing of the PPS. Also the MTP provides the setpoint modification function and resetting of the RTSS and ESFAS initiation signals.

The MTP provides the capabilities to perform surveillance and corrective maintenance, initiate tests, and display detailed system diagnostic messages.

The trip channel bypass, all-bypass, operating bypass, and setpoint reset switches are provided on the MTP switch panel. These switches are directly hardwired to DI modules of the BP or LCL processor.

The MTP also provides gateway function for unidirectional communication from safety I&C system (SDN) to the DCS (DCN-I network).

4.2.2 Design Features

4.2.2.1 General

The PPS comprises four redundant divisions (A, B, C, and D as depicted on Figure 4-4), which perform the necessary bistable logic, coincidence logic, initiation logic and associated maintenance/test functions. The system includes four OMs located in the MCR SC. Four redundant divisions are provided to satisfy SFC and support plant availability.

The BPs in each PPS channel receive the process sensor inputs through the APC-S as shown in Figure 4-5. It also receives hardwired discrete and analog signals from the ENFMS and hardwired discrete signals from the CPCS to perform the bistable trip functions.

An RT or ESFAS coincidence signal is generated whenever two out of the four redundant bistable trip conditions are sensed in the LCL processor for a respective trip function.

The PPS produces discrete output signals from each channel including:

- Pre-trip and trip signals used for RPS initiation, status and alarms
- Pre-trip and trip signals for each ESFAS initiation, status and alarms

Bistable trip inputs from a BP to the LCL processors are bypassed to perform maintenance and/or testing for instrument channel inputs to permit continued operation with a bypassed channel. The trip channel bypass results in a 2-out-of-3 coincidence for the voting logic.

Monitoring, testing and maintenance of the PPS is provided using both the MTP and ITP located in each safety division.

The PPS design includes the following features:

- Based on common PLC platform (see Common Qualified Platform Topical Report
- The common PLC platform provides for standardization of components, to minimize personnel training and spare parts inventory.
- Fiber optic cables and common PLC platform standard data communication are used to the extent practical.
- Software is designed, developed, tested and qualified in accordance with the SPM TeR.
- Non-combustible and heat resistant materials are used wherever practical and temperature alarms are included in the cabinet design.
- The PPS is designed and manufactured to satisfy Quality Class Q requirements and complies with the applicable codes and standards.
- The PPS is qualified to meet Class 1E and seismic Category I requirements. Class 1E is defined by IEEE Std. 603-1991 and seismic Category I is defined by RG 1.29.
- Security provisions within the PPS design include:
  - Equipment located within the PPS cabinets is administratively controlled by door key locks to protect against unauthorized access.
  - Provisions are provided by door switches to remotely indicate (via IPS/QIAS-N) that access has occurred to the PPS cabinets.
  - The PPS common platform operating system, base software and application software are protected against unauthorized alterations by a combination of cyclic redundancy checksums (CRCs) and control of access to software media.

The PPS is designed for fail safe operation under component failure or loss of electrical power.

- A single 120 volts alternating current (Vac) power is provided to redundant direct current (DC) power supplies in each PPS division. A loss of the 120 Vac power feeds to a PPS division causes the safety outputs for the division to fail to the predefined safe state.

- The heartbeat signal of the BP is supervised by the LCL to ensure appropriate trip signals are generated for the reactor trip function.

- Each PPS LCL RT processor is supervised by the built-in watchdog timer (WDT). The contacts outputs of WDT are hardwired in series to the RPS initiation circuit to ensure appropriate trip signals are generated for the reactor trip function as shown in Figure 4-7. If the WDT contained in the LCL RT processor module fails to be reset in the predefined time, the WDT will block the power going through the interposing relay. This will result in opening the interposing relay of the undervoltage trip device in the reactor trip initiation circuit. The detailed information on hardware watchdog timer configuration and relations to fail-safe operation are provided in Reference 12.

The hardware and software for the PPS meet the SFC outlined in IEEE Std. 603-1991 and IEEE Std. 379 as endorsed by RG 1.53 and RG 1.153.

The PPS is designed to detect any error condition of the PPS through the self-diagnostic and supervisory functions such as I/O module diagnostic, processor module diagnostic, application program CRC, communication error CRC, and etc. The detailed information is provided in Reference 12.

The PPS software execution is deterministic to ensure predictable system performance and response under worst-case plant loading condition. The task scheduler schedules the execution of the application programs and periodic system software tasks based on predefined priorities. The detailed information of the deterministic performance and the deterministic performance is provided in Reference 12.

Each PPS division contains a BP and LCL racks. Each BP sends its bistable trip status to each redundant LCL processors in the same division via non-fiber optic SDL and to other redundant divisions' LCL racks via fiber optic SDL. The redundant LCL racks within each division receive the bistable trip signals and perform the 2-out-of-4 local coincidence logic for each RT and ESFAS function. Each LCL rack has digital output (DO) module(s) whose outputs are combined to form the selective 2-out-of-4 coincidence initiation circuit. The configuration is shown in Figure 4-5.

The system, including the processor modules, is subject to continuous hardware monitoring and annunciation of failures to maximize system availability. A watchdog timer within the processor modules monitors the operability of the processor modules (PMs). Refer to Section 5.2.1.3 in Reference 12.

The PPS has redundancy and diversity features. Redundant PPS analog input parameters considering DBEs are assigned to each analog input module for minimizing the effects of a single failure of an analog input (AI) module as shown in Figure 4-5. Each BP processes the bistable logic in the reverse order to that of the other BP to increase the degree of software diversity. The design includes redundant BP racks in each division. The independent configuration of the I/O and communication devices in redundant cabinets is provided.

The selective 2-out-of-4 initiation logic combination of RPS initiation signals is designed to permit testing of the LCL processor without causing RT initiation in a division and still permit valid trip signals to propagate to the RTSS. This design provides hot swap capability for a single PLC module, without causing an output initiation signal. A design goal is to enhance the system's fault tolerance by accommodating a single processor module or SDL data communication link failure in the division without causing a division trip or component actuation (i.e., reactor trip circuit breaker opening or auxiliary feedwater pump/valve operation).

The PPS provides alarms to the QIAS-N and IPS to indicate system abnormalities. The PPS provides status alarms to the QIAS-N via the SDN (to the ITP), and SDL (from the ITP to the QIAS-N). The PPS also provides status alarms to the IPS via the MTP and divisionalized gateways to the DCS network

The PPS cabinets are powered by a single 120 Vac vital bus. The PPS is configured with redundant internal power supplies in each cabinet. The DC output is auctioneered. This makes the PPS safety system fault tolerant for internal power supply single failures. A single internal power supply failure will not result in interruption of system operation.

4.2.2.2 Manual Testing Features

The PPS includes manual testing function. These manual tests provide the means to confirm the operability of the PPS. Manual test features are designed not to interfere with the normal operation of the PPS and can be initiated during plant power operation as well as during plant shut down. To accomplish this, a set of overlapping manual tests, initiated from the MTP FPD, are provided to demonstrate proper operation of the PPS safety functions. The tests are performed over division paths that range from sensor inputs to the RTSS or the input of the ESF-CCS as shown in Figure 4-6.

The tests allow for injection of test signals that replace the actual input or calculated signals and provide monitoring points that can be displayed on the MTP FPD. The test injection points are just before the monitoring point used for a previous test (thus providing overlap). They are used to verify the operability of the processors and SDL communication paths.

These tests are performed under administrative control. Activation of these tests requires the permissive signal by the FE keyswitch.

There are three basic levels of testing:

- Bistable logic test
- LCL logic test
- Initiation test

The bistable logic test monitors the integrity of the trip path from the BP to the input of the LCL including the SDL.

The LCL logic test confirms the integrity of the trip path in the LCL processor.

The initiation test monitors the integrity from the LCL processor to the RPS initiation circuit test. Also, the initiation test confirms the integrity from the LCL processor to the ESF-CCS GC including the SDL.

The ITP together with the MTP provides overall PPS system testing as follows:

- Manual sensor test
- Watchdog timer test
- Interlock test
- AI module accuracy test
- DO module operability test

- RTSS test

The FE keyswitch is normally in the ‘Disable’ position. The FE keyswitch must be in the ‘Enable’ position to inject a test signal. The MTP FPD touch screen controls for the PPS testing are disabled while the FE keyswitch is not in the ‘Enable’ position.

Testing provisions contain a timer that removes the test signals upon time-out. The timer is implemented in the BPs and LCL processors.

4.2.3 Architecture Description

TS

.

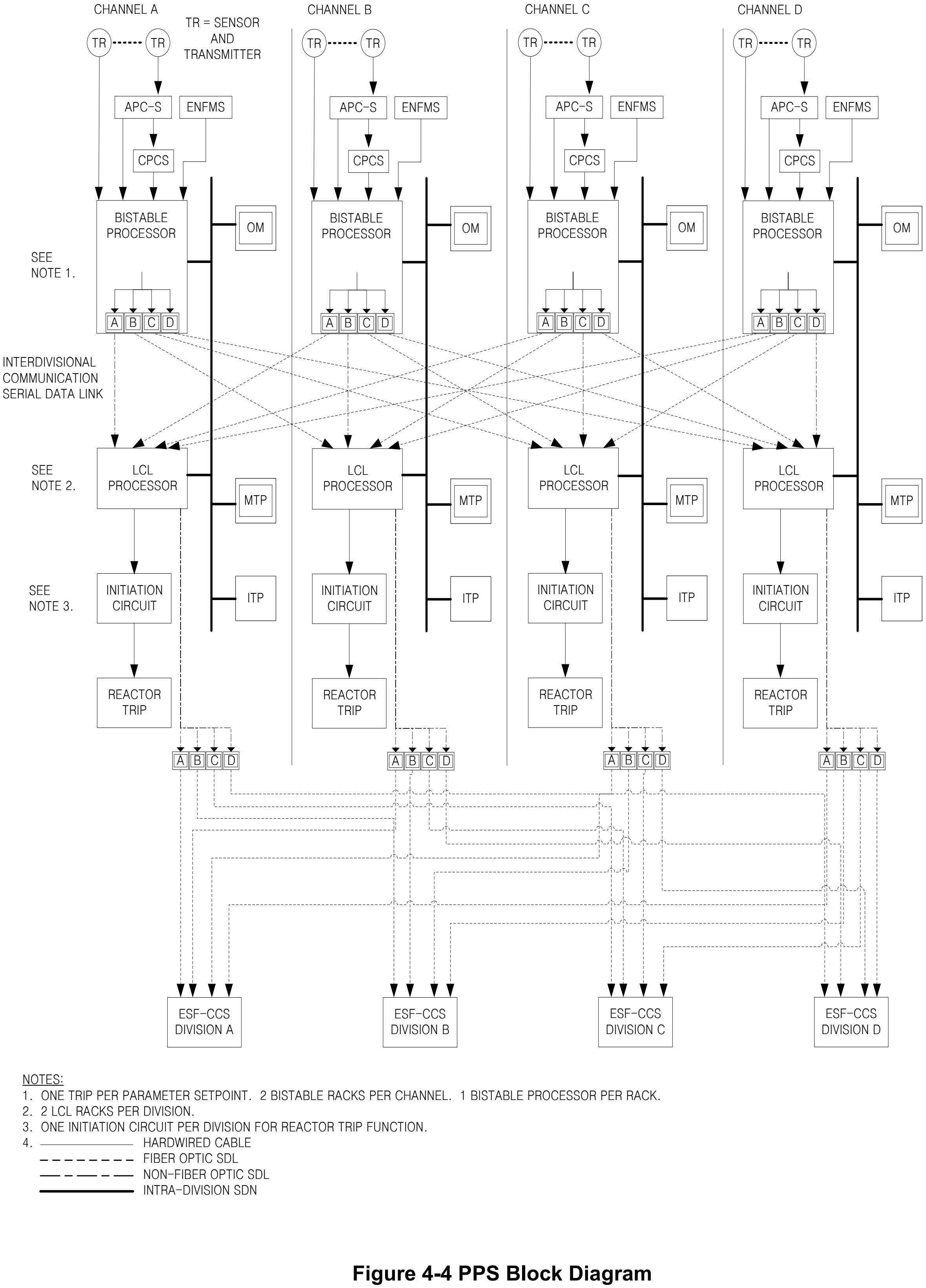
.

TS

.

TS

.



NOTES:
1. ONE TRIP PER PARAMETER SETPOINT. 2 BISTABLE RACKS PER CHANNEL. 1 BISTABLE PROCESSOR PER RACK.
2. 2 LCL RACKS PER DIVISION.
3. ONE INITIATION CIRCUIT PER DIVISION FOR REACTOR TRIP FUNCTION.
4. ───── HARDWIRED CABLE
– – – – – FIBER OPTIC SDL
— – — – NON-FIBER OPTIC SDL
━━━━━ INTRA-DIVISION SDN

Figure 4-4 PPS Block Diagram

TS

Figure 4-5 PPS Division A Trip Path Diagram

TS

Figure 4-6 Overlap in Functional Testing for the PPS

TS

Figure 4-7 Watchdog Timer for PPS

4.2.4 System Interfaces

The PPS cabinet interfaces with the following equipment:

- Auxiliary process cabinet - safety
- Core protection calculator system
- Ex-core neutron flux monitoring system
- Reactor trip switchgear system
- Engineered safety features - component control system
- Information processing system
- Qualified indication and alarm system – P
- Qualified indication and alarm system - non-safety
- Vital bus power supply system
- Control panel multiplexer
- DRCS remote I/O cabinet
- Operator module

The APC-S provides four channels, physically and electrically separate signals for each safety-related plant parameter to the PPS cabinet via hardwired cables. There are no programmable digital devices in the APC-S.

The CPCS provides four channels, physically and electrically separate DNBR and LPD states to the PPS cabinet via hardwired cables.

The PPS receives the log power, calibrated linear power, logarithmic power operating bypass permissive, and ex-core trouble annunciation for the power trip test interlock from the ENFMS safety channel via hardwired cables. These signals are not generated by a programmable digital device.

The RTSS receives a reactor trip signal from the initiation circuit in the PPS via hardwired cables. The RTSS interrupts power to the DRCS to allow gravity insertion of the CEAs upon receipt of a trip signal which is generated by either the RPS section of the PPS or one of the two sets of manual reactor trip switch on the MCR SC.

The PPS sends the ESFAS initiation signals to the ESF-CCS GCs in all ESF-CCS divisions through the fiber optic SDL.

The PPS sends the monitored plant parameters to the QIAS-P via the SDN.

The PPS provides status alarms to the IPS and QIAS-N via the MTP and ITP respectively. The description of the interfaces from the MTP to the IPS and from the ITP to the QIAS-N is provided in Section 4.6.

Each PPS division is powered from a vital bus power supply system (VBPSS) inverter. Each VBPSS division provides a non-interruptible battery backed 120 Vac, single phase, ungrounded power source for essential instrumentation and plant control. The RSR provides the capability to control selected equipment and monitor selected plant variables necessary to achieve an orderly plant safe shutdown when the MCR is uninhabitable.

The conventional switch signals for operating bypass and setpoint reset in the MCR and RSR are sent to the BP from the CPMs that acquire these signals and send them via the SDL.

The DRCS remote I/O cabinet receives a CWP signal via hardwired cables from division D of the PPS. A CWP logic signal is transmitted to the DRCS when a 2-out-of-4 coincidence condition occurs on either a CPC initiated CWP or PPS high pressurizer pressure pre-trip signal. This signal is treated as an associated circuit and isolated at the DRCS remote I/O cabinet.

The OM in each safety division is shared by the PPS, CPCS and ESF-CCS via SDN. The OMs are located on the MCR SC and provide the PPS status (trip/pre-trip/bypass), initiation circuit status, TCB phase current status and operating bypass information to the operator. Each division has its own dedicated OM, and it is physically separated and electrical isolated from other OMs in redundant divisions.

The PPS cabinets are located in divisionalized I&C equipment rooms. Equipment and circuits of the PPS require four division physical separation and electrical isolation meeting the requirements of IEEE Std. 384 as endorsed by RG 1.75.

Communication cablings between redundant PPS divisions are routed via fiber optic cables. The fiber optic cables satisfy the isolation and independence requirements.

The ESFAS initiation outputs from each PPS division to the four divisions of ESF-CCS cabinets are routed and isolated using fiber optic cables.

4.3 Core Protection Calculator System

4.3.1 Functions

The CPCS generates low DNBR and high LPD trip signals. The CPCS monitors pertinent reactor core conditions and calculates DNBR and LPD values from monitored process parameters in each of four redundant core protection calculators (CPCs).

The CPCS provides DNBR and LPD pre-trip and trip signals when either the calculated DNBR or LPD approaches or exceeds its respective setpoint or when certain auxiliary conditions are met. The CPCS channel pre-trip and trip outputs are used by the PPS logic where 2-out-of-4 voting is performed to generate a reactor trip signal.

4.3.1.1 Trip Functions

DNBR Trip

The low DNBR trip is provided to trip the reactor when the calculated DNBR approaches a preset value. The calculation of DNBR is performed by the CPCS based on core average power, reactor coolant pressure, reactor inlet temperature, reactor coolant flow, and the core power distribution. The CPCS calculation includes allowances for sensor and processing time delays and inaccuracies such that a trip is generated by the CPCS before violation of the DNBR safety limit in the limiting coolant channel of the core during incidents of moderate frequency or infrequent incidents.

LPD Trip

The high LPD trip is provided to trip the reactor when the calculated core peak LPD reaches a preset value. The preset value is less than that value which would cause fuel center-line melting. The calculation of LPD is based on the core average power and core power distribution and includes a compensation to account for the thermal capacity of the fuel. The calculated trip assures a core peak LPD below the safety limit for peak linear heat rate.

Auxiliary Trips

The CPCS is also designed to meet additional design bases via auxiliary trip functions.

An auxiliary trip is initiated in response to any one of the following conditions by setting both the DNBR and LPD trip contact outputs.

- Variable overpower trip provides protection for sudden power increases. The trip signal is generated when the calculated reactor power increases greater than the setpoint. The setpoint is a variable that changes based on the calculated reactor power within pre-defined rate limits. If the reactor power increases rapidly and exceeds the rate limited variable setpoint, the trip signal is generated.

- Asymmetric SG transient trip provides protection for instantaneous closure of the main steam isolation valves to a single SG. The temperature difference of two cold leg temperatures is monitored. If the difference is greater than the pre-defined setpoints, the trip signal is generated.

- Range trips on several parameters assure that the core conditions are within the analyzed operating space. If the input values or certain calculated variables exceed the pre-defined ranges, the range trip signal is generated.

- Pump trip precludes operation with fewer than two RCPs running.

- Hot leg saturation trip precludes operation with substantial void in the hot leg fluid. The saturation temperature at measured pressure condition is calculated. If the calculated difference between the current hot leg temperature and saturation temperature is less than the pre-defined value, the trip signal is generated.

- Hardware fault conditions provide trip signals whenever the CPC is in test mode, in initialization, when internal fault conditions occur, or fails to meet the timing requirements.

4.3.1.2 CEA Withdrawal Prohibit

In addition to the trip signal, the CPCS generates a CWP signal for the DRCS when the pre-trip conditions or CEA related conditions (such as reactor power cutback or CEA deviation) are reached. The CWP contact is a separate DO from the CPCS channel to inhibit the withdrawal of CEAs. Each channel of the system generates a CWP input to the PPS so as to produce a CWP signal to DRCS. The system provides CWP input in the form of a contact output to the PPS. The PPS generates a CWP signal upon coincidentally receiving CWP inputs from two of the four CPCS channels.

4.3.1.3 Alarm and indication Function

The CPCS provides major parameters to the QIAS-N for the following signals:

- Axial shape index
- DNBR
- LPD
- DNBR margin
- LPD margin
- RCP speed
- Cold leg temperature
- Hot leg temperature

The CPCS provides status alarms and indication to the IPS for the following signals:

- Low DNBR trip/pre-trip
- High LPD trip/pre-trip
- CEA withdrawal prohibit signal
- Field sensor input signals
- Trip buffer display
- Snapshot display
- DNBR margin

- LPD margin
- CPCS calculated values
- CPCS trouble
- Processor failure
- CPCS in test

4.3.1.4 Operator Module Function

The OM, which is shared with the PPS and ESF-CCS, is provided to monitor certain inputs and calculated results and status for operator. The OM has a dedicated area of display for alarm conditions. In the OM, the specific activities such as monitoring of values or changing addressable constants are performed.

4.3.1.5 Maintenance and Test Panel

The MTP provides the capability to modify the CPCS addressable constants, and displays information such as system parameters, various system status, and test results. The MTP also provides an interface to initiate and support testing. It is located in the MTC and is shared with other safety systems within the division.

The MTP provides the isolated interface to the non-safety DCN-I network via the gateway. This MTP interface is a unidirectional point-to-point Ethernet datalink from the MTP to the DCS gateway server. The uni-directional media converter is used for one-way data transmission across a single fiber optic cable from the MTP to the DCS gateway server in the IPS. Standard duplex fiber connectors are utilized with their full-duplex function disabled. This uni-directional media converter provides the Fast Ethernet RJ-45 ports which are switch-selectable to allow a choice of forced full duplex or auto-negotiated twist-pair connections with other network devices. The transmit (Tx) port of the transceiver converter is connected to the receive (Rx) port of the receiver converter using a single fiber strand; the RJ-45 port of each converter is then connected and configured with its associated host for secure, one-way data transmission. The MTP processor has a full-duplex link to the RJ-45 port in the transceiver converter. The transceiver converter receives data from the MTP processor and forwards one-way data, and provides a fiber optic path with transported and forwarded one-way data to the receiver converter. This receiver converter forwards one-way data to the DCS gateway server.

Manual switches and/or touch panels are used to enable the CPCS control functions such as addressable constant changes, test initiation, etc.

4.3.1.6 Interface and Test Processor

The ITP is located in the same cabinet as the MTP, separate from the CPC and CEA calculator (CEAC) cabinet. Data are shared with other safety systems in the same division using the SDN (e.g. the ITP communicates with the CPCS via the SDN). The ITP also provides the interfaces between the CPCS and QIAS-N by transmitting safety-related data to the QIAS-N via the SDL.

TS

Figure 4-8 CPCS Block Diagram

4.3.2 Design Features

4.3.2.1 General

The CPCS consists of four channels of equipment mounted in the four CPCS cabinets and four OMs mounted on the SC in MCR as shown in Figure 4-8. Each cabinet contains one CPC rack and two redundant CEAC racks. Each channel communicates to the OM via SDN. The OM and MTP provide the operator with an interface to the CPCS system and support plant operational activities.

The CPC rack and two CEAC racks are implemented using the common PLC platform. The OM and MTP utilize the processor unit with FPD. The PLC rack supports SDL communication and SDN communication.

Communication between PLCs (CPCS cabinet), the OM (SC in the MCR) and MTP (MTC) is via the SDN. Communication over a fiber optic cable is used for the SDN connections between the CPCS cabinets and the OM. The SDN connects all of the PLC stations in each CPCS channel together (i.e., CPC Rack, CEAC1 Rack, and CEAC2 Rack, plus the MTP and OM). The SDN is used to transmit the process data, status, and output information to the OM and MTP within the same channel.

The SDL communication is used to transmit the safety data within the safety channel or across safety channels. CEA position processor (CPP) 1 and 2 in each CPCS channel redundantly perform an analog to digital conversion on all CEA position inputs to that channel and transmit these CEA positions to the other three CPC channels over fiber optic isolated SDL cables. Each CPCS channel redundantly receives CEA position from the other CPCS channels.

Each CEAC receives analog CEA position measurement signals which originate from one of two RSPTs associated with each CEA. Each CEA position is measured by two redundant and independent RSPTs associated with each CEA. There are eight CEACs, two in each CPCS channel. Each CPCS channel has a CEAC 1, using RSPT 1 inputs from all CEAs, and a CEAC 2, using RSPT 2 inputs from all CEAs. RSPT inputs to each CPCS channel are converted to digital format in the channel AI module A/D converter, and transmitted to the other three CPCS channels via fiber optic isolated SDL cables.

The CEAC PM calculates the magnitude of CEA deviation penalty factors (PFs) based upon CEA position sensor input data obtained from each RSPT. Each CEAC PM transmits PFs to the CPC PM within the CPCS channel via SDL.

4.3.2.2 Design Implementation

The CPCS is a digital computer based design (i.e., common PLC platform) to take advantage of high accuracy and drift free operation.

- Utilizes the same common PLC platform as the PPS.
- The application software is designed, developed, tested and qualified in accordance with the SPM TeR.
- Designed to minimize, consistent with other safety requirements, the probability and effect of fires and explosions. Non-combustible and heat resistant materials are used wherever practical throughout the CPCS equipment.

Security provisions within the CPCS design include:

- Equipment located within CPCS cabinets are administratively controlled by door key locks to protect against unauthorized access.

- The CPCS software is protected against unauthorized alterations (this includes setpoints and code) by control of access to software media and CRC authentication.

4.3.2.3 Program Structure

TS

TS

Figure 4-9 Dynamic Adjustments to the Parameters

TS

TS

TS

Figure 4-10 CPCS Function Block Diagram

4.3.2.4 Channel Independence

TS

.

4.3.3 Architecture Description

TS

TS

.

TS

.

4.3.4 System Interfaces

The CPCS interface with other systems is shown in Figure 4-12. The CPCS cabinet housing the CPC rack and CEACs rack interfaces with the following equipment:

- Auxiliary protective cabinet - safety
- Ex-core neutron flux monitoring system
- Reactor coolant pump shaft speed sensing system
- Reed switch position transmitter
- Plant protection system
- Information processing system
- Qualified indication and alarm system - P
- Qualified indication and alarm system - non-safety
- Vital bus power supply system
- Field sensors

4.3.4.1 Auxiliary Process Cabinet-Safety

The CPC processor receives the pressurizer pressure signals via hardwired cable from the APC-S . The pressurizer pressure signals are used in the DNBR and the LPD calculations

4.3.4.2 Ex-core Neutron Flux Monitoring System

The CPC processor receives the linear sub-channel power signals from the ENFMS. via hardwired cable These are used for the reactor power calculation and power distribution calculation.

4.3.4.3 Reactor Coolant Pump Shaft Speed Sensing System

The CPC processor receives RCP speed signal from reactor coolant pump shaft speed sensing system (RCPSSSS). The RCP speed signal is used in the flow rate calculation.

4.3.4.4 Reed Switch Position Transmitter

The CEA position is provided by two RSPT inputs on each CEA. All RSPT inputs are converted to a digital value in the CPP PM and are input to all four CPC/CEAC channels over fiber optic isolated SDL data links. The CPPs in channel A(D) receive 23 CEA positions from RSPT1(2), and the CPPs in channel B(C) receive 70 CEA positions from RSPT1(2). The RSPTs are hardwired to the CPPs.

4.3.4.5 Plant Protection System

The CPCS system provides the following hardwired signals to the PPS.

- Low DNBR trip/pre-trip
- High LPD trip/pre-trip
- CEA withdrawal prohibit

4.3.4.6 Information Processing System

The CPC and auxiliary CPC processor transmit CPC data to the IPS via the MTP. The description of the interface from the MTP to the IPS is provided in Section 4.6. The CEAC also transmits CEAC data to the IPS via the MTP.

4.3.4.7 Qualified Indication and Alarm System-P

The CPCS transmits CEA position data to the QIAS-P via the SDN.

4.3.4.8 Qualified Indication and Alarm System-Non safety

The CPCS transmits pre-selected data to the QIAS-N via the ITP. The description of the interface from the ITP to the QIAS-N is provided in Section 4.6.

4.3.4.9 Field Sensors

The CPCS receives the following hardwired field sensor signals.

- Hot leg temperature loop 1
- Hot leg temperature loop 2
- Cold leg temperature loop 1
- Cold leg temperature loop 2

TS

Figure 4-11 CEA Position and PF Movement

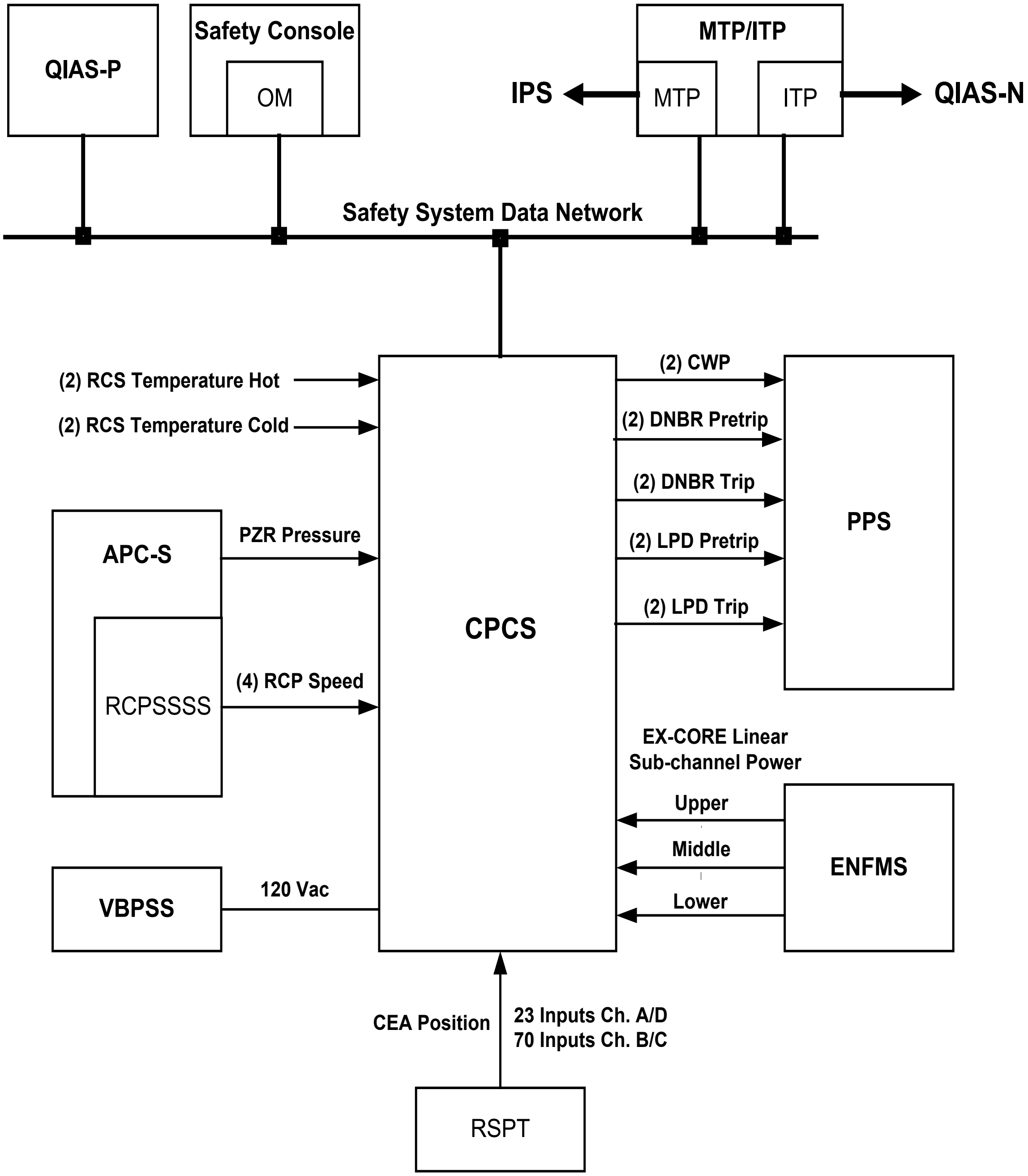


Figure 4-12 CPCS Interface Block Diagram

TS

Figure 4-13 Watchdog Timer for CPCS

4.4 Engineered Safety Features - Component Control System

4.4.1 Functions

The ESF-CCS generates the component control signals which are required to actuate the ESF functions and associated components as shown in Figure 4-14.

The ESF-CCS GC receives ESFAS initiation signals from the ESFAS portion of the PPS, safety-related divisionalized cabinet (SRDC) in the RMS, or manual ESF system-level actuation switch. The GC processor performs selective 2-out-of-4 coincidence logic and 1-out-of-2 logic for ESF component actuation. The ESF-CCS LC receives ESF actuation signals from the GC and the component-level minimum inventory (MI) switches to control safety components. The ESF-CCS performs prioritization of these signals. The output of the ESF-CCS is hardwired to the CIM which performs prioritization of system signals associated with a particular ESF component.

The ESF-CCS also receives an initiation signal for emergency diesel generator (EDG) load sequencer from the electrical panel. The signal is generated by undervoltage relays (one division per 4.16 kV power bus) consisting of 2-out-of-4 logic under loss of offsite power.

The output of the CIM is hardwired to the electrical equipment that supplies electrical power to the ESF components. The electrical equipment interfaces directly with the ESF components.

The ESF-CCS provides the control of other safety-related components as well as the actuation of ESF components. Such components include breaker and relay operated components (e.g., pumps, fans, heaters, and motor operated valves), and solenoid operated components (e.g., pneumatic, electro-pneumatic, and direct operated valves).

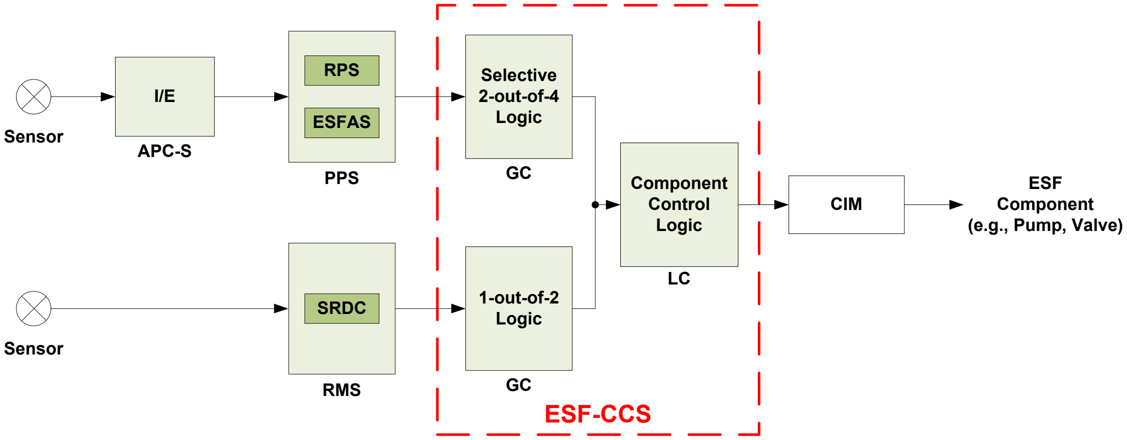


Figure 4-14 ESF-CCS Functional Block Diagram

4.4.2 Design Features

The ESF-CCS consists of four independent divisions (A, B, C, and D) which are physically separate and electrically independent. The ESF-CCS configuration is based on the common PLC platform. NSSS ESF initiation signals are received from the PPS via SDL for same division and via interdivisional communication SDL for other divisions. BOP ESFAS initiation signals are received from the SRDC in the RMS. These signals are transmitted as discrete contact signals to DI module in GC (divisions A and B only) via hardwired cables, and the SRDC provides the isolator to maintain electrical isolation between signals and the ESF-CCS.

NSSS ESFAS

Each ESF-CCS division receives ESFAS initiation signals from all four divisions of the PPS and performs an automatic actuation of the applicable ESF system(s) when certain coincidence logic conditions are satisfied. The ESF-CCS also provides provisions for manual ESF system-level actuation and manual component control of ESF components. The selective 2-out-of-4 coincidence logic for voting is performed in the ESF-CCS GC1 and GC2 process modules (PLC racks) which independently receive ESFAS initiation signals from the four PPS divisions (A, B, C, and D) and perform a selective 2-out-of-4 coincidence logic on the initiating signals. Valid ESF system-level actuation signals are latched and require manual reset before returning to the non-actuation status Two redundant GCs (GC1 and GC2) are provided for reliability within each ESF-CCS division (Refer to Figure 4-14). There are ESFAS initiation signals associated with each of the following six NSSS ESF functions:

- Safety injection actuation signal (SIAS)
- Main steam isolation signal (MSIS)
- Containment spray actuation signal (CSAS)
- Containment isolation actuation signal (CIAS)
- Auxiliary feedwater actuation signal for SG1 (AFAS-1) : valve portion of logics does not latch
- Auxiliary feedwater actuation signal for SG2 (AFAS-2) : valve portion of logics does not latch

Based on the outputs of the coincidence logic, the GC1 and GC2 provide actuation signals to the LCs in the same division via fiber optic SDLs. Each LC receives the ESF actuation signals from the both GC1 and GC2 and activates the appropriate ESF actuation signal for the ESF components.

BOP ESFAS

A redundant set of safety instrumentation and controls are provided for proper actuation of the BOP ESFAS equipment to mitigate the consequences of the fuel handling accidents in the reactor containment building and the fuel handling area as well as to provide a habitability condition for the plant operating personnel in the MCR during or after all phases of the DBE.

The GC receives ESFAS initiation signals from two safety radiation monitoring sensors located in the reactor containment building and control room air intake, and one safety radiation monitoring sensor located in fuel handling area for each division A and B. The BOP ESFAS is designed based on 1-out-of-2 logic taken twice except the FHEVAS initiation signal that performs 1-out-of-2 logic taken once. The following BOP ESF actuation signals are generated by the ESF-CCS when the monitored variables reach the levels that are indicative of a condition which require protective actions:

- Fuel handling area emergency ventilation actuation signal (FHEVAS),
- Containment purge isolation actuation signal (CPIAS)
- Control room emergency ventilation actuation signal (CREVAS)

COMPONENT CONTROL

TS

.

TS

TS

.

Table 4-4 List of components associated with ESF-1 and ESF-2 safety command signals TS

					(1 of 16)

Table 4-4 List of components associated with ESF-1 and ESF-2 safety command signals

TS

					(2 of 16)

Table 4-4 List of components associated with ESF-1 and ESF-2 safety command signals TS

(3 of 16)

Table 4-4 List of components associated with ESF-1 and ESF-2 safety command signals TS

(4 of 16)

Table 4-4 List of components associated with ESF-1 and ESF-2 safety command signals

TS

(5 of 16)					

Table 4-4 List of components associated with ESF-1 and ESF-2 safety command signals TS

(6 of 16)

Table 4-4 List of components associated with ESF-1 and ESF-2 safety command signals TS

(7 of 16)					

Table 4-4 List of components associated with ESF-1 and ESF-2 safety command signals

TS

					(8 of 16)

Table 4-4 List of components associated with ESF-1 and ESF-2 safety command signals TS

(9 of 16)

Table 4-4 List of components associated with ESF-1 and ESF-2 safety command signals TS

					(10 of 16)

Table 4-4 List of components associated with ESF-1 and ESF-2 safety command signals TS

					(11 of 16)

Table 4-4 List of components associated with ESF-1 and ESF-2 safety command signals

TS

(12 of 16)					

Table 4-4 List of components associated with ESF-1 and ESF-2 safety command signals TS

(13 of 16)

Table 4-4 List of components associated with ESF-1 and ESF-2 safety command signals TS

(14 of 16)

Table 4-4 List of components associated with ESF-1 and ESF-2 safety command signals TS

(15 of 16)

Table 4-4 List of components associated with ESF-1 and ESF-2 safety command signals TS

(16 of 16)					

TS

4.4.3 Architecture Description

TS

TS

TS

TS

Figure 4-15 ESF-CCS Functional Configuration

TS

Figure 4-16 ESF-CCS Block Diagram

TS

Figure 4-17 Simplified Component Control Logic

TS

Figure 4-18 Watchdog Timer for ESF-CCS

4.4.4 System Interfaces

TS

.

TS

TS

Table 4-5 Summary of Interdivisional ESF-CCS Signals

TS

Table 4-5 Summary of Interdivisional ESF-CCS Signals

TS

Table 4-5 Summary of Interdivisional ESF-CCS Signals

TS

Table 4-5 Summary of Interdivisional ESF-CCS Signals

TS

Table 4-5 Summary of Interdivisional ESF-CCS Signals

TS

Table 4-5 Summary of Interdivisional ESF-CCS Signals

TS

Table 4-5 Summary of Interdivisional ESF-CCS Signals

TS

Table 4-5 Summary of Interdivisional ESF-CCS Signals

4.5 Qualified Indication and Alarm System – P

4.5.1 Functions

The QIAS-P provides a continuous display of RG1.97, Rev. 4 AMI variables (Types A, B and C) and an unambiguous indication of the approach to and the recovery from ICC as a backup to the safety parameter display system (SPDS). The recording function for Type A, B and C variables is performed in the IPS.

The QIAS-P calculates representative core exit temperature, primary coolant subcooling margins, and reactor vessel water level.

The QIAS-P provides output signals to the QIAS-P display via the SDN, to the MTP for the IPS (via unidirectional Ethernet datalink), and to the ITP for the QIAS-N (via the SDL). In all cases, these output signals are for display of sensor signals, ICC variables, and AMI variables.

The QIAS-P provides a backup for the SPDS for ICC variables. The SPDS is implemented in the SPADES+ application in the IPS.

Upon receipt of the analog and digital signals, the QIAS-P performs signal checking. The QIAS-P displays are a major part of the overall MCR information system used for accident monitoring. The QIAS-P configuration is presented in Figure 4-19.

4.5.2 Design Features

The QIAS-P has two divisionalized cabinets. The QIAS-P cabinet for each division is located in the divisionalized I&C equipment room. The QIAS-P receives AMI variables from the PPS and ESF-CCS via the SDN; and APC-S and process instrumentation via hard-wired connection. The QIAS-P also displays the status of CIVs from both QIAS-P divisions. The status of the other QIAS-P division CIVs are obtained from the ITP through the interdivisional SDL.

4.5.2.1 Calculation

The QIAS-P processes the AMI variables (Types A, B and C) as determined from RG 1.97, Rev.4, for accident monitoring guidelines.

The QIAS-P calculates representative core exit temperature from the core exit thermocouples (CETs). The QIAS-P calculates primary coolant subcooling margins based on CET temperatures, hot and cold leg temperatures, heated junction thermocouple (HJTC) temperatures from the reactor vessel head region, and pressurizer pressure. The QIAS-P calculates reactor vessel level from the top of the core to the top of the reactor vessel (based on the signals from the HJTCs). The HJTCs are discrete level measurements throughout the height of the reactor vessel. Liquid uncovery of an HJTC is determined by the temperature difference between the heated and unheated thermocouple pair at a specific height location in the reactor vessel.

TS

Figure 4-19 QIAS-P Block Diagram

4.5.2.2 Displays

The QIAS-P has two FPDs on the SC. The QIAS-P division A(B) displays division A(B) variables except CIVs status.

The QIAS-P division A and B FPDs also display the CIVs status for all divisions to monitor the proper operation of CIVs to confirm the isolation of containment penetration to enhance plant safety. The compliance to DI&C-ISG-04 of the interdivisional SDL is addressed in Appendix C of this report.

The FPD displays provide backup displays for the ICC variables per NUREG-0737. The primary displays of ICC variables are implemented in the SPADES+ of the IPS.

Each FPD allows the operator to select the pages that display either:

- AMI variables or
- ICC variables

The QIAS-P displays output an unambiguous indication in accordance with Style Guide (Reference 16). The following ICC variables are calculated and validated using an algorithm executed by the QIAS-P PLC processor, and are displayed on the QIAS-P displays in the MCR.

- Primary coolant saturation margin (temperatures calculated from RTDs, HJTCs, CETs and PZR pressure)
- Coolant temperature at the core exit (calculated from CETs)
- Coolant level in the reactor vessel above the top of the core (calculated from HJTCs)

4.5.2.3 MTP Functions

The QIAS-P allows signal substitution for failed HJTC values, signal bypass for abnormal values by operator decision. The QIAS-P allows setpoint changes for ICC calculation parameters by the operator through the MTP to prevent software modifications for simple changes to the system. These functions are manually initiated from the MTP under administrative control.

4.5.2.4 Power Supply

Power distribution is assigned such that the loss of a single vital instrument power bus does not result in the loss of more than one QIAS-P division. Loss of electrical power to a QIAS-P FPD display results in a blank screen. The loss of electrical power to one QIAS-P controller processor results in an indication of an inactive state on the QIAS-P displays.

4.5.2.5 Alarms

The QIAS-P generates alarms (visual only) for ICC parameters and send them to the QIAS-N and IPS.:

- Low reactor vessel level-head
- Low reactor vessel level-plenum
- Low upper head temperature subcooling margin (IPS only)

- Low upper head pressure subcooling margin (IPS only)
- Low RCS temperature subcooling margin (IPS only)
- Low RCS pressure subcooling margin (IPS only)
- Low CET temperature subcooling margin
- Low CET pressure subcooling margin (IPS only)
- Low RCS /RV upper head temperature subcooling margin
- Low RCS /RV upper head pressure subcooling margin (IPS only)
- High representative CET temperature

4.5.2.6 Redundancy

The QIAS-P consists of the redundant safety divisions A and B for signal processing and displays. Redundancy is provided for both the instrument divisions supplying the signal and the displays in the MCR. Instrument channels are electrically independent and physically separated from non-safety equipment by qualified isolation devices. The QIAS-P cabinets are located in separated I&C equipment rooms. Credited redundancy for the display of RG 1.97, Rev. 4, Type A, B and C variables is provided by the QIAS-P divisions. Type A, B and C variables are also displayed on the QIAS-N and IPS.

To prevent ambiguity of the information presented to the operator, additional sensors or diverse variables are used to ensure that the information presented to the operator is correct as described in Table 7.5-1 of the DCD.

The QIAS-P monitors two redundant AMI instrument channels (A and B) for each RG1.97, Rev. 4 Type A, B and C process parameters. For CIVs, the QIAS-P displays all divisions on each QIAS-P display.

4.5.3 System Interfaces

The QIAS-P cabinet interfaces with the following systems and equipment:

- Process instrumentation
- Auxiliary process cabinet - safety
- HJTC (HJTC temperatures)
- In-core instrumentation system (CET temperatures)
- DIS
- ESF-CCS
- PPS
- MTP (then to IPS),
- ITP (then to QIAS-N),

- QIAS-P display

The signal interfaces between the QIAS-P cabinet and process instrumentation, in-core instrumentation system (ICIS), HJTC, and the APC-S are done by hardwired cables.

The signal interface between the QIAS-P cabinet and the DIS, which is a non-safety system, is done by hardwired cables and isolators.

The communications between the QIAS-P cabinet and the safety systems such as the PPS, CPCS, MTP, ITP, the QIAS-P display, and the ESF-CCS are done via SDN.

The communications between the QIAS-P cabinet and the IPS and QIAS-N, which are non-safety systems, are done through the MTP and the ITP, respectively.

Table 4-6 provides a summary of the I/O signals for the QIAS-P.

TS

Table 4-6 Summary of QIAS-P I/O Signals

4.6 Data Communication System

The data communication system uses the SDN, the SDL and the MTP unidirectional point-to-point Ethernet datalink. It provides high speed and error free communication paths between each PLC and FPD within a division, and between control/protection systems and information systems. In addition, Ethernet datalink is applied to send identification data of component selection from the IFPD to the ESCM. The data communication system ensures that any errors in data communication do not cause inadvertent actuations or prevent the safety functions from being performed.

4.6.1 Design Features

4.6.1.1 Safety and Quality Classification of Components and Modules

The fiber optic modems and communication modules used in the data communication system of the safety I&C system are classified as Class 1E, Quality Class Q and seismic Category I.

4.6.1.2 Data Communication System Software Categorization

The application of the data communication system is classified as follows (Refer to the SPM TeR):

- Interdivisional communication SDLs (PPS BP to LCL) – protection
- Interdivisional communication SDLs (PPS LCL to ESF-CCS GC) – protection
- ESF-CCS GC to LC SDLs – protection
- CPM to PPS SDLs - protection
- CPM to ESF-CCS SDLs - protection
- Safety system data network (SDN) – important-to-safety
- ITP datalink SDLs – important-to-safety
- ITP to QIAS-N SDLs – important-to-safety
- MTP to IPS Ethernet network – important-to-safety
- IFPD to ESCM datalink – important-to-availability (seismically qualified)

4.6.1.3 Performance (Real time & Deterministic timing)

The data communication system is deterministic (repeatable and predictable). Deterministic means that the data is predictably transmitted. Because it is predictably transmitted it has the characteristic of repeatability. The SDL communication is described in Section 5.6 of Reference 12. The deterministic behavior of the SDL communication is dependent on the repeatable and predictable execution of an application. The execution of an application program is repeated at predetermined intervals and is described in Section 5.3.1 of Reference 12.

The SDL time delay is considered in establishing the instrument response time.

There is no difference in data transfer rate, data bandwidth, data accuracy and error performance during normal and abnormal operations (i.e., whether the nuclear power plant is in a steady state or undergoing a transient or accident condition).

The SDN has a deterministic network protocol that is used for non-node communication within a division. The controllers of PPS and ESF-CCS and FPDs will be nodes on the SDN.

There are two modes of data transmission of the SDN:

- Process data transfer - deterministic
- Message transfer - non-deterministic

Process data transfer is the mode of communications between the nodes in the same division. It is also the mode in which the FPDs receive data from the SDN network.

Message transfer is not used in the safety systems. TS

Details for deterministic communication are described in Reference 12.

4.6.1.4 Reliability

Error checking techniques for data integrity such as CRC are incorporated into the communication protocol to assure the integrity of the transmitted data.

Upon detection of the communication loss within a safety system, the system is designed such that communication failures shall not prevent safety systems from performing their intended safety function as analyzed in Appendix C.

Refer to Appendix C and Section 5.6 of Reference 12 for a detailed description on the SDL compliance to the criteria in DI&C-ISG-04 Section 1.

4.6.1.5 Control of Access

Security provisions are provided for the data communication system associated with the system to which it is connected such as key locked door and protection against unauthorized software alteration.

4.6.1.6 Single Failure Criterion

The configuration of the data communication system is designed so that the requirements of the SFC are satisfied. The FMEA shows that no single failure will defeat more than one of the four redundant safety I&C system divisions as applicable.

The FMEA for the safety I&C system in the DCD Chapter 7 describes and provides a detailed evaluation; including network cable and equipment failures, failure to transmit and receive data or transmission of erroneous data. The data communication system is designed with redundancy and multiple data paths, if necessary.

4.6.1.7 Independence

The data communication system is designed to maintain the independence between the safety divisions (A, B, C, D), and the independence between the safety and non-safety systems.

Communication between safety I&C systems is performed via SDL fiber optic cables only.

The communication independence is designed to satisfy DI&C-ISG-04 (see Appendix C of this report and Section 5.6 of Reference 12).

4.6.1.8 Failure Modes (including Fail-Safe Design Strategy)

The safety I&C system application uses the data communication system to fail into a safe state or into a state established as acceptable in the event of loss of power supply. These communication systems are also used by the application so that any single failure does not prevent proper protective action at the system-level. The FMEA shows that no single failure results in the failure of more than one of the four redundant divisions of safety I&C system or prevents proper protective action at the system-level. The FMEA includes a data communication interface failure to transmit, failure to receive or transmit of erroneous data. The FMEA considers the credible failures of all components including communication modules and communication links/networks. The FMEA also addresses the consequences of a postulated “broadcast storm” occurring in the communication system.

With regard to power supply requirements, the PPS function is designed such that the failure of the data communication system power supply required for performing the PPS function will result in a reactor trip for that redundant protective division (fail-safe design). The ESFAS functions are designed to ensure that failure of a data communication system power supply required to perform ESFAS functions will result in a fail-as-is of the related actuation division.

4.6.1.9 System Testing and Inoperable Surveillance

There are two testing modes: one is to monitor the operation of data communication by diagnostic functions, the other is to do integrated testing to transmit the data between the each system.

The SDN uses bus master to continuously monitor the status of nodes on the bus. The communication interface (CI) module monitors the validity of the data sets it is designated to receive. If no data is received for the predetermined cycles for the data sets, or when the communication interface has failed, the database element for data set will be flagged as failed. The CI module programming will constantly monitor the database element flag and perform the appropriate error processing.

For the SDL, the PM executes continuously monitors the SDL supervision, memory checking, report and fault detected. The SDL diagnostics are executed to detected physical layer failures and failures of the communication link to another PM.

For integrated testing, the MTP provides test function to confirm the communication of the signals between each controllers, one division at a time to prevent inadvertent safety system trips. Testing follows a logical and predetermined progression on the MTP display, which guides the operator through the test sequence.

4.6.1.10 EMI/RFI Susceptibility

The data communication system is EMI/RFI qualified as part of each related system.

The data communication media do not provide a fault propagation path due to environmental effects, such as high-energy electrical faults or lightning, from one redundant portion of a system to another or from a non-safety system to a safety system because of the use of fiber optic cabling.

4.6.1.11 Diversity and Defense-in-Depth

The D3 TeR address the capability of the overall plant design to cope with a DBE concurrent with a postulated software CCF in the safety I&C system including the associated data communication system.

4.6.1.12 Data Communication System exposed to Seismic Hazard

The data communication system for safety I&C system is designed and qualified to meet seismic Category I requirements.

4.6.2 System Description

Figure 4-20 illustrates the safety I&C data communication system which consists of the SDN, interdivisional SDLs, PPS to ESF-CCS SDL, CPM to PPS/ESF-CCS SDL, MTP to IPS interface (unidirectional point-to-point Ethernet datalink), ITP to QIAS-N SDL interface, and IFPD to ESCM interface (unidirectional point-to-point Ethernet datalink).

TS

Figure 4-20 Safety I&C Data Communication System

4.6.2.1 Interdivisional Serial Data Links

There are two sets of interdivisional SDLs per redundant PPS division. These SDLs originate from the BPs and LCLs.

Each BP, LCL, GC, and LC is composed of a function processor (FP, processing section) and communication processor (CP, communication section (CS)). The FP executes the safety application programs. The CP provides the interface for the SDL. Each CS in the PM supports SDL communication. Each BP broadcasts data to the LCL processors connected to its SDL. The SDLs connected to redundant PPS division LCLs use fiber optic modems and cable to provide independence and isolation. The interdivisional SDLs are also used to transmit ESFAS initiation signals from the LCLs to the ESF-CCS GCs in the same division and to the three redundant ESF-CCS divisions using fiber optic modems.

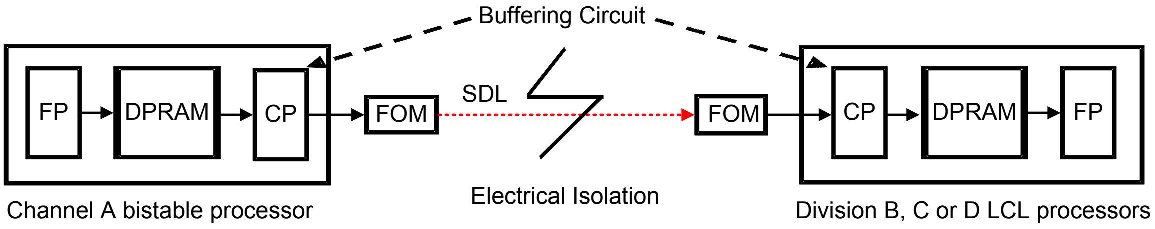
The fiber optic communication used for the interdivisional SDL between the redundant PPS divisions is RS-422 serial data transmission link. The interdivisional SDL’s purpose is to provide the bistable trip information to the LCLs and send ESFAS initiation signals from LCLs to the ESF-CCS GCs in all divisions.

Failure of a BP is compensated for the redundant BP in the same division. Failure of both BPs in a division causes the LCL to set that division’s input signals to a trip state for the RPS function and to a no trip state for ESFAS function.

Failure of a LCL is compensated for the redundant LCL in the PPS division.

To ensure communication independence, each of the BP and LCL includes two separate processors (FP and CP) as shown in Figure 4-21. Data flow between redundant PPS divisions is buffered at both ends ensuring independence of the redundant divisions. One way communication using fiber optic cable is applied for communication isolation and the fiber optic cables are used for electrical isolation.

This communication method is also applied to the data links between the PPS and ESF-CCS.



CP:	communication processor
DPRAM:	dual-ported random access memory
FOM:	fiber optic modem
FP:	function processor
LCL:	local coincidence logic
SDL:	serial datalink

Figure 4-21 Data Communication between Redundant Divisions in PPS

4.6.2.2 Intradivision Communication Safety System Data Network

The intra-division SDN connects the PLC stations and FPDs in each safety division together (i.e., BP, LCL, ESF-CCS GC and LC, CPCS, MTP, ITP, OM, QIAS-P, ESCM, CPM and CCG, etc.) as shown in Figure 4-20. Each PLC station includes a CI module to connect to the SDN within a division. The MTP, OM and ESCM have a CI module to connect to the SDN within a division.

The SDN provides the sharing of status and testing information among the PLCs and FPDs. The MTP and OM are connected to the SDN for the purpose of status monitoring, setpoint changes, and testing. Failure of this network does not prevent the continued operation of the safety system from performing its intended safety function because the SDN is functionally separated from the SDL communications for protection. The SDN is contained within a division and does not cross safety division boundaries.

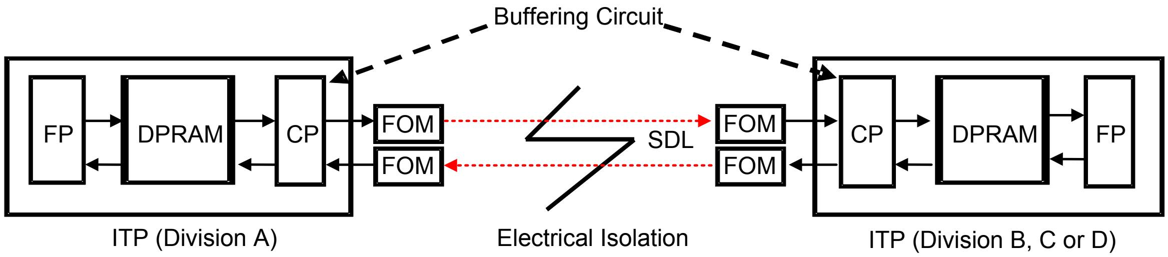
The SDN provides data communication among the following systems and components within same division:

- PPS bistable processors
- PPS LCL processors
- ESF-CCS group controllers
- ESF-CCS loop controllers
- CPCS processors
- QIAS-P processors
- Operator module
- Maintenance and test panel
- Interface and test processor
- Control panel multiplexers
- ESCM
- CCG

4.6.2.3 ITP Data Link

The ITP communicates with the ITPs in the other safety divisions via dedicated SDLs. The SDLs between the ITPs are functionally isolated from the SDN in each division.

Each ITP has an inbound SDL and an outbound SDL as shown in Figure 4-22.



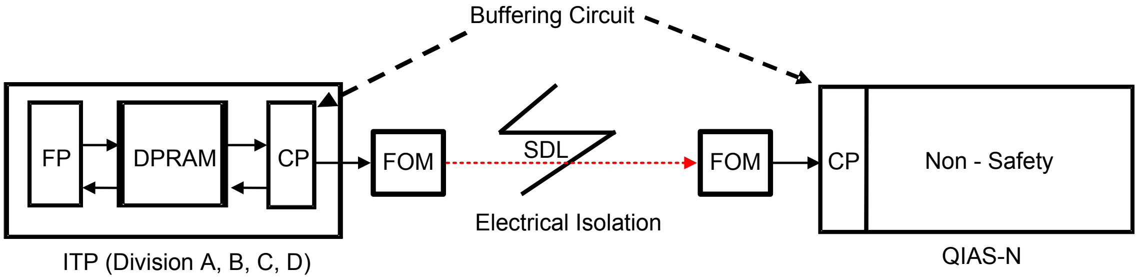
CP:	communication processor
DPRAM:	dual-ported random access memory
FOM:	fiber optic modem
FP:	function processor
ITP:	interface and test processor
SDL:	serial datalink

Figure 4-22 Interface & Test Processor Data Link

4.6.2.4 ITP to QIAS-N Network

The ITP to QIAS-N SDL provides communications between the ITPs and QIAS-N. The information for monitoring and/or testing of the safety system and the necessary data are provided to the QIAS-N via the ITP, which performs a gateway function. The data flow from the ITP to the QIAS-N is unidirectional via fiber optic cable. The QIAS-N is programmed only to receive data and the transmission of any raw data is not allowed via the ITP. A complete failure of this data link will not prevent the safety systems from performing their intended safety functions.

The data flow from safety system to non-safety system is unidirectional as shown in Figure 4-23.



CP:	communication processor
DPRAM:	dual-ported random access memory
FOM:	fiber optic modem
FP:	function processor
ITP:	interface and test processor
QIAS-N:	qualified indication and alarm system – non-safety
SDL:	serial datalink

Figure 4-23 Data Communication from ITP to QIAS-N

4.6.2.5 MTP to IPS Network

The MTP to IPS network is used to provide data transmission to the IPS as shown in Figure 4-24. The data flow from the MTP to the IPS is unidirectional via a simplex fiber optic cable.

The communication between the MTP and IPS does not require any acknowledgment. A failure of this network does not prevent the RPS and ESFAS functions.

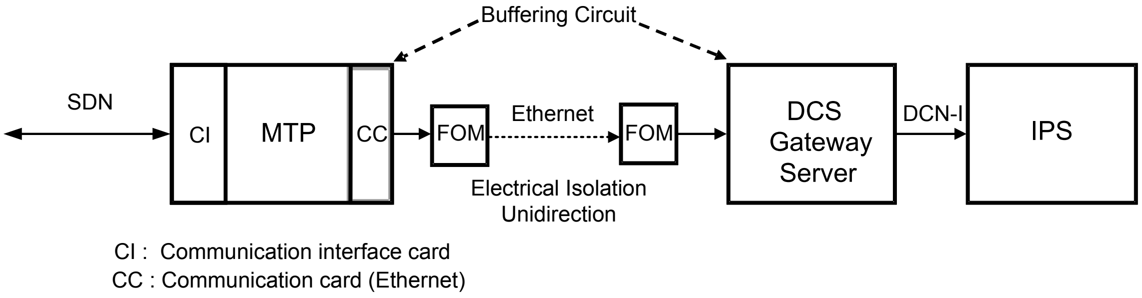


Figure 4-24 Data Communication from MTP to IPS

4.6.2.6 Communication of ESCM

TS

.

4.7 Safety HSI System

4.7.1 Safety Control HSI

TS

TS

TS

TS

TS

Figure 4-25 System Directory – Primary Systems

TS

Figure 4-26 System Directory – Secondary Systems

TS

Figure 4-27 System Mimic Page

TS

Figure 4-28 ESCM Soft Control Template - Discrete Type (Example)

TS

Figure 4-29 ESCM Soft Control Template – Modulation Type (Example)

4.7.1.1 Task Timing Analysis for IFPD to ESCM Interface

TS

4.7.2 Qualified Indication and Alarm HSI

TS

.

4.7.3 Diverse HSI

TS

.

4.7.4 Remote Shutdown Console HSI

TS

TS

.

4.7.5 Control Panel Multiplexers

TS

TS

TS

Figure 4-30 ESF Control Block Diagram

4.7.6 Main Control Room/Remote Shutdown Room Master Transfer Switch

TS

TS

.

TS

Figure 4-31 Transfer of ESCM control function signals from MCR to RSR

TS

Figure 4-32 Transfer of control functions for MI switch signals from MCR to RSR

TS

.

Figure 4-33 Master transfer switch configuration for P-CCS and PCS

4.8 Reactor Trip Switchgear System

4.8.1 Functions

TS

.

4.8.2 Design Features

TS

.

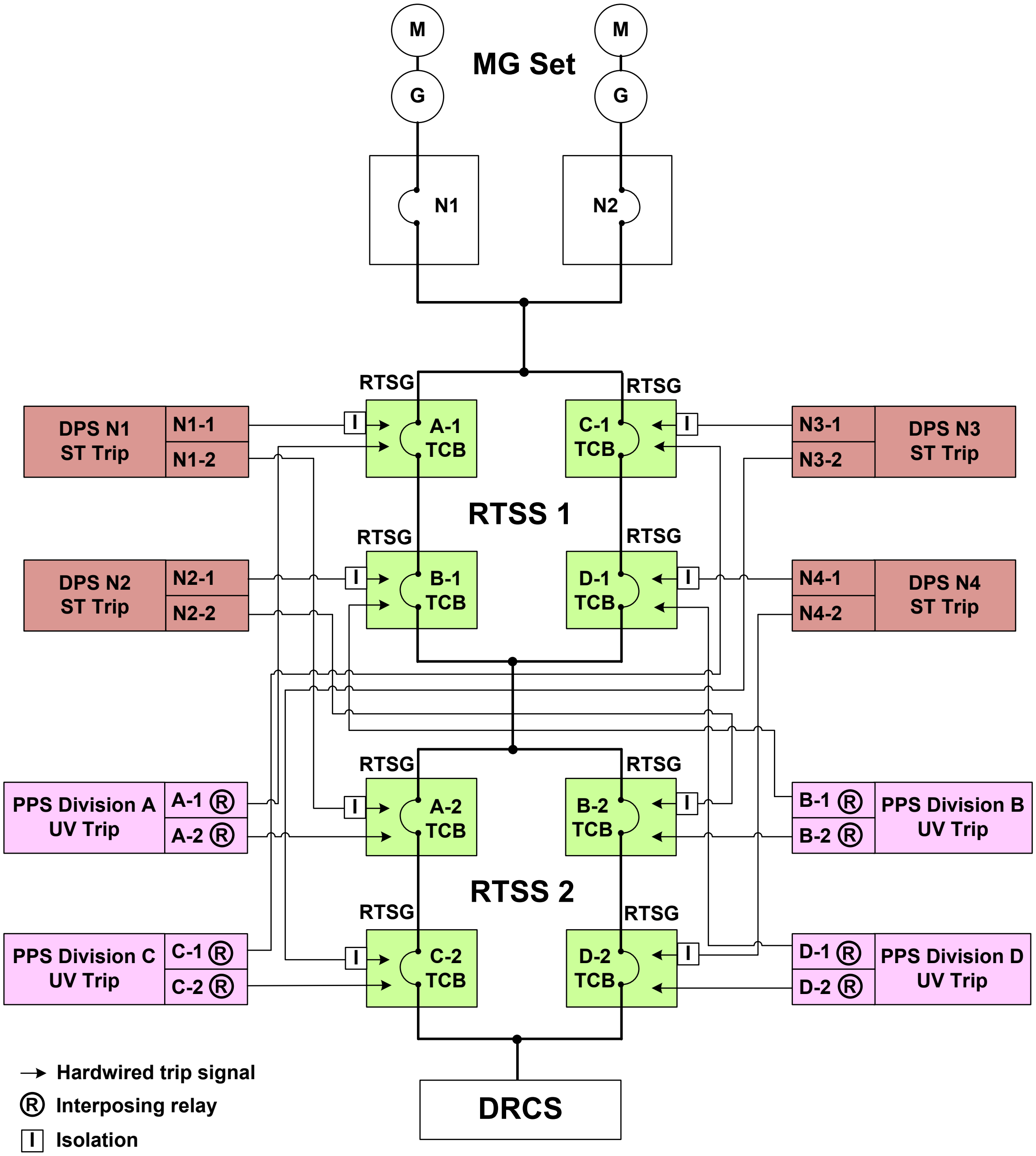


Figure 4-34 Reactor Trip Switchgear System Configuration

5 SOFTWARE RELIABILITY

5.1 Software Design Overview

Reliable computer software is essential to the design and operation of the safety I&C system equipment. The SPM TeR describes the software life cycle processes for the reliability and design quality of the safety I&C system and expands the procedural requirements of the APR1400 DC Quality Assurance Manual (QAM).

The SPM TeR is based on a software life cycle model consistent with industry standards (IEEE Std. 7-4.3.2 as endorsed by RG 1.152 and IEEE Std. 1012 as endorsed by RG 1.168) that include the following phases:

- Concept phase
- Requirements phase
- Design phase
- Implementation phase
- Test phase
- Installation and checkout phase
- Operation and maintenance phase

6 EQUIPMENT QUALIFICATION

The objective of equipment qualification is to demonstrate that the safety I&C system equipment is capable of performing its designated safety functions during and following a DBE.

Equipment qualification is composed of three major components: environmental, seismic and electromagnetic compatibility (EMC) qualification.

Equipment testing and analysis are performed to meet the requirements of IEEE Std. 603-1991, IEEE Std. 323-2003, EPRI TR-107330, EPRI TR-102323 Rev.1 and RG 1.180 Rev. 1. This testing/analysis includes electrical fast transient, electrostatic discharge, surge withstand capability, and Class 1E to Non-Class 1E isolation testing and confirms that the safety I&C system is fully qualified and capable of performing its designated safety functions while exposed to normal, abnormal, test, accident, and post-accident environmental conditions, as required.

6.1 Environmental Qualification

The safety I&C system equipment is qualified to meet the guidance of IEEE Std. 323-2003, as endorsed by RG 1.209. Since this equipment is located in the mild environments (MCR/RSR and/or I&C equipment rooms) where qualified heating, ventilation, and air conditioning (HVAC) is provided, the qualification is performed by a heat rise test and a subsequent analysis using linear temperature data extrapolation.

The tests are performed with the cabinet/enclosure energized to obtain temperature heat rise data at various locations within the cabinet assembly. Temperatures are monitored until they are stable within the cabinet with its doors and cable entrance areas closed. Then by linear extrapolation, the internal temperature profile based on a change in the external ambient temperature is determined.

The analysis demonstrates, using extrapolated test data, that individual component and equipment temperature specifications are not exceeded within the cabinet/enclosure when exposed to the environmental conditions. The environmental ranges to which equipment is exposed are specified in Table 6-1.

Table 6-1 Environmental Design Requirements

Environmental Parameter	Normal		
	Min.	Max.	Duration
Safety I&C System Cabinets in I&C Equipment Room			
Temperature Humidity Pressure Radiation	21ºC (70ºF) 40 %RH [1] Atmospheric 10 Gamma [3]	25ºC (77ºF) 60 % RH	Continuous Continuous Continuous Continuous
Safety I&C System in the MCR SC and RSC			
Temperature [2] Humidity Pressure Radiation	21ºC (70 ºF) 40 %RH Atmospheric 10 Gamma [3]	35ºC (95 ºF) 60 % RH	Continuous Continuous Continuous Continuous

Notes:

(1) Relative humidity is based on standard temperature and pressure of 21ºC (70 ºF) and 0 psig.

(2) Includes 10ºC (18 ºF) temperature rise within the MCR SC and RSC.

(3) Total integrated doses over equipment life time (40-yr TID Gy)

In regards to I&C cabinet protection design, the Class 1E cabinets located in the MCR and safety I&C equipment rooms are designed and fabricated to operate without loss of function when exposed to the environmental design requirements specified in Table 6-1.

The other Class 1E cabinets located in the auxiliary building area (except main control room and safety I&C equipment rooms) are designed and fabricated to operate without loss of function when exposed to the following environmental conditions:

• Temperature (°F)...............................	50-104 °F
• Relative humidity (%).........................	7-90 %
• Radiation (Gy)...................................	< 10 Gy (Gamma)

The non-Class 1E cabinets for DPS and DIS are located in the non-safety I&C equipment rooms and designed and fabricated to operate without loss of function for the following environmental conditions of the room:

• Temperature (°F)...............................	70 – 77 °F
• Relative humidity (%).........................	40 – 60 %
• Radiation (Gy)...................................	Negligible

The non-Class 1E cabinets for PCS and P-CCS are designed and fabricated to operate without loss of function for the following environmental conditions of the room:

• Temperature (°F)……………….……...	50-104 °F in auxiliary building area 70-77 °F in non-safety I&C equipment room 65-85 °F for DRCS power cabinets of PCS
• Relative humidity (%)..........................	7-90 % in auxiliary building area 40-60 % in non-safety I&C equipment room 40-60 % for DRCS power cabinets of PCS
• Radiation (Gy)...................................	Negligible

For these cabinets, the cooling and ventilation are provided by a fan mounted in the cabinet. Each cabinet contains a temperature sensor in the cabinet that is monitored. The fans are designed for continuous operation when the cabinet is powered. Though an alarm for loss of the fan is not provided, trouble alarms to indicate a high temperature in the cabinet are provided.

6.2 Seismic Qualification

The safety I&C system equipment is qualified by test, analysis or a combination of both methods to comply with the guidance of IEEE Std. 344-2004 as endorsed by RG 1.100. Functional operability tests are conducted during seismic qualification tests with the equipment energized and using simulated inputs and interfaces.

The safety I&C system is designated as seismic Category I meeting the guidance of RG 1.29. It is designed and qualified to maintain functional and physical integrity to withstand the cumulative effects of five (5) 1/2 SSE followed by one SSE. The 1/2 SSE and SSE at the safety I&C system cabinet and SC mounting points are characterized by the required response spectra , which envelope the I&C equipment room, multiplexer rooms and MCR SC.

The safety I&C system electro-mechanical components that have a significant aging mechanism, such as relays, are cycled to the end of operational life condition prior to qualification.

The seismic tests and/or analysis demonstrate that:

During the seismic events, no parts of the equipment will loosen, bend or crack in a manner that impairs proper operation. In addition, no parts of the equipment will become a missile hazard.
During and after the seismic event, the safety-related parameters of the equipment will be maintained.

6.3 EMI/RFI Testing

The safety I&C system equipment is qualified to comply with the guidance of MIL Std. 461E and IEC 61000 Part 4 Series as endorsed by RG 1.180. EMC testing of the equipment is performed for both conducted and radiated signals as follows:

- EMI/RFI emissions
- EMI/RFI susceptibility / immunity
- Surge withstand capability

The tests are performed on each system in various modes of operation such that successful completion of the test demonstrates that the safety system function has not been compromised and the equipment performs the function within its design specifications.

When conducting EMC equipment qualification, the test equipment represents the as-delivered configuration. The equipment grounding and power line filter are identical to the tested equipment.

The basis for selecting the specific tests and operating envelopes (test level, applicable frequency and limitations) is based on RG 1.180.

7 EQUIPMENT RELIABILITY

The safety I&C system architecture is designed for high reliability using PLC equipment as described in Section 8. The reliability (availability) of these system configurations to perform their safety functions, using the SFC, is demonstrated by the failure modes and effects analysis (FMEA).

7.1 Failure Modes and Effects Analysis (FMEA)

The FMEA is a “qualitative” evaluation which identifies various failure modes that can occur to the components that comprise a system. It is not a “Quantitative” reliability / availability analysis which produces calculated numerical values. The FMEA identifies potential single failures and their effects or consequences on the system’s ability to perform its functions. The system-level FMEA is provided in the DCD Chapter 7.

The FMEA is performed at the replaceable module level (i.e., PM, CI, I/O module). The FMEA is performed for the protection systems' sensors, and components responsible for the bistable/coincidence and actuating logic. The FMEA is prepared conservatively assuming that one division is already bypassed for maintenance.

At the hardware interface level, the FMEA considers the failure modes of all components from the input circuits to the output circuits, including all intermediate circuits and components, which process the system information/data. For the PLCs, the FMEA bounds all cases by considering the worst case effects at the outputs (e.g. communications failures, stalls, etc.). For binary outputs, open and closed statuses are addressed. For digital communication data (e.g., SDL), interfaces are analyzed for failure to transmit data, failure to receive data, and communication of erroneous data.

The safety I&C system is designed so that any single failure will not prevent proper protective action at the system-level. The FMEA shows that this objective is met.

The FMEA is typically documented in tabular format which includes the following table entries:

Element no.: Sequential number assigned to element/module/component

Name: Element/module/component descriptive name

Failure mode: Failure mode description: such as high/low output, on/off, open/closed, tripped/ not tripped, no data output, etc.

Cause: Most predictable cause of associated failure mode listed such as:

- External input/output circuits/cabling (open/shorted)
- Mechanical failure
- Vital instrument power buses (off/open/shorted/grounded)
- Internal AC/DC power supplies (off/open/shorted)
- Input and output modules (fail off/on/high/low/as-is)
- PLC processor modules (fail off/on/stalls)
- SDN and SDL data communications (fail off/transmit/ receive/as-is)

- Software (fails off/stalls/spurious data)
- Fiber optic receiver/transmitter modules (off/open/shorted)
- Relay coils/contact (open/shorted)
- Manual switches (open/shorted)

Symptoms and local effects: Identifies the immediate consequence of each failure mode and any secondary side effects.

Method of detection: Identifies method by which failure is detected, e.g.: self- annunciating, automatic or manual test, etc.

Inherent compensating provisions: Any compensating features within the design are addressed such as:

- Redundant divisions of the PPS and ESF-CCS
- Auctioneered AC/DC power supplies
- Fail-safe design. For example, outputs go to appropriate trip, initiation or actuation state upon loss of electrical power. Fail-safe design upon loss of data communications. For example, SDN failures (due to a CI failure, or break in an interconnecting coaxial or fiber optic cable, etc.) that result in loss of data communications to the receiving PM. Upon detection of the loss of communications, the effected PM will force its safety-related trip output signals to their “fail-safe” state.

Effect upon system: Describes the ultimate effect of the failure mode on the overall system, e.g.: the resulting logic becomes 2-out-of-3 coincidence or ESFAS function is actuated.

Remarks and other effects: Identifies the effects of the failure on overall plant operations or interfacing systems.

The FMEA considers the effects of these types of failures on the system and any other impacts on interfacing plant systems or components.

The system-level FMEA results for the PPS and ESF-CCS are included in the DCD.

8 SAFETY I&C SYSTEM PLATFORM

The safety I&C system is implemented on a common PLC platform using Common Q^{TM}. The platform has been dedicated and qualified for nuclear power plants and accepted by NRC after reviewing Common Qualified Platform Topical Report Revision 3 (Reference 12). The platform is configured using various hardware building blocks and loaded with application software to develop safety I&C systems such as PPS, ESF-CCS, CPCS and QIAS-P. The CPM, CCG, and ITP use the platform. The QIAS–N is also implemented on the common PLC platform even though it is a non-safety system.

The platform is Class 1E and consists of the following major building blocks.

- Controller with Processor Module
- Input and Output Modules
- Power Supply
- Flat Panel Display System
- AF100 Communication (AF100)
- High Speed Link (HSL)

The building blocks are used to design a specific safety system. The SDN and SDL are implemented using AF100 and HSL, respectively.

The Common Q^{TM} flat panel display system qualified in Common Qualified Platform Topical Report Revision 3 (Reference 12) is used for implementation of the safety FPDs for the ESCM, QIAS-P, and OM.

These FPDs are designed as Class 1E, and the development is performed under quality assurance program in accordance with 10 CFR Part 50 Appendix B. Also, the software development is verified and validated to ITS software grade.

The platform software resides in the processor module and consists of a real-time operating system, task scheduler, diagnostic functions, communication interfaces, and an application program. The application program is created using a software development tool that includes a function block library and developed according to the structured software life cycle process as described in the SPM TeR.

The supplemental information not found in the Common Q Topical Report is described in Reference 17.

The resolution of 2 Generic Open Items and 25 Plant Specific Action Items associated with NRC review of the Common Qualified Platform Topical Report for the APR1400 safety I&C system design is summarized in Reference 18.

9 REFERENCES

1. APR1400-Z-J-NR-14002-P, “Diversity and Defense-in-Depth,” February 2017

2. APR1400-Z-A-NR-14019-P, “CCF Coping Analysis”, February 2017

3. APR1400-E-J-NR-14001-P, “Component Interface Module,” February 2017

4. DI&C-ISG-04,Rev.1, “Highly Integrated Control Rooms – Communications Issues,” 2009

5. APR1400-K-Q-TR-11005-N, “KHNP Quality Assurance Program Description (QAPD) for the APR1400 Design Certification”

6. APR1400 DC Quality Assurance Manual (QAM)

7. APR1400-Z-J-NR-14004-P, “ Uncertainty Methodology and Application for Instrumentation,” February 2017

8. APR1400-Z-J-NR-14005-P, “Setpoint Methodology for Plant Protection System,” February 2017

9. APR1400-F-C-NR-14001-P, “CPC Setpoint Analysis Methodology for APR1400,” September 2014.

10. APR1400-Z-J-NR-14003-P, Rev. 0, “Software Program Manual”, February 2017

11. Design Control Document for the APR1400

12. WCAP-16097-P-A, “Common Qualified Platform Topical Report”, Rev. 3, February 2013

13. APR1400-Z-J-NR-14013-P, “Response Time Analysis of Safety I&C System,” February 2017

14. APR1400-Z-J-NR-14012-P, “Control System CCF Analysis,” February 2017

15. APR1400-F-C-NR-14003-P, “Functional Design Requirements for a Core Protection Calculator System for APR1400,” February 2017

16. APR1400-E-I-NR-14012-P, “Style Guide,” February 2017

17. APR1400-A-J-NR-14004-P (WCAP-17922-P, “Common Q Platform Supplemental Information in Support of the APR1400 Design Certification, “ Rev. 0, August 2014

18. APR1400-A-J-NR-14003-P (WCAP-17926-P), “APR1400 Disposition of Common Q Topical Report NRC Generic Open Item and Plant Specific Action Items,” Rev.0, October 2014

19. APR1400-E-I-NR-14011-P, “Basic Human-System Interface,” February 2017

20. APR1400-E-I-NR-14007-P, “Human-System Interface Design Implementation Plan,” February 2017

21. APR1400-E-I-NR-14004-P, “Task Analysis Implementation Plan,” February 2017

10 DEFINITIONS

Addressable Constant
A constant which can be changed on-line by plant personnel (or operator)

All-bypass
Bypass for all trip channel bypass bistable processing parameters at once

CEA shadowing
An effect in which the repositioning of control rods changes the reactivity worth of adjacent rods or causes a change in power level indication on ex-core neutron detectors when power level has remained constant

Checksum
A small-size datum from an arbitrary block of digital data for the purpose of detecting errors which may have been introduced during its transmission or storage

Flag
A flag refers to one or more bits that are used to store a binary value or code that has an assigned meaning

Gateway
A network node equipped for interfacing with another network that uses different communication protocols

Heartbeat
A periodic signal generated by application software to indicate normal operation of the system

Latch-reset
Output exists when latch input signal is generated until the reset signal is activated. The latch input is continuously blocked even after the reset signal is cleared. The block is removed only when the actuation signal is cleared and is re-actuated.

Partial trip
A trip state from either one of the redundant BPs

Penalty factor
A multiplicative number necessary to ensure that the CPCS calculates DNBR and LPD conservatively

Preset
Already determined or defined

Radial peaking factor
Radial direction ratio of maximum power to average power

SDN(AF100)
A communication system used for transferring process data and message within a single division which is implemented using Common Q Advant Fieldbus 100. The process data are used for monitoring and controlling a process, and the messages are used for program loading and for diagnostic purposes.

SDL(HSL) A communication system used to transmit data to other divisions in a multidivisional system which is implemented using Common Q High Speed Link (HSL) . Fiber-optic modems and cables maintain isolation of redundant safety divisions.

Self-checking Detecting faults or errors of the system automatically and constantly without any external command or action

Shape annealing A correction to adjust the ex-core signal so that each detector effectively sees only those core nodes immediately adjacent to it

Page intentionally blank

APPENDIX A CONFORMANCE TO IEEE STD. 603-1991

This Appendix describes how the safety I&C system satisfies the requirements of IEEE Std. 603-1991. The APR1400 is an advanced nuclear power plant and includes computer based safety I&C system. The following heading numbers with “A” correspond to the clause numbers of IEEE Std. 603-1991.

A.1 Scope

The safety system criteria contained in IEEE Std. 603 are applicable to the safety I&C system such as the PPS, CPCS, ESF-CCS, and QIAS-P, which initiate safety actions to mitigate the consequences of DBEs and monitor the status of the system. It is also applicable to those parts of data communication system that supports safety system functions.

A.2 Definitions

There is no exception in the safety I&C system designs to the definitions in IEEE Std. 603. It is noted that there is an alternative proposal for the independence requirements for the CPCS as discussed in Appendix D of this report.

A.3 References

RG 1.153 states that “Section 3 of IEEE Std. 603-1991 references several industry codes and standards. If a referenced standard has been incorporated separately into the Commission's regulations, licensees and applicants must comply with that standard as set forth in the regulation. If the referenced standard has been endorsed in a regulatory guide, the standard constitutes a method acceptable to the NRC staff of meeting a regulatory requirement as described in the regulatory guide. If a referenced standard has been neither incorporated into the Commission's regulations nor endorsed in a regulatory guide, licensees and applicants may consider and use the information in the referenced standard if appropriately justified, consistent with current regulatory practice.”

The safety I&C system complies with those referenced codes and standards that have either been endorsed by the NRC in a Regulatory Guide or are incorporated by reference in the Code of Federal Regulations.

A.4 Safety System Designation

The design of the safety I&C system is based on a set of specific design bases as follows. The heading number is consistent with the subclause number in Clause 4 of IEEE Std. 603-1991.

1. The DBEs applicable to each mode of operation of the generating station along with the initial conditions and allowable limits of plant conditions for each such event:

   The RPS is designed to ensure adequate protection of the fuel, fuel cladding, and RCS boundary during AOOs.

   In addition, the RPS is designed to assist the ESF Systems in mitigating the consequences of accidents.

   The ESFAS mitigates the result of an event to within the allowable value during the DBE.

   Each DBE is described in the DCD Chapter 15.

The allowable limit for each DBE and accident is described in the DCD Chapter 15.

2. The safety functions and corresponding protective actions of the execute features for each DBE:

The safety functions and corresponding protective actions for DBE stated in item 1 are as follows:

The RPS consists of fifteen trips in each of the four RPS divisions that will initiate the required automatic protective action utilizing a coincidence of two or more trip signals.

a) Variable Overpower Trip

(a) Input

Neutron flux power from the ENFMS.

(b) Purpose

To provide a reactor trip to assist the ESF systems in the event of an ejected CEA accident.

b) High Logarithmic Power Level Trip

(a) Input

Neutron flux power from the ENFMS.

(b) Purpose

To ensure the integrity of the fuel cladding and RCS boundary in the event of unplanned criticality from a shutdown condition, resulting from either dilution of the soluble boron concentration or uncontrolled withdrawal of CEAs.

If CEAs are in the withdrawn position, automatic trip action will be initiated. If all CEAs are inserted, an alarm is provided to alert the operator to take appropriate action in the event of an unplanned criticality.

c) High LPD Trip

(a) Inputs

Neutron flux power and hot pin axial power distribution from the ENFMS.

Radial peaking factors from CEA position measurement system (reed switch assemblies).

ΔT power from coolant temperatures, pressure and flow measurements.

PFs from CEACs for CEA deviation within a subgroup.

PFs generated within the CPC for subgroup deviation and groups out-of-sequence.

(b) Purpose

To prevent the linear heat rate (W/cm or kW/ft) of fuel pin in the core from exceeding fuel design limits in the event of AOOs.

d) Low DNBR trip

(a) Inputs

Neutron flux power and hot pin axial power distribution from the ENFMS.

RCS pressure from pressurizer pressure measurement.

ΔT power from coolant temperatures, pressure and flow measurements.

Radial peaking factors from CEA position measurement (reed switch assemblies).

Reactor coolant mass flow from reactor coolant pump speeds and temperatures.

Core inlet temperature from reactor coolant cold leg temperature measurements.

PFs from CEACs for CEA deviation within a subgroup.

PFs generated within the CPC for subgroup deviation and groups out-of-sequence.

(b) Purpose

To prevent the DNB ratio of the coolant channel in the core from exceeding the fuel design limit in the event of AOOs. In addition, this trip will provide a reactor trip to assist the ESF systems in limiting the consequences of the steam line break outside containment, SG tube rupture and reactor coolant pump shaft seizure accidents.

e) High Pressurizer Pressure Trip

(a) Input

Reactor coolant pressure from narrow range pressurizer pressure measurement.

(b) Purpose

To assure the integrity of the RCS boundary for any defined AOO that could lead to an over pressurization of the RCS.

f) Low Pressurizer Pressure Trip

(a) Input

Reactor coolant pressure from wide range pressurizer pressure measurements.

(b) Purpose

To provide a reactor trip to assist the ESF systems in the event of reduction in system pressure and a LOCA

g) Low SG Water Level Trips

(a) Input

Level of water in each SG downcomer region from wide range differential pressure measurements.

(b) Purpose

To provide a reactor trip to assist the ESF systems ensuring that there is sufficient time for actuating the auxiliary feedwater pumps to remove decay heat from the reactor in the event of a reduction of SG water inventory.

h) Low SG Pressure Trips

(a) Input

Steam pressure in each SG.

(b) Purpose

To provide a reactor trip to assist the ESF systems in the event of a steam line break accident.

i) High Containment Pressure Trip

(a) Input

Pressure inside containment.

(b) Purpose

To assist the ESF systems by tripping the reactor coincident with the initiation of safety injection caused by excessive pressure in containment.

j) High SG Water Level Trips

(a) Input

Level of water in each SG downcomer region from narrow range differential pressure measurements.

(b) Purpose

To assist the ESF systems by tripping the reactor coincident with initiation of main steam isolation caused by a high SG water level.

k) Low Reactor Coolant Flow

(a) Input

Differential pressure measured across the SG primary side.

(b) Purpose

To provide a reactor trip in the event of a reactor coolant pump sheared shaft.

l) Manual Reactor Trip

(a) Input

Two independent pairs of trip switches are provided at MCR and one set of trip switches in the RSR consoles.

(b) Purpose

Manual reactor trip is provided to permit the operator to trip the reactor.

The ESFAS utilizes bistable logic and coincidence logic in the PPS and coincidence logic and component control logic in the ESF-CCS to generate actuation signals. Actuation signals are provided as input signals to the ESF system. Upon receipt of ESFAS initiation signal from the PPS, the ESF-CCS generates the following actuation signals.

- Containment isolation actuation signal (CIAS) initiated by high containment pressure trip and low pressurizer pressure trip
- Containment spray actuation signal (CSAS) initiated by high-high containment pressure trip
- Main steam isolation signal (MSIS) initiated by high containment pressure trip, low SG1/2 pressure trips, and high SG1/2 water level trips
- Safety injection actuation signal (SIAS) initiated by high containment pressure trip and low pressurizer pressure trip
- Auxiliary feedwater actuation signal (AFAS)-1 initiated by low SG1 water level trips
- Auxiliary feedwater actuation signal (AFAS)-2 initiated by low SG2 water level trips

3. The permissive conditions for each operating bypass capability that is to be provided:

a) The RPS operating bypass types (name and function), permissive and removal condition are described in Table 7.2-1 of the DCD.

b) The ESFAS operating bypass types (name and function), permissive and removal condition are described in Table 7.3-1 of the DCD.

4. The variables or combination of variables, or both, that are to be monitored to manually or automatically, or both, control each protective action:

The monitored variables are provided in Table 7.2-2 of the DCD.

The RPS monitors the following generating station conditions in order to provide adequate protection during AOOs:

a) Core power (neutron flux)

b) Reactor coolant system pressure

c) DNBR in the limiting coolant channel in the core.

d) Peak local power density in the limiting fuel pin in the core

e) SG water level

f) Reactor coolant flow

The RPS monitors the following generating station conditions in order to assist the ESF in mitigating the consequences of accident:

a) Core power

b) RCS pressure

c) SG pressure

d) Containment pressure

e) Reactor coolant flow

The ESFAS monitors the process variables, listed in Table 7.3-3 of the DCD, in order to actuate the protective action during the DBE.

The system is designed so that protective action will not be initiated during normal operations. The selection of these trip setpoints is such that adequate protection is provided, since all sensor and processing time delays and inaccuracies have been taken into accounts. Uncertainties methodology is described in the Uncertainty Methodology and Application for Instrumentation TeR and setpoint methodology is described in the Setpoint Methodology for Plant Protection System TeR.

Reactor trip delay times and analysis setpoints used in the Chapter 15 are given in Tables 7.2-5 and 15.0-2 of the DCD.

The RPS sensor response times, reactor trip delay times, and analysis setpoints used in Chapter 15 of the DCD are representative of the manner in which the RPS and associated instrumentation will operate. These quantities are used in the transient analysis documented in Chapter 15 of the DCD. Actual RPS equipment uncertainties, response times and reactor trip delay times are obtained from calculations and tests performed on the RPS and associated instrumentation. The verified system uncertainties are factored into all RPS setpoints to ensure that the system works as intended when the errors and uncertainties combine in a conservative manner.

5. The following minimum criteria for each action whose operation may be controlled by manual means initially or subsequent to initiation:

5.1. The points in time and the plant conditions during which manual control is allowed.

Manual control is not credited within 30 minutes of an accident occurring. The assumption, initial condition, event details and plant state for each accident and event is described in Chapter 15 of the DCD. Manual control after RPS initiation is performed according to EOP for plant state.

The manual initiation is not allowed in principle prior to the actuation of ESFAS by exceeding the setpoint after event onset. The assumption, initial condition, event details and plant state for each accident and event are described in the DCD Chapter 15. The manual control after ESFAS initiation is performed in accordance with the EOP which is established for the plant status.

5.2 The justification for permitting initiation or control subsequent to initiation solely by manual means.

The RPS and ESFAS are not designed to permit initiation only by manual means.

5.3 The range of environmental conditions imposed upon the operator during normal, abnormal, and accident circumstances throughout which the manual operations shall be performed.

MCR environmental conditions during manual operation are described in Section 6.4 of the DCD.

5.4 The variables in item 4 that shall be displayed for the operator to use in taking manual action.

The variable list in item 4 that is displayed for the operator for taking manual action is described in Table 7.5-1 of the DCD.

6. For those variables in item 4 that have a spatial dependence, the minimum number and locations of sensors required for protective purpose:

   The number and location of the sensors provided to monitor those variables in item 4 are given in Tables 7.2-3 and 7.3-4 of the DCD. The location of precision RTD for measuring RCS hot leg temperature is assigned to measure appropriate coolant transmission effects by temperature difference and temperature distribution of hot leg.

7. The range of transient and steady state conditions of both motive and control power and the environment during normal, abnormal, and accident conditions throughout which the safety system shall perform:

   The safety I&C system is qualified to meet environmental conditions in Section 3.11 of the DCD, in accordance with IEEE 323. In addition, the system is capable of performing its intended function under the most degraded conditions of the energy supply, as addressed in Section 8.3 of the DCD.

8. The conditions having the potential for functional degradation of safety performance and for which provisions shall be incorporated to retain the capability for performing the safety functions:

   The RPS and ESFAS logic design takes account of functional degradation that could occur in the following conditions:

   a) System actuation due to the power loss of measurement channel

   b) Appropriate system-level protective action due to single accident in system

   c) The system is verified according to IEEE 344 to demonstrate that the RPS and ESFAS can perform the intended function for seismic conditions.

   d) The RPS is verified according to IEEE 323 to demonstrate that the RPS can perform the intended function for environment conditions.

   e) System components are qualified according to an established plan for EMC that requires the equipment to function properly when subjected to electrical surges, electromagnetic interference, radio frequency interference, and electrostatic discharge. Qualification is applied in equipment based on operating environment and/or inherent design characteristics. Electromagnetic interference qualification is performed in accordance with RG 1.180 and IEC 61000-4-2. Radiated and conducted electromagnetic interference envelopes are established for qualification.

9. The methods to be used to determine that the reliability of the safety system design is appropriate for each safety system design and any qualitative or quantitative reliability goals that may be imposed on the system design:

   The reliability is described in Section 7.

10. The critical points in time or the plant conditions, after the onset of a DBE, including:

    10.1 The points in time or the plant conditions for which the protective actions of the safety system shall be initiated.

    The point, for which the reactor shutdown shall be initiated (trip setpoint) is described in Tables 7.2-4 and 7.3-5A of the DCD, and initial event and frequency causing initiation of protective action are described in Table 15.0-3 of the DCD.

10.2 The points in time or the plant conditions that define the proper completion of the safety function

The point in time for the proper completion of RPS safety function is when CEA is injected completely into the core.

The completion of the ESFAS function means from the ESFAS initiation to the generation of the required function.

In this time, plant maintains the following conditions.

Core reactivity maintains the subcritical state with sufficient margin corresponding to TS and, does not exceed thermal design limit of core and reactor coolant system by removing core decay heat at controlled cooling rate.

The vital equipment and system operate within design range for maintaining the above conditions.

The equipment and system for maintaining offsite dose within an acceptable limit are operating appropriately.

10.3 The points in time or the plant conditions that require automatic control of protective actions

The accident analysis in Chapter 15 of the DCD does not consider manual control in the first 30 minutes after accident and the point in time (RPS trip set point (Refer to Table 7.2-4 of the DCD)) for automatic control of protection system is set based on accident analysis results.

The accident analysis in the DCD Chapter 15 does not consider manual control in the first 30 minutes after accident and the point (ESF actuation set point (Refer to Table 7.3-5A of the DCD)) for automatic control of protection system is established based on accident analysis results.

Automatic initiation is required for maintaining item 10.2 condition when reaching setpoint.

Manual control is possible after the 30 minutes according to the EOP based on the plant condition, if required.

10.4 The points in time or the plant conditions that allow returning a safety system to normal

When the plant operates in condition of 10.2 above, returning a safety system to normal is allowed.

11. The equipment protective provisions that prevent the safety systems from accomplishing their safety functions:

The PPS and ESF-CCS consist of redundant channels with independence features. The safety functions are initiated and accomplished by the PPS and ESF-CCS at the system level. Therefore, there is no single failure of an equipment protective device which prevents initiating and accomplishing the safety functions at the system level.

Each component control logic in the ESF-CCS LC detects the conditions of equipment and determines if the equipment can be operated. Examples for the load center circuit are as follows:

a) Circuit breaker not in the operating position, detected by a cell switch that indicates the draw-out circuit breaker position,

b) Loss of trip or closing circuit control power, detected by a control power monitoring circuit,

c) Loss of breaker trip or closing circuit continuity, detected by a coil circuit continuity monitoring circuit

d) Absence of starting circuit permissive interlock signals that normally exist to permit starting of the equipment, when shown on individual control logic,

e) Existence of mechanical protection signal that would block starting of the equipment, when shown on individual control logic,

f) Module disable condition including internal disabled conditions, detected by self-test and error detection by ESF-CCS.

In addition, descriptions of the protective devices for electrical power circuits, such as protection relays, are provided in the following sections of APR1400 DCD Tier 2:

- Section 8.3.1.1.1.1 for large motors,
- Section 8.3.1.1.1.2 for 4.16kV motors,
- Section 8.3.1.1.1.3 for 480V load centers,

As described in DCD Tier 2, Section 8.3.1.1.3.12, protective devices for the Class 1E ac power system are designed with the same non-Class 1E ac power system described in Subsections 8.3.1.1.1.1, 8.3.1.1.1.2, and 8.3.1.1.1.3.

The description of the protective relay trip of the EDG is described in Section 8.3.1.1.3.3 of APR1400 DCD Tier 2.

The ESCM provides component control signals such as start or stop signal for components. The equipment protective logic is implemented in the component control system or electrical panel. Therefore, the component data from IFPD to ESCM are not used to control equipment protective devices.

12. Any other special design basis that may be imposed on the system design (example., diversity, interlocks, regulatory agency criteria):

    The system is designed to reduce the failure of redundant divisions anticipated by CCF.

A.5 Safety System Criteria

Clause 5 states:

The safety systems shall, with precision and reliability, maintain plant parameters within acceptable limits established for each design basis event. The power, instrumentation, and control portions of each safety system shall be comprised of more than one safety group of which any one safety group can accomplish the safety function.

Analysis:

In addressing Clauses 5.1 through 5.15 below, the analysis confirms that the general functional criteria for the safety I&C system have been appropriately allocated to the various system components. The design review in this regard concludes that the system design fulfills the APR1400 system design basis criteria established. This design review is from an integrated hardware/software perspective.

A.5.1 Single-Failure Criterion

Clause 5.1:

“The safety systems shall perform all safety functions required for a DBE in the presence of: (1) any single detectable failure within the safety systems concurrent with all identifiable but non-detectable failures; (2) all failures caused by the single failure; and (3) all failures and spurious system actions that cause or are caused by the DBE requiring the safety functions. The single-failure criterion applies to the safety systems whether control is by automatic or manual means. IEEE Std. 379-1988 provides guidance on the application of the single-failure criterion.

This criterion does not invoke coincidence (or multiple-division) logic within a safety group; however, the application of coincidence logic may evolve from other criteria or considerations to maximize plant availability or reliability. An evaluation has been performed and documented in other standards to show that certain fluid system failures need not be considered in the application of this criterion. The performance of a probable assessment of the safety systems may be used to demonstrate that certain postulated failures need not be considered in the application of the criterion. A probable assessment is intended to eliminate consideration of events and failures that are not credible; it shall not be used in lieu of the SFC, IEEE Std. 352-1987 and IEEE Std. 577-1976 provide guidance for reliability analysis.

Where reasonable indication exists that a design that meets the SFC may not satisfy all the reliability requirements specified in 4.9 of the design basis, a probable assessment of the safety system shall be performed. The assessment shall not be limited to single failures. If the assessment shows that the design basis requirements are not met, design features shall be provided or corrective modifications shall be made to ensure that the system meets the specified reliability requirements.”

Analysis:

The BP in the PPS provides their trip signals to the LCL processor located in the four redundant divisions. The local coincidence logic processors determine the local coincidence logic trip based on the state of the four bistable trip signals and their respective bypasses. Single failures at the coincidence logic level are accommodated by either redundancy within each division or redundancy across the four divisions. The coincidence trip signals are used in the generation of the RTSS or ESF-CCS initiation. The PPS is designed so that any single failure within the system shall not prevent proper protective action at the system-level, even when a channel is intentionally bypassed for test or maintenance. No single failure will defeat more than one of the four protective divisions associated with any one trip function.

Single failure of RTSG is accommodated by the full 2-out-of–4 arrangement of the devices. A spurious opening of a RTSG does not result in either spurious trip or loss of ability to trip.

The ESFAS initiation signals from the PPS are sent to separate ESF-CCS cabinets. Each cabinet contains the actuation logic for only one division; therefore, a failure in one cabinet cannot affect the circuitry and actuated equipment of the other divisions.

However, the BOP ESF systems are 1-out-of-2 logic taken twice except the FHEVAS initiation signal that performs 1-out-of-2 logic taken once. For these cases, the single failure criterion is met by changing the logic to a 1-out-of-2 (1-out-of-1 during maintenance bypass).

Since the BOP ESFAS design is based on 1-out-of-2 taken twice, if one division is placed in bypass during testing and simultaneously an accident and single failure in another division occurs, then, the bypassed division will be automatically switched to operation mode.

Also, the purpose of bypass mode of the BOP ESFAS is to test a measurement channel. For the BOP ESFAS design, redundant measurement channels are provided. Even if one measurement channel is placed in test mode, the other measurement channel in same division is available.

Single failures of the actuation (or control) logic will cause, at worst, only a failure of a component, group of components, or one entire redundant train; actuation of the remaining redundant division is sufficient for the protective action.

The wiring in the system is grouped so that no single fault or failure, including either an open or shorted circuit, will negate protective system operation. Signal conductors and power leads coming into or going out of each cabinet are protected and routed separately for each division of each system to minimize possible interaction.

Single failures considered in the design of the safety I&C system are described in the FMEA in the DCD (Refer to Tables 7.2-7 and 7.3-8 in the DCD).

A.5.2 Completion of Protective Action

Clause 5.2:

“The safety systems shall be designed so that, once initiated automatically or manually, the intended sequence of protective actions of the execute features shall continue until completion. Deliberate operator action shall be required to return the safety systems to normal. This requirement shall not preclude the use of equipment protective devices identified in 4.11 of the design basis or the provision for deliberate operator interventions. Seal-in of individual channels is not required.”

Analysis:

The design for safety I&C system meets the requirements of IEEE Std. 603-1991 Clause 5.2, Completion of Protective Action. The safety I&C system design is such that, once initiated, the protective action will proceed to completion. Return to normal operation requires manual reset action by the operator.

The system is designed to ensure that protective actions such as RPS and ESFAS will go to completion once initiated. Operator action is required to clear the trip (or initiation) and return to operation.

An RPS function is initiated when the TCBs in RTSS open. A protective action is completed when the CEAs arrive at their full-in position.

An ESFAS function is initiated when the 2-out-of-4 logic in the PPS is met. A protective action is completed when all of the appropriate ESF components are actuated to the proper state for their ESF function.

The ESF components remain in the actuated safe state until the ESF system-level actuation signal is manually reset after the trip condition in the PPS is cleared.

A.5.3 Quality

Clause 5.3:

“Components and modules shall be of a quality that is consistent with minimum maintenance requirements and low failure rates. Safety system equipment shall be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a pre-scribed quality assurance program (ANS/ASME NQA-1-1989).”

Analysis:

The platform to be used for the safety I&C system is qualified as described in Reference 12. Development of the safety I&C system is performed under a quality assurance program in accordance with 10 CFR Part 50 Appendix B.

The QAPD describes the quality assurance program that is used for the design, manufacture, inspection, installation, testing, operation, and maintenance of the safety I&C system.

A.5.4 Equipment Qualification

Clause 5.4:

“Safety system equipment shall be qualified by type test, previous operating experience, analysis, or any combination of these three methods, to substantiate that it will be capable of meeting, on a continuing basis, the performance requirements as specified in the design basis. Qualification of Class 1E equipment shall be in accordance with the requirements of IEEE Std. 323-1983 and IEEE Std. 627-1980.”

Analysis:

Equipment qualification (environmental, seismic and EMI/RFI qualification) of the safety I&C system is described in Section 6.

Section 6 of this report provides a summary of the equipment testing and analysis performed to meet the requirements of IEEE Std. 603-1991, IEEE Std. 323-2003, EPRI TR-107330, EPRI TR-102323 Rev.1 and RG 1.180 Rev.1. This report addresses the specific required environmental conditions and testing/analysis performed to qualify this equipment.

A.5.5 System Integrity

Clause 5.5:

“The safety systems shall be designed to accomplish their safety functions under the full range of applicable conditions enumerated in the design basis.”

Analysis:

Type testing of components, separation of sensors and channels, and qualification of the cabling are performed to ensure that the channels maintain their functional capability required under applicable extremes of environment, power supplied, malfunction, and DBE conditions.

Loss of any one channel will not prevent the protective action of the PPS and ESF-CCS. Sensors are connected so that blockage or failure of any one connection does not prevent protective system action. The process transducers located in the containment building are specified and rated for the intended service. Components that must operate during or after a limiting fault (postulated accident) are qualified for the most limiting environment for the period of time for which they must maintain their functional capability. Results of type tests are used to verify this.

The system response time test is performed before and after installation to ensure the protective function completes within the allocated time as specified in Chapter 7 of the DCD. The PPS and ESF-CCS meet the requirements of IEEE Std. 7-4.3.2 for design considering computer system integrity, test and calibration. When the critical failure of hardware and software is detected by the PLC’s diagnostic functions, the outputs of the PPS and ESF-CCS go to fail-safe state and generate alarms. The PPS provides alarms to the QIAS-N and IPS to indicate system abnormalities.

During PPS restart, all outputs are set to the trip or initiation condition and the ESF-CCS to non-actuated condition. These initial conditions are maintained until the application program is executing properly.

The test and maintenance equipment such as the MTP/ITP are designed not to affect the system safety function. The FE keyswitch is used to force a permissive before performing system test and maintenance functions.

The safety I&C system application software development, verification and validation, testing and configuration management for safety I&C system software meet the requirements in the SPM TeR.

A.5.6 Independence

Clause 5.6.1: Between Redundant Portions of a Safety System.

“Redundant portions of a safety system provided for a safety function shall be independent of and physically separated from each other to the degree necessary to retain the capability to accomplish safety function during and following any DBE requiring that safety function.”

Analysis:

The safety I&C system cabinets for each division are geographically distributed into four separate divisionalized I&C equipment rooms.

The routing of Class 1E and associated cabling and sensing lines from sensors meet the requirements of RGs 1.75 and 1.151.

This requires that the cabling for the four safety divisions be routed separately; however, the cables of different safety functions within one division may be routed together. Low energy signal cables are generally routed separately from all power cables. Safety-related sensors are separated. The separation of safety-related cables requires that the cables be routed in separate cable trays.

The safety I&C system division receives non-interruptable AC power from the Vital Bus Power Supply System. The safety I&C system does not share power between divisions to preserve electrical separation and isolation.

Redundant portions of the safety I&C system are independent from one another so that a failure in any one portion of the system does not prevent the redundant portions from performing the RPS and ESFAS function.

The LCL in the PPS receives the signals from redundant channel and the GC in the ESF-CCS receives signals from each division through fiber optic modem and cables electrical isolation.

Refer to Appendix C for communication independence between divisions and Appendix D for the alternative compliance of the CPCS design.

Clause 5.6.2: Between Safety Systems and Effects of Design Basis Event

“Safety system equipment required to mitigate the consequences of a specific DBE shall be independent of, and physically separated from, the effects of the DBE to the degree necessary to retain the capability to meet the requirements of this standard. Equipment qualification in accordance with 5.4 is one method that can be used to meet this requirement.”

Analysis:

Independence of the components in the safety I&C system to the effects of a design-basis event is provided by qualifying the equipment in accordance with the requirements in Section 6 of this report.

Clause 5.6.3: Between Safety Systems and Other Systems

"The safety system design shall be such that credible failures in and consequential actions by other systems, as documented in 4.8 of the design basis, shall not prevent the safety systems from meeting the requirements of this standard."

Analysis:

All qualification test and analysis methods, envelopes and acceptance criteria for the isolation devices are the same as those defined in Section 6 because the isolation devices are installed inside of the ESF-CCS LC cabinets.

"5.6.3.1 Interconnected Equipment

(1) Classification: Equipment that is used for both safety and non-safety functions shall be classified as part of the safety systems, Isolation devices used in a safety system boundary shall be classified as part of the safety system.

(2) Isolation: No credible failure on the non-safety side of an isolation device shall prevent any portion of a safety system from meeting its minimum performance requirements during and following any DBE requiring that safety function. A failure in an isolation device shall be evaluated in the same manner as a failure of other equipment in a safety system."

Analysis:

The safety I&C system consists of four independent divisions except the QIAS-P and the BOP ESFAS which consist of two divisions. The protection division is physically separated and electrically isolated from the other three protection divisions. All connections to non-safety equipment, including the signal interface from the PPS to the TCS and from the ENFMS to the NIMS, are through isolation devices that are Class 1E qualified and are one way during plant operation. As an exception, the IFPD communicated to the ESCM to send identification data, which does not adversely affect safety functions and systems, through communication isolation to meet the guidance DI&C-ISG-04. The details for communication independence are described in Appendix C.5. As a result, failures of non-safety systems cannot prevent any safety I&C system from performing its safety function. All equipment/components used for safety-related functions are qualified as safety.

Outputs from the safety system to non-safety-related areas are isolated utilizing fiber optic cable so that a failure in the non-safety-related area does not cause loss of the safety system function. Also, these communications are unidirectional.

A non-Class 1E instrumentation circuits and cables that are in proximity of Class 1E circuits without adequate physical separation or electrical isolation are classified as an associated circuit regardless of whether or not analyses or tests can demonstrate that credible failures therein cannot adversely affect Class 1E circuits.

"5.6.3.2 Equipment in Proximity

(1) Separation: Equipment in other systems that is in physical proximity to safety system equipment, but that is neither an associated circuit nor another Class 1E circuit, shall be physically separated from the

safety system equipment to the degree necessary to retain the safety systems' capability to accomplish their safety functions in the event of the failure of non-safety equipment. Physical separation may be achieved by physical barriers or acceptable separation distance. The separation of Class 1E equipment shall be in accordance with the requirements of IEEE Std. 384-1981.

(2) Barriers: Physical barriers used in a safety system boundary shall meet the requirements of 5.3, 5.4 and 5.5 for the applicable conditions specified in 4.7 and 4.8 of the design basis."

Analysis:

Physical separation is achieved by physical barriers or acceptable separation distance. The separation of Class 1E equipment is designed in accordance with the requirements of IEEE Std. 384-1981.

"5.6.3.3 Effects of a Single Random Failure

Where a single random failure in a non-safety system can (1) result in a design basis event, and (2) also prevent proper action of a portion of the safety system designed to protect against that event, the remaining portions of the safety system shall be capable of providing the safety function even when degraded by any separate single failure.

See IEEE Std. 379-1988 for the application of this requirement."

Analysis:

Separate CPs are utilized to protect the Class 1E functional processors from handshaking and data communication errors (PM CS for SDL communication and the MTP and Ethernet interface module for the IPS). Therefore, the SDL and IPS communication are both functionally and electrically isolated. These communications are functionally isolated because a separate CP is used, and electrically isolated because fiber optic modems and cabling are used for the communication media.

Failures have been analyzed (FMEA) to ensure that a single failure cannot result in a design basis event and then prevent proper protective action to mitigate the event. The design meets the guidance provided in IEEE 379-1988

Clause 5.6.4:

"IEEE Std. 384-1981 provides detailed criteria for the independence of Class 1E equipment and circuits."

Analysis:

Each division is independent of the other redundant divisions. The sensors are separated, power supplies are separated, cabling is routed separately and each redundant division is located in a separate cabinet in a separate room. This minimizes the possibility of a single event causing more than one division's failure. The outputs from these redundant divisions are isolated from each other so that a single failure does not cause impairment of the system function.

Within the safety I&C system, physical and electrical independence is maintained between divisions for trip functions by using fiber optic cables to transmit data via interdivisional SDL to redundant divisions for coincidence processing.

The details for communication independence are described in Section 4 and Appendix C.

A.5.7 Capability for Test and Calibration

Clause 5.7: Capability for Test and Calibration

“Capability for testing and calibration of safety system equipment shall be provided while retaining the capability of the safety systems to accomplish their safety functions. The capability for testing and calibration of safety system equipment shall be provided during power operation and shall duplicate, as closely as practicable, performance of the safety function. Testing of Class 1E systems shall be in accordance with the requirements of IEEE Std. 338-1987. Exceptions to testing and calibration during power operation are allowed where this capability cannot be provided without adversely affecting the safety or operability of the generating station. In this case:

(1) appropriate justification shall be provided (for example, demonstration that no practical design exists),

(2) acceptable reliability of equipment operation shall be otherwise demonstrated, and

(3) the capability shall be provided while the generating station is shut down.”

<u>Analysis</u>:

The safety I&C system design complies with IEEE Std. 338-1987 and RG 1.22.

The safety I&C system incorporates enhanced continuous system self-checking features. System self-checking features include on-line diagnostics for the PLC software, hardware, and communications systems. Administrative procedures provide appropriate guidance in the event a portion of the safety system is in bypass or is manually tripped. These procedures are augmented by automatic indication at the system-level that a portion of the system is in bypass or that a portion of the protection system and/or the systems actuated or controlled by the protection system is tripped.

The PPS, CPCS, and ESF-CCS make extensive use of watchdog timers in performing built-in self tests. The output of the watchdog timer causes the fail-safe state for RPS and ESFAS functions.

Provisions for periodic manual surveillance testing provide the overlapped testing functions that confirm operability of the system and specifically determine operability of portion of the system that is not tested by the system’s self-diagnostics.

The requirement for periodic testing is addressed by channel calibrations, channel checks and functional testing. The channel calibrations are performed during refueling outages when the PPS is not required to be operable. Calibration and testing will be performed according to plant specific approved procedures that establish specific surveillance techniques and surveillance intervals intended to maintain high reliability.

Manual surveillance testing verifies that the system components and connections have not failed or degraded, and that trip signal paths for safety functions are correct. Software itself does not "degrade" over time unless there is an associated hardware failure. Also, V&V confirms that the software is correct. Therefore, the purpose of surveillance testing is to validate system operability. The PLC internal diagnostic functions check the hardware integrity and supervise software integrity by CRC checks.

The test feedback of one division is displayed only by the MTP of that division. The ITP puts the data on the SDN for the MTP displays.

The PPS bypasses are initiated via channel bypass switches on the MTP switch panel.

The response time is verified by measurement during plant startup testing. Sensor responses are measured during factory or laboratory testing and provided to the site operator for use in the test program.

A.5.8 Information Display

Clause 5.8.1 Displays for Manually Controlled Actions

“The display instrumentation provided for manually controlled actions for which no automatic control is provided and that are required for the safety systems to accomplish their safety functions shall be part of the safety systems and shall meet the requirements of IEEE Std. 497-1981. The design shall minimize the possibility of ambiguous indications that could be confusing to the operator.”

Analysis:

The QIAS-P provides a continuous and dedicated display of RG 1.97, Rev.4, Types A, B and C variables including the ICC monitoring variables.

The QIAS-N processes and displays variables for Type A, B and C. The QIAS-N also displays selected variables of Type D and E to support performing plant safe shutdown and EOPs.

The IFPD presents the displays for all variables for Type A, B, C, D and E, and provides recording function for Type A, B and C variables.

Clause 5.8.2: System Status Indication

“Display instrumentation shall provide accurate, complete, and timely information pertinent to safety system status. This information shall include indication and identification of protective actions of the sense and command features and execute features. The design shall minimize the possibility of ambiguous indications that could be confusing to the operator. The display instrumentation provided for safety system status indication need not be part of the safety systems.”

Analysis:

System status indication is provided for all protective actions at the OM, IPS and MTP, including identification of division trips.

Clause 5.8.3: Indication of Bypasses

“If the protective actions of some part of a safety system have been bypassed or deliberately rendered inoperative for any purpose other than an operating bypass, continued indication of this fact for each affected safety group shall be provided in the control room.”

Analysis*:*

The operating bypass and trip channel bypass status is available for display at the IPS display and OM in the MCR, and MTP in the I&C equipment room.

“5.8.3.1 This display instrumentation need not be part of the safety systems.”

Analysis:

Although the requirement does not mandate the displays be safety-related in the MCR, the OMs, which are part of the safety system, do display this information in the MCR. In addition, the status information is provided to the non-safety IPS for display in the MCR.

“5.8.3.2 This indication shall be automatically actuated if the bypass or inoperative condition (a) is expected to occur more frequently than once a year, and (b) is expected to occur when the affected system is required to be operable.”

Analysis:

Regardless of the frequency of the bypass or inoperative condition, these indications are always provided in the MCR.

“5.8.3.3 The capability shall exist in the control room to manually activate this display indication.”

Analysis:

These indications are always provided in the LDP and can be simply viewed by navigating to the appropriate displays in the IFPD.

Clause 5.8.4: Locations

“Information displays shall be located accessible to the operator. Information displays provided for manually controlled protective actions shall be visible from the location of the controls used to effect the actions.”

Analysis:

Information regarding displays is provided throughout this report. The display instrumentation provided for manually controlled actions for all displays necessary for the safety systems to accomplish their safety functions are part of the safety systems and meet these requirements.

The PLC used by the safety I&C system supports interfaces with a variety of analog and digital devices, including SC analog indicators and digital visual display units (e.g., OM). The safety I&C system provides the status indication signals to satisfy the requirements of RG 1.47 (i.e., to be provided to the MCR from each protection set for indication that a protection division has been placed in an inoperable condition).

Status information including input variable value, setpoint, trip, pre-trip, initiation, trip channel bypass and operating bypass is displayed on the IPS display’ the OM FPD in the MCR, and MTP in the I&C equipment room.

A.5.9 Control of Access

Clause 5.9:

“The design shall permit the administrative control of access to safety system equipment. These administrative controls shall be supported by provisions within the safety systems, by provision in the generating station design, or by a combination thereof.”

Analysis:

The safety I&C system has several design features to control physical assess including access for maintenance and test.

Control of the software and hardware during development (secure development environment) comply with the provisions of RG 1.152, Rev 3, as described in the SPM TeR.

Keys or built-in features are provided to control access to setpoints, calibration data, and test point adjustments. Access is indicated to the operator. Access is controlled via key locks, administrative procedures. Access to equipment rooms and cabinets are controlled by the utility to only personnel who are intended to have access

A.5.10 Repair

Clause 5.10:

"The safety systems shall be designed to facilitate timely recognition, location, replacement, repair and adjustment of malfunctioning equipment."

Analysis:

The safety I&C system is designed with monitoring features to detect both hardware and software faults and to assist in diagnostic and repair activities. Most failures will be detectable within each protection system including the processors, I/O modules and the communication features. The safety I&C system is designed for high reliability, extensive self-diagnostics (see Section 5.4 of Reference 12), minimal maintenance and simple on-line replacement of hardware. Maintenance and repair provisions will be described in the user's manual.

Identification of a defective input channel is accomplished by observation of system status indication or by testing. Replacement or repair of components is accomplished with the affected input channel bypassed.

The affected trip function then operates in a 2-out-of-3 trip logic while maintaining the coincidence of two required for trip or actuation.

For the 1-out-of-2 ESFAS (BOP portion), the affected trip function then operates in single active channel trip logic.

A.5.11 Identification

Clause 5.11:

"In order to provide assurance that the requirements given in this standard can be applied during the design, construction, maintenance, and operation of the plant, the following requirements shall be met:

(1) Safety system equipment shall be distinctly identified for each redundant portion of a safety system in accordance with the requirements of IEEE Std. 384-1981 and IEEE Std. 420-1982.

(2) Components for modules mounted in equipment or assemblies that are clearly identified as being in a single redundant portion of a safety system do not themselves require identification.

(3) Identification of safety system equipment shall be distinguishable from identifying markings placed on equipment for other purposes (for example, identification of fire protection equipment, phase identification of power cables).

(4) Identification of safety system equipment and its divisional assignment shall not require frequent use of reference material.

(5) The associated documentation shall be distinctly identified in accordance with the requirements of IEEE Std. 494-1974."

Analysis:

The safety I&C system meets the identification requirements of IEEE 384-1992, as endorsed by RG 1.75, Rev.3.

All equipment, including panels, modules, and cables associated with the RPS and ESF systems, are marked in order to facilitate identification. The safety I&C system is configured in accordance with specific identification requirements which provide a standardized method for identifying equipment, diagrams and signals for the purpose of consistency during the installation process. Interconnecting cabling is color-coded.

The physical identification is provided so that an operator can confirm if the safety I&C system cabinets and related cable are the safety class. The safety I&C system cabinets are distinguished by name plates. The safety I&C system components are uniquely identified by designations per project procedures and as defined in contract specifications. The physically isolated cable from sensor to actuation devices is identified by different colors between divisions.

The identification of software is assured by identification provisions as discussed in the SPM TeR.

A.5.12 Auxiliary Features

Clause 5.12:

"5.12.1 Auxiliary supporting features shall meet all requirements of this standard.

5.12.2 Other auxiliary features that (1) perform a function that is not required for the safety systems to accomplish their safety functions, and (2) are part of the safety systems by association (that is, not isolated from the safety system) shall be designed to meet those criteria necessary to ensure that these components, equipment, and systems do not degrade the safety systems below an acceptable level. Examples of these other auxiliary features are shown in Figure 3 and an illustration of the application of this criterion is contained in Appendix A."

Analysis:

Any features (components, equipment and systems) of the safety I&C system that perform safety functions satisfy the Clause 5.12 requirements of IEEE Std. 603-1991. All of these features are designated as safety-related and are part of the safety I&C system. The Communication architecture provides the ability to transmit information to non-safety related devices and is classified as safety-related until the non-safety boundary.

Auxiliary features (bypass, CWP signal, test, and calibration functions) are designed not to affect the protection system from accomplishing their safety functions.

The list of the auxiliary features is as follows:

Auxiliary Supporting Features

(1) Electric power supply system for the reactor protection system and engineered safety features systems

(2) I&C portions of the component cooling water system, essential service water system, and ultimate heat sink

(3) I&C portions of safety-related heating, ventilation, and air conditioning systems

<u>Other Auxiliary Features</u>

(1) Equipment protection devices (monitoring for door open and cabinet high temperature)

(2) Operating bypass, trip channel bypass

(3) Setpoint reset/change function

(4) Built-in test functions

(5) Diagnostic functions

(6) Trip, pre-trip, sequence of events, and status indications/alarms

(7) Qualified isolators to interface with non-safety systems

(8) Emergency diesel generator support systems

- Emergency diesel engine fuel oil system
- Emergency diesel engine cooling water system
- Emergency diesel engine starting air system
- Emergency diesel engine lubrication system
- Emergency diesel engine combustion air intake and exhaust system

A.5.13 Multi-Unit Stations

Clause 5.13:

“The sharing of structures, systems, and components between units at multi-unit generating stations is permissible provided that the ability to simultaneously perform required safety functions in all units is not impaired. Guidance on the sharing of electrical power systems between units is contained in IEEE Std. 308-1980. Guidance on the application of the single failure criterion to shared systems is contained in IEEE Std. 379-1988.”

<u>Analysis</u>:

This requirement is not applicable as there is no planned sharing between units.

A.5.14 Human Factors Considerations

Clause 5.14:

“Human factors shall be considered at the initial stages and throughout the design process to assure that the functions allocated in whole or in part to the human operator(s) and maintainer(s) can be successfully accomplished to meet the safety system design goals, in accordance with IEEE Std. 1023-1988.”

Analysis:

The safety I&C system is designed for the operator and maintenance personnel to accomplish their assigned functions successfully during the various plant conditions.

The HSI design for operator and maintenance personnel is designed in accordance with relevant parts of GDC 19 of 10 CFR 50 & 10 CFR 52. The safety I&C system interfaces with the operator follows the guidance set forth in NUREG-0700 and NUREG-0711. Verification and validation activities are performed under the conditions specified in the APR1400 HF Verification and Validation (V&V) Implementation Plan.

A.5.15 Reliability

Clause 5.15:

“For those systems for which either quantitative or qualitative reliability goals have been established, appropriate analysis of the design shall be performed in order to confirm that such goals have been achieved. IEEE Std. 352-1987 and IEEE Std. 577-1976 provide guidance for reliability analysis.”

Analysis:

The PPS and ESF-CCS reliability is described in Section 7.

The reliability of software is assured by implementing the design requirements of the SPM TeR.

Final determination of the RPS and ESFAS reliability requires an application specific reliability analysis and a system-level FMEA. This includes the plant specific test intervals and the final safety system design in order to make the final determination of achieving the reliability goal.

Both reliability and availability are calculated with the assumption that periodic testing will uncover faults that are not normally detected.

A.6 Sense and Command Features – Functional and Design Requirements

A.6.1 Automatic Control

Clause 6.1:

“Means shall be provided to automatically initiate and control all protective actions except as justified in 4.5. The safety system design shall be such that the operator is not required to take any action prior to the time and plant conditions specified in 4.5 following the onset of each design basis event. At the option of the safety system designer, means may be provided to automatically initiate and control those protective actions of 4.5.”

Analysis:

The PPS performs sense and command functions by automatically providing trip and actuation signals for use by the ESF-CCS which performs the execute functions.

The safety functions performed by the PPS are described in Section 4.2.

The design of the PPS and ESF-CCS includes the functions for the automatic control (bistable logic, local coincidence logic, and circuits) in each division to initiate the required protective actions. The operator does not need to perform any action while the automatic control function is active.

The RTSS circuit breaker is actuated when it receives the automatic reactor trip signals.

A.6.2 Manual Control

Clause 6.2:

“6.2.1 Means shall be provided in the control room to implement manual initiation at the division level of the automatically initiated protective actions. The means provided shall minimize the number of discrete operator manipulations and shall depend on the operation of a minimum of equipment consistent with the constraints of 5.6.1.

6.2.2 Means shall be provided in the control room to implement manual initiation and control of the protective actions identified in 4.5 that have not been selected for automatic control under 6.1.

The displays provided for these actions shall meet the requirements of 5.8.1.

6.2.3 Means shall be provided to implement the manual actions necessary to maintain safe conditions after the protective actions are completed as specified in 4.10. The information provided to the operators, the actions required of these operators, and the quantity and location of associated displays and controls shall be appropriate for the time period within which the actions shall be accomplished and the number of available qualified operators. Such displays and controls shall be located in areas that are accessible, located in an environment suitable for the operator, and suitably arranged for operator surveillance and action.”

Analysis:

Four manual reactor trip switches (per each division) are provided to permit the operator to trip the reactor. Single failure does not prevent the manual trip function from being performed properly.

Manual ESF system-level actuation switches are provided for each ESFAS function for SIAS, CIAS, MSIS, CSAS, AFAS, FHEVAS, CREVAS, and CPIAS. All ESF actuation signals can be manually initiated by these switches from the MCR operators in accordance with procedures.

Subsequent to initiation, each ESF system, including latched portions of AFAS, must be manually reset to restore the initiation logic to the non-actuated state. No single failure will prevent a manual actuation at the system-level.

MI switches and ESCM on the SC provide manual control means to maintain plant safe shutdown under transient and accident conditions. The MI indications and alarms are used to support the required operator actions under the accident conditions.

The manual control is not allowed administratively until the actuation setpoint of the PPS is reached. The manual control is carried out in accordance with EOP only when the manual control is required to mitigate the accident at the initiation of protective function.

The Class 1E control means are provided to perform manual actions necessary to maintain the safety condition after completing the protective action automatically by the PPS.

Design means are provided in the control room for manual initiation at the division/system-level automatically initiated protective actions. The manual ESF actuation switches are sent to the ESF-CCS. The manual reactor trip switches and DMA switches are provided downstream of the PPS and ESF-CCS.

The PPS does not affect the information provided to the operators, the actions by the operators, and the quantity of the associated displays and controls available to the operators. Safety-related controls and indicators are Class 1E; non safety related indicators are driven through qualified isolation devices.

Critical indications, such as those required for post-accident monitoring, are derived from raw instrument loop signals at the front end of the PPS, independent of any digital processing.

A.6.3 Interaction between the Sense and Command Features and Other Systems

Clause 6.3:

“6.3.1 Where a single credible event, including all direct and consequential results of that event, can cause a non-safety system action that results in a condition requiring protective action, and can concurrently prevent the protective action in those sense and command feature channels designated to provide principal protection against the condition, one of the following requirements shall be met:

(1) Alternate channels not subject to failure resulting from the same single event shall be provided to limit the consequences of this event to a value specified by the design basis. Alternate channels shall be selected from the following:

1. Channels that sense a set of variables different from the principal channels.

2. Channels that use equipment different from that of the principal channels to sense the same variable.

3. Channels that sense a set of variables different from those of the principal channels using equipment different from that of the principal channels.

4. Both the principal and alternate channels shall be part of the sense and command features.

(2) Equipment not subject to failure caused by the same single credible event shall be provided to detect the event and limit the consequences to a value specified by the design bases. Such equipment is considered a part of the safety system.

6.3.2 Provisions shall be included so that the requirements in 6.3.1 can be met in conjunction with the requirements of 6.7 if a channel is in maintenance bypass. These provisions include reducing the required coincidence, defeating the non-safety system signals taken from the redundant channels, or initiating a protective action from the bypassed channel.”

Analysis:

The Diversity and Defense-in-Depth TeR describes the capability to mitigate events in conjunction with a software CCF of the safety I&C system.

For events not associated with a software CCF, the PPS, CPCS, and ESF-CCS design minimizes the possibility of occurrence of events described in IEEE Std. 603, Clause 6.3.1. No portion of the PPS is used for both protective and control functions with the following exception: The CPCS's low DNBR, high LPD, and PPS’s high PZR pressure provide a CWP, which is treated as an associated circuit. As an associated circuit, it meets the requirements of IEEE Std. 603-1991.

The analog signal for use by the control system is not processed by the PPS and thus is not subject to software CCF. Signals from the PPS are isolated such that a failure will not affect the protective action of the PPS.

Analog signals to the SC are provided from the transmitter through the isolation devices and are not be processed by the PPS and thus not subject to software CCF.

A.6.4 Derivation of System Inputs

Clause 6.4:

“To the extent feasible and practical, sense and command feature inputs shall be derived from signals that are direct measures of the desired variables as specified in the design basis.”

Analysis:

The process variables and derived parameters used for the PPS actuation functions are set by the safety analysis. In so far as is practicable, system inputs are derived from signals that are direct measures of the desired variables. Variables that are measured directly include neutron flux, temperatures, and pressures. Level information is derived from appropriate differential pressure measurements. Flow information is derived from reactor coolant pump speed measurement, SG differential pressure, and reactor coolant temperature.

The plant parameters monitored are presented in report which provides signal descriptions for RPS and ESFAS.

A.6.5 Capability for Testing and Calibration

Clause 6.5:

“6.5.1 Means shall be provided for checking, with a high degree of confidence, the operational availability of each sense and command feature input sensor required for a safety function during reactor operation. This may be accomplished in various ways; for example:

(1) by perturbing the monitored variable,

(2) within the constraints of 6.6, by introducing and varying, as appropriate, a substitute input to the sensor of the same nature as the measured variable, or

(3) by cross-checking between channels that bear a known relationship to each other and that have readouts available.

6.5.2 One of the following means shall be provided for assuring the operational availability of each sense and command feature required during the post-accident period:

(1) Checking the operational availability of sensors by use of the methods described in 6.5.1.

(2) Specifying equipment that is stable and retains its calibration during the post-accident time period.”

Analysis:

The safety I&C system incorporates self-testing diagnostic features as well as range checking on all sensor inputs. A trouble alarm is generated upon detection of an input failure such as an out-of-range low or out-of-range high input condition.

The capability for testing or calibration in bypass or partial-trip mode at all power levels is provided with indication of bypass provided in the main control room in accordance with RG 1.47.

The PPS provides the capability for channel checks using the IPS provided in the main control room.

Accident monitoring capabilities are enhanced with the PPS.

Refer to item “A.5.7 Capability for Test and Calibration”.

A.6.6 Operating Bypasses

Clause 6.6:

“Whenever the applicable permissive conditions are not met, a safety system shall automatically prevent the activation of an operating bypass or initiate the appropriate safety function(s). If plant conditions change so that an activated operating bypass is no longer permissible, the safety system shall accomplish one of the following actions:

(1) Remove the appropriate active operating bypass(es).

(2) Restore plant conditions so that permissive conditions once again exist.

(3) Initiate the appropriate safety function(s).”

Analysis:

Where the APR1400 operating requirements necessitate manual bypass of a protective function, the PPS design is such that the bypass is initiated and removed automatically whenever permissive conditions for the bypass are not satisfied. Devices used to achieve automatic removal of the bypass of a protective function are considered part of the protective system and are designed accordingly. Indication is provided in the main control room if some part of the protection system has been administratively bypassed or taken out of service.

The operating bypasses are provided to permit orderly startup and shutdown of the plant and to allow low power testing. If a protection channel has been bypassed, a signal is provided to allow this condition to be continuously indicated in the MCR. The operating bypasses are automatically removed when plant conditions require their removal and automatically restored when plant conditions require their restoration.

The operating bypasses have automatic features that provide a permissive range at which they can be actuated. The ability to initiate appropriate safety functions is available at all times.

A.6.7 Maintenance Bypass

Clause 6.7:

“Capability of a safety system to accomplish its safety function shall be retained while sense and command features equipment is in maintenance bypass. During such operation, the sense and command features shall continue to meet the requirements of 5.1 and 6.3.

EXCEPTION: One-out-of-two portions of the sense and command features are not required to meet 5.1 and 6.3 when one portion is rendered inoperable, provided that acceptable reliability of equipment operation is otherwise demonstrated that is, that the period allowed for removal from service for maintenance bypass is sufficiently short to have no significantly detrimental effect on overall sense and command features availability).”

Analysis:

The bypasses are always set manually as there are no automatic bypass provisions for maintenance bypasses for the PPS.

The bypass of the PPS parameters results in 2-out-of-3 coincidence logic. The bypass of the BOP ESFAS changes 1-out-of-2 logic to 1-out-of-1 logic.

The BISI in the MCR are designed to meet the RG 1.47. The PPS channel can be placed in Manual Bypass mode to facilitate maintenance activities. Indication is provided in the main control room whenever a PPS channel has been administratively bypassed for maintenance or taken out of service.

The PPS is designed to permit an inoperable channel to be placed in a bypass condition for the purpose of troubleshooting or periodic test of a redundant channel. If the PPS channel has been bypassed for any purpose, a signal is provided to allow this condition to be continuously indicated in the MCR. During such operation, the PPS continues to satisfy the SFC.

The FMEA for the PPS assumes that one of the initial conditions is a PPS channel is placed in the Bypass Mode. This initial condition imposed on the FMEA determines the overall effect of an evaluated failure on the safety system’s capability to perform the required safety functions in this non-conservative mode.

The PPS supports maintenance activities, such as periodic maintenance, instrument loop testing, troubleshooting, etc. Access to features beyond displaying data such as the maintenance bypass would be under strict administrative and physical controls. These activities would be performed in accordance with site-specific administrative (procedural) and physical-access controls to set and/or change addressable constants, setpoints, and testing while the channel is in bypass mode. Such procedures would require manipulation of the FE keyswitch.

RPS and ESFAS parameters can be bypassed for maintenance. When one channel is in bypass, the coincidence logic in the LCL reverts to 2-out-of-3. The administrative procedure prohibits more than one channel from being placed in bypass.

The protection functions of the RPS and ESFAS are maintained while the system is bypassed.

A.6.8 Setpoints

Clause 6.8:

“6.8.1 The allowance for uncertainties between the process analytical limit documented in Clause 4, item d) and the device setpoint shall be determined using a documented methodology. Refer to ANSI/ISA S67.04-1994.

6.8.2 Where it is necessary to provide multiple setpoints for adequate protection for a particular mode of operation or set of operating conditions, the design shall provide positive means of ensuring that the more restrictive setpoint is used when required. The devices used to prevent improper use of less restrictive setpoints shall be part of the sense and command features.”

Analysis:

The safety I&C system conforms to ISA-S67.04-1994 as described in the Setpoint Methodology for PPS TeR.

The environment considered when determining errors is the most detrimental realistic environment calculated or postulated to exist until the worst case time of the required RPS or ESFAS. This environment may be different for different events analyzed. For the setpoint calculation, the accident environment error calculation for process equipment uses the environmental conditions up to the longest required time of trip or actuation that results in the largest errors, thus providing additional conservatism to the resulting setpoints.

The reference leg heating component uncertainties for SG level also take into account pressure and temperature variation within the SG.

For all temperature and pressure setpoints, the trip will be initiated at a point that is not at saturation for the equipment. For level setpoints, no analysis setpoint is within 5% of the ends of the level span.

When the pressure (or temperature) reaches to saturation condition, the pressure (or temperature) is not increased by temperature (or pressure). The temperature (or pressure) could not be used for trip parameter in this range. Therefore, the trip shall be initiated before saturation condition.

Analysis setpoint for high level is determined to be less than 95% and analysis setpoint for low level to be more than 5%. This is to protect the equipment considering delay time.

Manual reduction of the setpoints for low pressurizer pressure and low SG pressure trips is used for the controlled reduction of pressurizer pressure and SG pressure. The setpoint reductions are initiated by the MCR SC two pushbutton switches for each division, one pushbutton switch for the pressurizer pressure and one pushbutton switch for both SG pressures within the division. This method of setpoint reduction provides positive assurance that the setpoint is never decreased below the existing pressure by more than a predetermined amount.

The variable overpower trip setpoint tracks the actual reactor power from a minimum value to a high value or vice versa, if the power changes slowly enough. The variable overpower trip setpoint is designed with a maximum rate of decrease or increase. If the actual power increases at too rapid rate, it will catch up with the more slowly increasing setpoint and cause a trip.

The low reactor coolant flow trip setpoint automatically tracks below the input variables by a fixed margin for all decreasing inputs with a rate less than the rate limit. The setpoint decreases at a fixed rate for all decreasing input variable changes greater than the rate limit. If the input variable decreases at too rapid rate, it will catch up with the more slowly decreasing setpoint and cause a trip. The setpoint automatically increases as the input variable increases.

Refer to the Setpoint Methodology for Plant Protection System TeR for detailed setpoint methodology.

A.7 Execute Features - Functional and Design Requirements

A.7.1 Automatic Control

Clause 7.1:

“Capability shall be incorporated in the execute features to receive and act upon automatic control signals from the sense and command features consistent with 4.4 of the design basis.”

Analysis:

The RTSG is operated automatically by automatic reactor trip signal.

The ESF components are activated automatically by the ESF-CCS.

A.7.2 Manual Control

Clause 7.2:

“If manual control of any actuated component in the execute features is provided, the additional design features in the execute features necessary to accomplish such manual control shall not defeat the requirements of 5.1 and 6.2. Capability shall be provided in the execute features to receive and act upon manual control signals from the sense and command features consistent with the design basis.”

Analysis:

There is manual reactor trip switch in the RTSG. The single failure of a manual reactor trip switch in the RTSG does not prevent manual shutdown function of the PPS.

The RTSG is operated by manual reactor trip switch in the MCR SC or RSR console or pushbutton switch on the RTSG cabinet.

The ESFAS is actuated by the actuation signals of the manual ESF system-level actuation switches on the MCR SC or MI switches. The ESCMs are provided for component controls on the MCR and RSR consoles.

A.7.3 Completion of Protective Action

Clause 7.3:

“The design of the execute features shall be such that once initiated, the protective actions of the execute features shall go to completion. This requirement shall not preclude the use of equipment protective devices identified in 4.11 of the design basis or the provision for deliberate operator interventions. When the sense and command features reset, the execute features shall not automatically return to normal; they shall require separate, deliberate operator action to be returned to normal. After the initial protective action has gone to completion, the execute features may require manual control or automatic control (that is, cycling) of specific equipment to maintain completion of the safety function.”

Analysis:

The PPS and ESF-CCS are designed to complete the protective action (reactor trip or ESFAS initiation) once it is initiated. An operator's action is required to reset the trip conditions and TCBs in RTSS before returning to the normal operation condition. Also ESFAS initiation signals are latched (except the valve portion of AFAS logic) and require manual reset.

A.7.4 Operating Bypass

Clause 7.4:

“Whenever the applicable conditions are not met, a safety system shall automatically prevent the activation of an operating bypass or initiate the appropriate safety function(s). If plant conditions change so that an activated operating bypass is no longer permissible, the safety system shall automatically accomplish one of the following actions:

(1) Remove the appropriate active operating bypass(es).

(2) Restore plant conditions so that permissive conditions once again exist.

(3) Initiate the appropriate safety function(s).”

Analysis:

The operating bypasses are provided to permit orderly startup and shutdown of the plant and to allow low power testing.

The operating bypasses have automatic features that provide a permissive range at which they can be actuated. Should the permissive range be exceeded, the bypass is automatically removed.

A.7.5 Maintenance Bypass

Clause 7.5:

"The capability of a safety system to accomplish its safety function shall be retained while execute features equipment is in maintenance bypass. Portions of the execute features with a degree of redundancy of one shall be designed such that when a portion is placed in maintenance bypass (that is, reducing temporarily its degree of redundancy to zero), the remaining portions provide acceptable reliability."

Analysis:

One set of the redundant PPS bistable trip channels is bypassed for maintenance.

The protection functions of the RPS and ESFAS are maintained while the system is bypassed.

A.8 Power Source Requirements

A.8.1 Electrical Power Sources

Clause 8.1:

"Those portions of the Class 1E power system that are required to provide the power to the many facets of the safety system are governed by the criteria of this document and are a portion of the safety systems. Specific criteria unique to the Class 1E power systems are given in IEEE Std. 308-1980."

Analysis:

The safety I&C system division receives non-interrupt AC power from VBPSS. The PPS power is provided with single phase 120 Vac from four independent A, B, C, and D division inverters. The ESF-CCS receives the single phase 120 Vac from four independent A, B, C, and D division inverters and 120 Vac from MCC alternate sources.

A.8.2 Non-electrical Power Sources

Clause 8.2:

"Non-electrical power sources, such as control-air systems, bottled-gas systems, and hydraulic systems, required to provide the power to the safety systems are a portion of the safety systems and shall provide power consistent with the requirements of this standard. Specific criteria unique to non-electrical power sources are outside the scope of this standard and can be found in other standards."

Analysis:

The safety I&C system does not rely on non-electrical power sources for performance of its safety related functions. Further, the safety I&C system does not impact any non-electrical power source used by any other safety system.

A.8.3 Maintenance Bypass

Clause 8.3:

“The capability of the safety systems to accomplish their safety functions shall be retained while power sources are in maintenance bypass. Portions of the power sources with a degree of redundancy of one shall be designed such that when a portion is placed in maintenance bypass (that is, reducing temporarily its degree of redundancy to zero), the remaining portions provide acceptable reliability.”

Analysis:

The safety I&C system power supplies are operational in all modes as required.

APPENDIX B CONFORMANCE TO IEEE STD. 7-4.3.2-2003

This Appendix describes how the safety I&C system satisfies the requirements of IEEE Std. 7-4.3.2-2003 endorsed by RG 1.152. The following heading numbers with “B” correspond to the clause numbers of IEEE Std. 7-4.3.2-2003.

B.1 Scope

The computer based safety system criteria contained in IEEE Std. 7-4.3.2 are applicable to the safety I&C system, which initiate safety actions to mitigate the consequences of DBE. It is also applicable to those parts of data communication systems that support safety system functions. The detailed software conformances are described in the SPM TeR.

B.2 References

The safety I&C system complies with those referenced codes and standards that have either been endorsed by the NRC in a Regulatory Guide or are incorporated by reference in the Code of Federal Regulations.

B.3 Definitions and Abbreviations

There is no exception in the safety I&C system designs.

B.4 Safety System Design Basis

Clause 4:

“No requirements beyond IEEE Std. 603-1998 are necessary.”

B.5 Safety System Criteria

B.5.1 Single-Failure Criterion

Clause 5.1:

“No requirements beyond IEEE Std. 603-1998 are necessary.”

B.5.2 Completion of Protective Action

Clause 5.2:

“No requirements beyond IEEE Std. 603-1998 are necessary.”

B.5.3 Quality

B.5.3.1 Software Development

Clause 5.3.1:

“Computer software shall be developed, modified, or accepted in accordance with an approved software quality assurance (QA) plan consistent with the requirements of IEEE/EIA 12207.0-1996. The software QA plan shall address all software that is resident on the computer at run time (i.e., application software, network software, interfaces, operating systems, and diagnostics). Guidance for developing software QA plans can be found in IEC 60880 (1986-09) and IEEE Std.730-1998."

Analysis:

The software development life cycle for the safety I&C system application software is described in the SPM TeR.

B.5.3.1.1 Software Quality Metrics

Clause 5.3.1.1:

"The use of software quality metrics shall be considered throughout the software life cycle to assess whether software quality requirements are being met. When software quality metrics are used, the following life cycle phase characteristics should be considered:

- Correctness/Completeness (Requirements phase)
- Compliance with requirements (Design phase)
- Compliance with design (Implementation phase)
- Functional compliance with requirements (Test and Integration phase)
- On-site functional compliance with requirements (Installation and Checkout phase)
- Performance history (Operation and Maintenance phase)

The basis for the metrics selected to evaluate software quality characteristics should be included in the software development documentation. IEEE Std.1061-1998 provides a methodology for the application of software quality metrics."

Analysis:

Software quality is assured through the application of a rigorous software life cycle process. The process covers software development (or qualification of commercial off-the-shelf software), verification review and validation testing at the different stages of development, and software configuration management during all phases of software development.

Throughout the software life cycle, a requirements traceability matrix (RTM) is maintained and requirements traceability analyses are performed for each software system. The author of each software document to be used for the requirements traceability analyses is responsible for providing trace information from each item in the document to the items in the upstream document. The V&V team is responsible for analyzing the trace information provided. The V&V team reviews the trace information for the adequacy and accuracy.

B.5.3.2 Software Tools

Clause 5.3.2:

"Software tools used to support software development processes and verification and validation (V&V) processes shall be controlled under configuration management.

One or both of the following methods shall be used to confirm the software tools are suitable for use:

a) A test tool validation program shall be developed to provide confidence that the necessary features of the software tool function as required.

b) The software tool shall be used in a manner such that defects not detected by the software tool will be detected by V&V activities.

Tool operating experience may be used to provide additional confidence in the suitability of a tool, particularly when evaluating the potential for undetected defects.”

Analysis:

The software development tools (e.g., application programming tool, requirements management tool, compiler, linker, etc) are placed under the configuration management program. Tools are qualified with a degree of rigor and level of detail appropriate to the safety significance of the software which is to be developed using the tools.

The defects induced by any software tool used are detected and removed through the comprehensive V&V and testing process described in the SPM TeR.

B.5.3.3 Verification and Validation

Clause 5.3.3:

“V&V is an extension of the program management and systems engineering team activities. V&V is used to identify objective data and conclusions (i.e., proactive feedback) about digital system quality, performance, and development process compliance throughout the system life cycle. Feedback consists of anomaly reports, performance improvements, and quality improvements regarding the expected operating conditions across the full spectrum of the system and its interfaces.

V&V processes are used to determine whether the development products of an activity conform to the requirements of that activity, and whether the system performs according to its intended use and user needs.

This determination of suitability includes assessment, analysis, e valuation, review, inspection, and testing of products and processes.

This standard adopts the IEEE Std.1012-1998 terminology of process, activity and task, in which software V&V processes are subdivided into activities, which are further subdivided into tasks. The term V&V effort is used to reference this framework of V&V processes, activities, and tasks.

V&V processes shall address the computer hardware and software, integration of the digital system components, and the interaction of the resulting computer system with the nuclear power plant.

The V&V activities and tasks shall include system testing of the final integrated hardware, software, firmware, and interfaces.

The software V&V effort shall be performed in accordance with IEEE Std.1012-1998. The IEEE Std.1012-1998 V&V requirements for the highest integrity level (level 4) apply to systems developed using this standard (i.e., IEEE Std.7-4.3.2™). See IEEE Std.1012-1998 Annex B for a definition of integrity level 4 software.”

Analysis:

The verification and validation for the safety I&C system application software is described in the SPM TeR.

B.5.3.4 Independent V&V Requirements

Clause 5.3.4:

“The previous section addresses the V&V activities to be performed. This section defines the levels of independence required for the V&V effort. IV&V activities are defined by three parameters: technical independence, managerial independence, and financial independence. These parameters are described in Annex C of IEEE Std.1012-1998.

The development activities and tests shall be verified and validated by individuals or groups with appropriate technical competence, other than those who developed the original design.

Oversight of the IV&V effort shall be vested in an organization separate from the development and program management organizations. The V&V effort shall independently select

a) The segments of the software and system to be analyzed and tested,

b) The V&V techniques, and

c) The technical issues and problems upon which to act.

The V&V effort shall be allocated resources that are independent of the development resources. See Annex C of IEEE Std.1012-1998 for additional guidance.”

<u>Analysis:</u>

Independence of verification and validation for the safety I&C system is described in the SPM TeR.

B.5.3.5 Software Configuration Management

Clause 5.3.5:

“Software configuration management shall be performed in accordance with IEEE Std.828™-1998 which provides guidance for the development of software configuration management plans.

The minimum set of activities shall address the following:

a) Identification and control of all software designs and code

b) Identification and control of all software design functional data (e.g., data templates and data bases)

c) Identification and control of all software design interfaces

d) Control of all software design changes

e) Control of software documentation (user, operating, and maintenance documentation)

f) Control of software vendor development activities for the supplied safety system software

g) Control and retrieval of qualification information associated with software designs and code

h) Software configuration audits

i) Status accounting

Some of these functions or documents may be performed or controlled by other QA activities. In this case, the software configuration management plan shall describe the division of responsibility.

A software baseline shall be established at appropriate points in the software life cycle process to synchronize engineering and documentation activities. Approved changes that are created subsequent to a baseline shall be added to the baseline.

The labeling of the software for configuration control shall include unique identification of each configuration item, and revision and/or date time stamps for each configuration item.

Changes to the software/firmware shall be formally documented and approved consistent with the software configuration management plan. The documentation shall include the reason for the change, identification of the affected software/firmware, and the impact of the change on the system. Additionally, the documentation should include the plan for implementing the change in the system (e.g., immediately implementing the change, or scheduling the change for a future version)."

Analysis:

The software configuration management for the safety I&C system is described in the SPM TeR.

B.5.3.6 Software Project Risk Management

Clause 5.3.6:

"Software project risk management is a tool for problem prevention: identifying potential problems, assessing their impact, and determining which potential problems must be addressed to assure that software quality goals are achieved. Risk management shall be performed at all levels of the digital system project to provide adequate coverage for each potential problem area. Software project risks may include technical, schedule, or resource-related risks that could compromise software quality goals, and thereby affect the ability of the safety computer system to perform safety related functions. Software project risk management differs from hazard analysis, as defined in 3.1.31, in that hazard analysis is focused solely on the technical aspects of system failure mechanisms.

Risk management shall include the following steps:

a) Determine the scope of risk management to be performed for the digital system.

b) Define and implement appropriate risk management strategies.

c) Identify risks to the software project in the project risk management strategy and as they develop during the conduct of the project.

d) Analyze risks to determine the priority for their mitigation.

e) Develop risk mitigation plans for risks that have the potential to significantly impact software quality goals, with appropriate metrics for tracking resolution progress. (These risks may include technical, schedule, or resource-related project risks that could compromise the ability of the safety computer system to perform safety related functions.)

f) Take corrective actions when expected quality is not achieved.

g) Establish a project environment that supports effective communications between individuals and groups for the resolution of software project risks.

Additional guidance on the topic of risk management is provided in IEEE/EIA 12207.0-1996, and IEEE Std.1540™-2001.”

Analysis:

The software management plan in the SPM TeR describes the software project risk management.

B.5.4 Equipment Qualification

B.5.4.1 Computer System Testing

Clause 5.4.1:

“Computer system qualification testing (see 3.1.36) shall be performed with the computer functioning with software and diagnostics that are representative of those used in actual operation. All portions of the computer necessary to accomplish safety functions, or those portions whose operation or failure could impair safety functions, shall be exercised during testing. This includes, as appropriate, exercising and monitoring the memory, the CPU, inputs and outputs, display functions, diagnostics, associated components, communication paths, and interfaces. Testing shall demonstrate that the performance requirements related to safety functions have been met.”

Analysis:

The computer-based system testing process for the safety I&C system is described in the SPM TeR.

B.5.4.2 Qualification of Existing Commercial Computers

Clause 5.4.2:

“The qualification process shall be accomplished by evaluating the hardware and software design using the criteria of this standard. Acceptance shall be based upon evidence that the digital system or component, including hardware, software, firmware, and interfaces, can perform its required functions. The acceptance and its basis shall be documented and maintained with the qualification documentation.

In those cases in which traditional qualification processes cannot be applied, an alternative approach to verify a component is acceptable for use in a safety-related application is commercial grade dedication. The objective of commercial grade dedication is to verify that the item being dedicated is equivalent in quality to equipment developed under a 10 CFR 50 Appendix B program.

The dedication process for the computer shall entail identification of the physical, performance, and development process requirements necessary to provide adequate confidence that the proposed digital system or component can achieve the safety function. The dedication process shall apply to the computer hardware, software, and firmware that are required to accomplish the safety function. The dedication process for software and firmware shall, whenever possible, include an evaluation of the design process. There may be some instances in which a design process cannot be evaluated as part of the dedication process. For example, the organization performing the evaluation may not have access to the design process information for a microprocessor chip to be used in the safety system. In this case, it would not be possible to perform an evaluation to support the dedication. Because the dedication process involves all aspects of life cycle processes and manufacturing quality, commercial grade item dedication should be limited to items that are relatively simple in function relative to their intended use.

Commercial grade item dedication involves preliminary phase and detailed phase activities. These phase activities are described in 5.4.2.1 through 5.4.2.2."

Analysis:

The qualification for the safety I&C system is described in Section 6 and in Reference 12.

B.5.5 System Integrity

B.5.5.1 Design for Computer Integrity

Clause 5.5.1:

"The computer shall be designed to perform its safety function when subjected to conditions, external or internal, that have significant potential for defeating the safety function. For example, input and output processing failures, precision or roundoff problems, improper recovery actions, electrical input voltage and frequency fluctuations, and maximum credible number of coincident signal changes.

If the system requirements identify a safety system preferred failure mode, failures of the computer shall not preclude the safety system from being placed in that mode. Performance of computer system restart operations shall not result in the safety system being inhibited from performing its function."

Analysis:

The safety I&C system including the software is designed for fail-safe operation under component failure including processor failures or loss of electrical power.

The safety I&C system software integrity is assured by software development process and activities described in the SPM TeR.

B.5.5.2 Design for Test and Calibration

Clause 5.5.2:

"Test and calibration functions shall not adversely affect the ability of the computer to perform its safety function. Appropriate bypass of one redundant channel is not considered an adverse effect in this context. It shall be verified that the test and calibration functions do not affect computer functions that are not included in a calibration change (e.g., setpoint change).

V&V, configuration management, and QA shall be required for test and calibration functions on separate computers (e.g., test and calibration computer) that provide the sole verification of test and calibration data. V&V, configuration management, and QA shall be required when the test and calibration function is inherent to the computer that is part of the safety system.

V&V, configuration management, and QA are not required when the test and calibration function is resident on a separate computer and does not provide the sole verification of test and calibration data for the computer that is part of the safety system."

Analysis:

All processor stations have self-diagnostics that continuously monitor the hardware modules and software functions. This diagnostic information is sent to the ITP/MTP FPD for display and alarm processing. The IPS monitors the process values and setpoint values received from for all division ITPs. These features do not interfere with normal system operation.

Channels are maintained and calibrated in a bypassed condition without initiating a protective action at the system-level. Lifting electrical leads or installing jumpers need not be done to accomplish this process. Periodic testing is permitted during power operation.

B.5.5.3 Fault Detection and Self-Diagnostics

Clause 5.5.3:

“Computer systems can experience partial failures that can degrade the capabilities of the computer system, but may not be immediately detectable by the system. Self-diagnostics are one means that can be used to assist in detecting these failures. Fault detection and self-diagnostics requirements are addressed in this subclause.

The reliability requirements of the safety system shall be used to establish the need for self-diagnostics. Self-diagnostics are not required for systems in which failures can be detected by alternate means in a timely manner. If self-diagnostics are incorporated into the system requirements, these functions shall be subject to the same V&V processes as the safety system functions.

If reliability requirements warrant self-diagnostics, then computer programs shall incorporate functions to detect and report computer system faults and failures in a timely manner. Conversely, self-diagnostic functions shall not adversely affect the ability of the computer system to perform its safety function, or cause spurious actuations of the safety function. A typical set of self-diagnostic functions includes the following:

- Memory functionality and integrity tests (e.g., PROM checksum and RAM tests)
- Computer system instruction set (e.g., calculation tests)
- Computer peripheral hardware tests (e.g., watchdog timers and keyboards)
- Computer architecture support hardware (e.g., address lines and shared memory interfaces)
- Communication link diagnostics (e.g., CRC checks)

Infrequent communication link failures that do not result in a system failure or a lack of system functionality do not require reporting.

When self-diagnostics are applied, the following self-diagnostic features shall be incorporated into the system design:

a) Self-diagnostics during computer system startup

b) Periodic self-diagnostics while the computer system is operating

c) Self-diagnostic test failure reporting”

Analysis:

Upon power-up, diagnostics are performed on the digital equipment including processors, I/O and memory to confirm readiness of the safety I&C system. A complete set of these diagnostics are executed during initialization. This will detect any fatal errors prior to execution of the process loop. (See Section 5.4 of Reference 12)

During initialization, the watchdog function remains in the actuated state. Upon completion of the initialization tests, the processors will start automatically and run. Upon entry to the run mode, the watchdog function will automatically reset to the non-actuated state. Processor operability is continuously tested in the run mode and the watchdog function is actuated upon detection of failure. The detailed information for the diagnostic function is provided in Reference 12.

B.5.6 Independence

Clause 5.6:

“In addition to the requirements of IEEE Std.603-1998, data communication between safety channels or between safety and non-safety systems shall not inhibit the performance of the safety function.

IEEE Std.603-1998 requires that safety functions be separated from non-safety functions such that the non-safety functions cannot prevent the safety system from performing its intended functions. In digital systems, safety and non-safety software may reside on the same computer and use the same computer resources.

Either of the following approaches is acceptable to address the previous issues:

a) Barrier requirements shall be identified to provide adequate confidence that the nonsafety functions cannot interfere with performance of the safety functions of the software or firmware. The barriers shall be designed in accordance with the requirements of this standard. The nonsafety software is not required to meet these requirements.

b) If barriers between the safety software and nonsafety software are not implemented, the nonsafety software functions shall be developed in accordance with the requirements of this standard.

Guidance for establishing communication independence is provided in Annex E.”

Analysis:

The methods used to ensure communication independence between different safety divisions and safety and non-safety systems is described in Section 4.6 of this report. The methods include:

a. Electrical isolation

Fiber optic cables are used for electrical isolation between computers in different safety divisions or safety and non-safety computers. The fiber optic cables provide inherent isolation for electrical faults since it does not carry the electrical current.

b. Communication independence

The communication independence conformance is described in Appendix C.

c. Physical separation

Physical separation is achieved by physical barriers or acceptable separation distance. The separation of Class 1E equipment is designed in accordance with the requirements of IEEE Std. 384-1992. The separation between safety and non-safety equipment meets IEEE Std. 384 and RG 1.75.

B.5.7 Capability for Test and Calibration

Clause 5.7:

“No requirements beyond IEEE Std. 603-1998 are necessary.”

B.5.8 Information Displays

Clause 5.8:

“No requirements beyond IEEE Std. 603-1998 are necessary.”

B.5.9 Control of Access

Clause 5.9:

“No requirements beyond IEEE Std. 603-1998 are necessary.”

B.5.10 Repair

Clause 5.10:

“No requirements beyond IEEE Std. 603-1998 are necessary.”

B.5.11 Identification

Clause 5.11:

“To provide assurance that the required computer system hardware and software are installed in the appropriate system configuration, the following identification requirements specific to software systems shall be met:

a) Firmware and software identification shall be used to assure the correct software is installed in the correct hardware component.

b) Means shall be included in the software such that the identification may be retrieved from the firmware using software maintenance tools.

c) Physical identification requirements of the digital computer system hardware shall be in accordance with the identification requirements in IEEE Std.603-1998.”

Analysis:

All software and documentation is uniquely identified by a system name, number, and corresponding revision date, appropriate category and software classification as described in the SPM TeR.

The configuration Items referenced and controlled by the Software Configuration Management Plan are as follows:

- Operating System including Compiler and Linker
- Run time source and executable files

- Associated Software Documents

B.5.12 Auxiliary Features

Clause 5.12:

“No requirements beyond IEEE Std. 603-1998 are necessary.”

B.5.13 Multi-Unit Stations

Clause 5.13:

“No requirements beyond IEEE Std. 603-1998 are necessary.”

B.5.14 Human Factor Considerations

Clause 5.14:

“No requirements beyond IEEE Std. 603-1998 are necessary.”

B.5.15 Reliability

Clause 5.15:

“In addition to the requirements of IEEE Std. 603-1998, when reliability goals are identified, the proof of meeting the goals shall include the software. The method for determining reliability may include combinations of analysis, field experience, or testing. Software error recording and trending may be used in combination with analysis, field experience, or testing.”

Analysis:

The reliability analysis method for the safety I&C system is described in Section 7.

B.6 Sense and Command Features – Functional and Design Requirements

Clause 6:

“No requirements beyond IEEE Std. 603-1998 are necessary.”

B.7 Execute Features – Functional and Design Requirements

Clause 7:

“No requirements beyond IEEE Std. 603-1998 are necessary.”

B.8 Power Source Requirements

Clause 8:

“No requirements beyond IEEE Std. 603-1998 are necessary.”

APPENDIX C CONFORMANCE TO DI&C-ISG-04

This Appendix describes how data communication systems satisfy the requirements of DI&C-ISG-04, “Task Working Group #4: Highly-Integrated Control Rooms-Communications Issues (HICRc) Interim Staff Guidance”.

C.1 Scope

DI&C-ISG-04 addresses 3 positions: Section 1. Interdivisional communications, Section 2. Command prioritization, and Section 3. Multidivisional control and display stations.

The scope of this Appendix is to demonstrate the compliances of the safety I&C system with regard to DI&C-ISG-04 Section 1, Section 2, and Section 3.

C.2 Reference

The data communication systems of the APR 1400 comply with the guidance of DI&C-ISG-04, “Task Working Group #4: Highly-Integrated Control Rooms-Communications Issues Interim Staff Guidance”, Rev.1, March 2009.

C.3 Data Communication Systems

TS

TS

.

TS

Figure C.3-1 Data Communication System

C.4 System Descriptions

TS

.

TS

.

C.5 Compliance Analysis to Criteria

TS

TS

.

.

TS

TS

“

TS

TS

.

TS

.

TS

TS

TS

“

TS

.

TS

TS

”.

TS

TS

TS

.

Table C.5.1-1 RSPT1 and RSPT2 Channel Assignment

TS

TS

TS

TS

“

TS

TS

TS

TS

TS

Table C.5.1-2 Software Comparison between the Palo Verde and APR1400 CPCS

.

TS

Table C.5.1-3 CPCS Design Conformance to CPU Load Restrictions

TS

TS

TS

TS

TS

TS

TS

TS

TS

TS

TS

TS

.

TS

Table C.5.1-4 Operating Step When the IFPD to ESCM Interface Exists

TS

Table C.5.1-5 Operating Step When the IFPD to ESCM Interface Does Not Exist (1/2)

TS

Table C.5.1-5 Operating Step When the IFPD to ESCM Interface Does Not Exist (2/2)

TS

Figure C.5-1 Operating Step When the IFPD to ESCM Interface Exists (1/6)

TS

Figure C.5-1 Operating Step When the IFPD to ESCM Interface Exists (2/6)

TS

Figure C.5-1 Operating Step When the IFPD to ESCM Interface Exists (3/6)

TS

Figure C.5-1 Operating Step When the IFPD to ESCM Interface Exists (4/6)

TS

Figure C.5-1 Operating Step When the IFPD to ESCM Interface Exists (5/6)

TS

Figure C.5-1 Operating Step When the IFPD to ESCM Interface Exists (6/6)

TS

Figure C.5-2 Operating Step When the IFPD to ESCM Interface Exists (1/10)

TS

Figure C.5-2 Operating Step When the IFPD to ESCM Interface Exists (2/10)

TS

Figure C.5-2 Operating Step When the IFPD to ESCM Interface Exists (3/10)

TS

Figure C.5-2 Operating Step When the IFPD to ESCM Interface Exists (4/10)

TS

Figure C.5-2 Operating Step When the IFPD to ESCM Interface Exists (5/10)

TS

Figure C.5-2 Operating Step When the IFPD to ESCM Interface Exists (6/10)

TS

Figure C.5-2 Operating Step When the IFPD to ESCM Interface Exists (7/10)

TS

Figure C.5-2 Operating Step When the IFPD to ESCM Interface Exists (8/10)

TS

Figure C.5-2 Operating Step When the IFPD to ESCM Interface Exists (9/10)

TS

Figure C.5-2 Operating Step When the IFPD to ESCM Interface Exists (10/10)

TS

TS

TS

.

TS

.

Figure C.5-3 ESCM Interface Diagram

TS

TS

:

TS

TS

.

TS

TS

TS

TS

TS

TS

TS

.

TS

TS

TS

TS

TS

TS

TS

TS

TS

TS

TS

TS

TS

Figure C.5-4 Control Procedure on System Directory Page of ESCM

TS

TS

TS

TS

Figure C.5-5 Operating Procedure for the Soft Control using the IFPD and ESCM

TS

TS

TS

TS

TS

TS

APPENDIX D ALTERNATIVE TO INDEPENDENCE REQUIREMENTS OF IEEE STD. 603-1991

D.1 Systems/Components Affected

TS

.

D.2 Applicable Code Requirement

TS

.

D.3 Reason for Alternative Request

TS

D.4 Proposed Alternative and Basis for Use

TS

.

D.5 Summary

TS

TS

.

APPENDIX E SAFETY COMPONENTS CONTROLLED BY ESCM

E.1 List of Components Controlled by ESCM

TS

Table E.1-1 Safety Components Controlled by ESCM (1 of 6)

TS

Table E.1-1 Safety Components Controlled by ESCM (2 of 6)

TS

Table E.1-1 Safety Components Controlled by ESCM (3 of 6)

TS

Table E.1-1 Safety Components Controlled by ESCM (4 of 6)

TS

Table E.1-1 Safety Components Controlled by ESCM (5 of 6)

TS

Table E.1-1 Safety Components Controlled by ESCM (6 of 6)

TS

Acronyms and Abbreviations for Table E.1-1

AAC	alternate alternating current
ACU	air cleaning unit
AF	auxiliary feedwater
AHU	air handling unit
BAST	boric acid storage tank
CBO	controlled bleedoff
CCW	component cooling water
CS	containment spray
ESW	essential service water
HVAC	heating, ventilation, and airconditioning
HVT	holdup volume tank
IRWST	in-containment refueling water storage tank
LC	load center
MSADV	main steam atmospheric dump valve
MSIV	main steam isolation valve
PCB	power circuit breaker
POSRV	pilot-operated safety relief valve
RCP	reactor coolant pump
RSSH	resin sluice supply header
SAT	standby auxiliary transformer
SC	shutdown cooling
SCS	shutdown cooling system
SFP	spent fuel pool
SG	steam generator
SI	safety injection
SWGR	switchgear
UAT	unit auxiliary transformer
UHS	ultimate heat sink
VCT	volume control tank
XFMR	transformer