REVISED RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

APR1400 Design Certification

Korea Electric Power Corporation / Korea Hydro & Nuclear Power Co., LTD

Docket No. 52-046

RAI No.:	**45-7883**
SRP Section:	**07.09 – Data Communication System**
Application Section:	**07.09**
Date of RAI Issue:	**06/23/2015**

Question No. 07.09-2

List all safety system to safety system interfaces and their connection types and all safety system to non-safety system interfaces and their connection types.

10 CFR 50.55a(h) requires compliance to IEEE Std. 603-1991. IEEE Std. 603-1991, Clause 5.6.1, states, in part, “Redundant portions of a safety system provided for a safety function shall be independent of and physically separated from each other to the degree necessary to retain the capability to accomplish the safety function during and following any design basis event requiring that safety function,” and Clause 5.6.3, states, in part, “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.” RG 1.75 provides guidance on the physical separation requirements of IEEE Std. 603-1991, Clause 5.6. BTP 7-11 provides guidance on application and qualification of isolation devices to meet the electrical isolation requirements of IEEE Std. 603-1991 Clause 5.6. DI&C-ISG-04 provides guidance for meeting the communications independence requirements of IEEE Std. 603-1991, Clause 5.6.

Technical Report, APR1400-Z-J-NR-14001-P, Rev. 0, “Safety I&C System,” describes the design features of the APR1400 digital I&C system and how the design complies with NRC regulations. Section 4.2.4 of the technical report, "System Interfaces," discusses Plant Protection System (PPS) cabinet interfaces. The applicant provided description for some of the system interfaces and their type (e.g. Auxiliary Process Cabinet - Safety connects to PPS cabinets via hardwire cables, Core Protection Calculator System connects to PPS cabinets via hardwire cables, and PPS sends initiation signals to Engineered Safety Features-Component Control System Group Controllers through fiber optic Serial Data Link). It is not clear how other safety systems and non-safety systems are connected. List all safety to safety system interfaces and their interface type, and to list all safety to non-safety system interfaces and their interface type, and provide information on how these interfaces meet the requirements of IEEE Std. 603-1991, Clause 5.6, or provide a reference to sections of the

FSAR or technical reports where this information resides. Update the FSAR with the requested information.

Response – (Rev. 6)

Conformance to IEEE Std. 603 and RG1.75 independence requirements is described and provided in Section 7.1.2.42 of DCD Tier 2 and Appendix A of Safety I&C System Technical Report.

The system interfaces for the PPS, and the connection types, are described in Section 4.2.4 of the Safety I&C System Technical Report. The connection types that are not clearly described in Section 4.2.4 of the Safety I&C System Technical Report were revised to clarify what type of connection is used.

The system interfaces for the core protection calculator system (CPCS), and the connection types, are described in Section 4.3.4 of the Safety I&C System Technical Report. The connection types that are not clearly described in Section 4.3.4 of the Safety I&C System Technical Report were revised to clarify what type of connection is used.

The system interfaces for the ESF-CCS and the connection types are described in Section 4.4.4 of the Safety I&C System Technical Report.

The system interfaces for the qualified indication and alarm system-P(QIAS-P) and the connections types are described in Section 4.5.3 of the Safety I&C System Technical Report. The connections types that are not clearly described were added to Section 4.5.3 of the Safety I&C System Technical Report.

The interfaces for the reactor trip switchgear system (RTSS), and the connection types, are described in Section 4.8.2 of the Safety I&C System Technical Report. The connection types that are not clearly described in Section 4.8 of the Safety I&C System Technical Report were revised to clarify what type of connection is used.

In summary, Sections 4.2.4, 4.3.4, 4.5.3, and 4.8.2 of the Safety I&C System Technical Report were revised to include the corresponding interface types as indicated on the attached mark-up.

The detailed interface information between redundant portions of the safety system and between the safety and non-safety systems is provided as Tables 1 and 2. These tables (to be incorporated into the Safety I&C System technical report as Tables 4.1-1 and 4.1-2, respectively) also provide clarification of the as-built interface type such as hardwired connection, data link connection (SDL), data network connection (SDN), and Ethernet data link connection. The attached Table 3 (to be incorporated into the Safety I&C System technical report in response to RAI 45-8279 Question 07.09-9 Rev. 1 and is included for information) is provided as the list of interdivisional hardwired links in the ESF-CCS.

Table 1. Interface between redundant portions of the safety system

No.	FROM	TO	SIGNAL DESCRIPTION	INTERFACE TYPE	Safety I&C TeR 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

Note 1: The ESF-CCS in each division sends the CIV signals to the ITP of the same division via fiber optical data network connection (SDN).

Table 2. Interface between safety and non-safety system

No.	FROM	TO	SIGNAL DESCRIPTION	INTERFACE TYPE	Safety I&C TeR 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 4-17, Table 4-2
3	QIAS-P	DIS	CETs, HJTCs, control status	Hardwired	Figure 4-17, Table 4-2
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,	SDL	3.3.2, 4.1.1.4, 4.2.2.1, 4.2.3.5, 4.3.1.6,

No.	FROM	TO	SIGNAL DESCRIPTION	INTERFACE TYPE	Safety I&C TeR Section
			operating ESF-CCS status for EOP, plant safe shutdown, cabinet trouble alarm, system in test		
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 control system)	Turbine trip signal	Hardwired	4.2.1.1
11	ENFMS (ex-core neutron flux monitoring system)	NIMS (NSSS integrity monitoring system)	Sub-channel neutron flux signal	SDL	A.5.6

Some of the descriptions in Section 4.4.4.12, “Process-Component Control System” of the Safety I&C System technical report were modified as indicated in the attachment. The detailed information on these signals is provided in Sections 4.9.1, 4.9.2, and 4.9.3 of the Control System CCF Analysis technical report and the related mark-up that was provided in the response to RAI 68-7892 Question 07.07-8 Rev. 1 (refer to KHNP submittal MKD/NW-16-0986L dated September 20, 2016; ML16264A400) and 475-8596 Question 10.04.08-6 (refer to submittal MKD/NW-16-1034L dated October 11, 2016; ML16285A524). The description in Section 4.4.4.12 of the Safety I&C System technical report was revised to include additional clarification that the non-safety signals cannot block the operation of the ESF actuation signals and to reference Section 7.3.1.9 of DCD Tier 2 that was added in the response to RAI 475-8596, Question 10.04.08-6.

A description of the communication with external interfaces, such as the Emergency Operations Facility, will be revised by a new Section 4.6.2.7. The corresponding interface will be revised in Figure 4-1 of the Safety I&C System Technical Report, Figure 4-1 of the Diversity and Defense-in-Depth Technical Report and Figure 7.1-1 of the DCD Tier 2.

Impact on DCD

Figure 7.1-1 of the DCD will be revised as indicated in the attached mark-up.

Impact on PRA

There is no impact on the PRA.

Impact on Technical Specifications

There is no impact on the Technical Specifications.

Impact on Technical/Topical/Environmental Reports

Sections 4.6.2.7 and Figure 4-1 of the Safety I&C System Technical Report will be revised as indicated in the attached mark-up.
Figure 4-25 of the Safety I&C System Technical Report will be added as indicated in the attached mark-up.
Figure 4-1 of the Diversity and Defense-in-Depth Technical Report and CCF Coping Analysis TeR will be revised as indicated in the attached mark-up.
Figure 4.1-1 Control System CCF Analysis TeR will be revised as indicated in the attached mark-up.

LIST OF FIGURES

Figure 4-1 APR1400 I&C System Overview Architecture 26
Figure 4-2 Diversity Design Concept between Protection System and Diverse Protection System 27
Figure 4-3 PPS Functional Block Diagram 28
Figure 4-4 PPS Block Diagram 39
Figure 4-5 PPS Division A Trip Path Diagram 40
Figure 4-6 Overlap in Functional Testing for the PPS 41
Figure 4-7 Watchdog Timer for PPS 42
Figure 4-8 CPCS Block Diagram 48
Figure 4-9 Dynamic Adjustments to the Parameters 51
Figure 4-10 CPC Function Block Diagram 53
Figure 4-11 CEA Position and PF Movement 58
Figure 4-12 CPCS Interface Block Diagram 59
Figure 4-13 Watchdog Timer for CPCS 60
Figure 4-14 ESF-CCS Functional Block Diagram 61
Figure 4-15 ESF-CCS Functional Configuration 86
Figure 4-25 Signal Flow & Interface Diagram of External Data Communication--------116
Figure 4-17 Simplified Component Control Logic 88
Figure 4-18 Watchdog Timer for ESF-CCS 89
Figure 4-19 QIAS-P Block Diagram 102
Figure 4-20 Safety I&C Data Communication System 111
Figure 4-21 Data Communication between Redundant Divisions in PPS 112
Figure 4-22 Interface & Test Processor Data Link 114
Figure 4-23 Data Communication from ITP to QIAS-N 114
Figure 4-24 Data Communication from MTP to IPS 115
Figure 4-25 System Directory – Primary Systems 119
Figure 4-26 System Directory – Secondary Systems 119
Figure 4-27 System Mimic Page 120
Figure 4-28 ESCM Soft Control Template - Discrete Type (Example) 120
Figure 4-29 ESCM Soft Control Template – Modulation Type (Example) 121
Figure 4-30 ESF Control Block Diagram 125
Figure 4-31 Transfer of ESCM control function signals from MCR to RSR 128
Figure 4-32 Transfer of control functions for MI switch signals from MCR to RSR 129
Figure 4-33 Master transfer switch configuration for P-CCS and PCS 130

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
EOF	emergency operation facility
EOP	emergency operating procedure
EP	Ethernet processor
EPRI	Electric Power Research Institute
ESCM	ESF-CCS soft control module
ESF	engineered safety features

EDS External Data communication system

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
NERC	nuclear emergency response center
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
NDL	nuclear data link

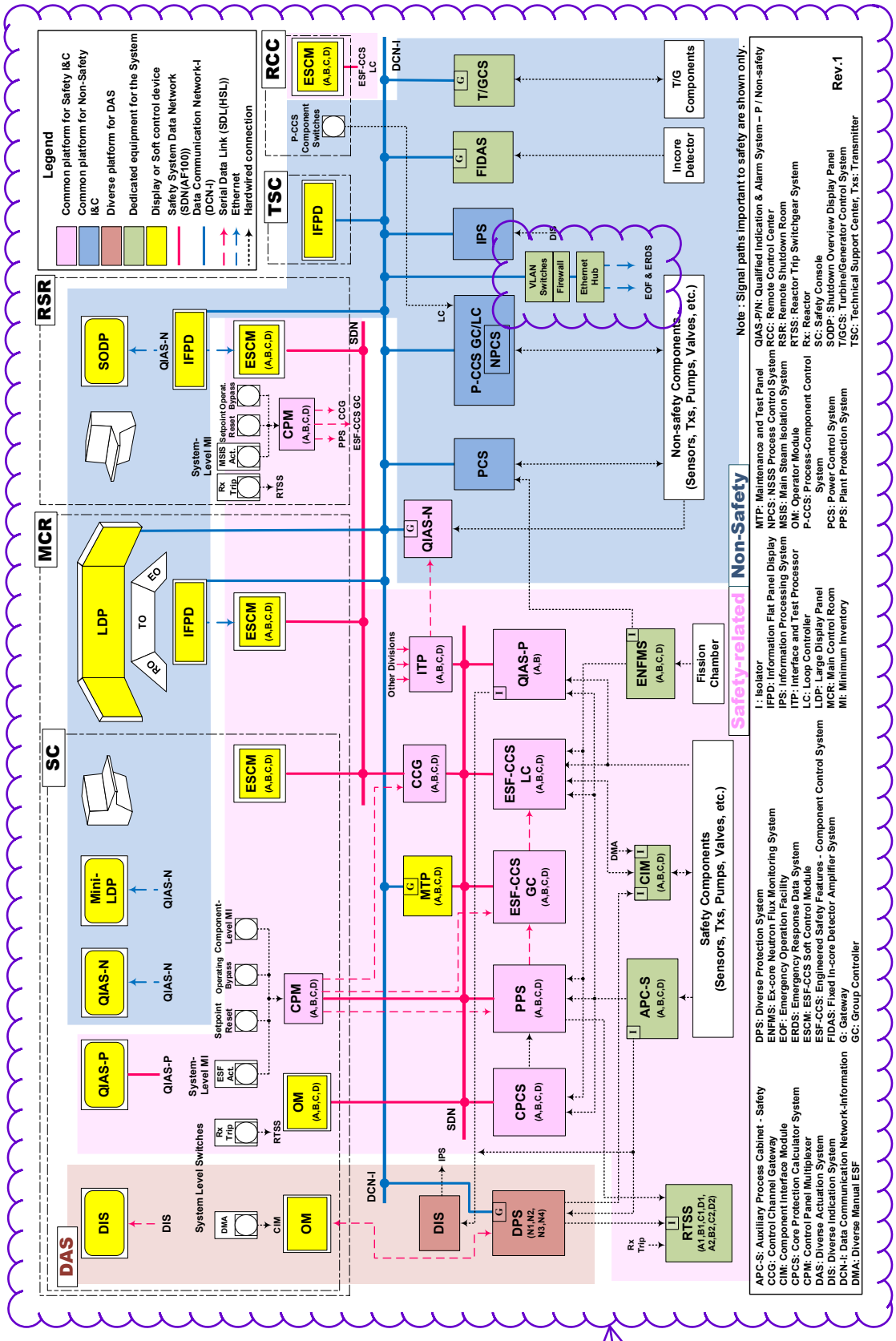

Figure 4-1 APR1400 I&C System Overview Architecture

Replace with "A" on the following page

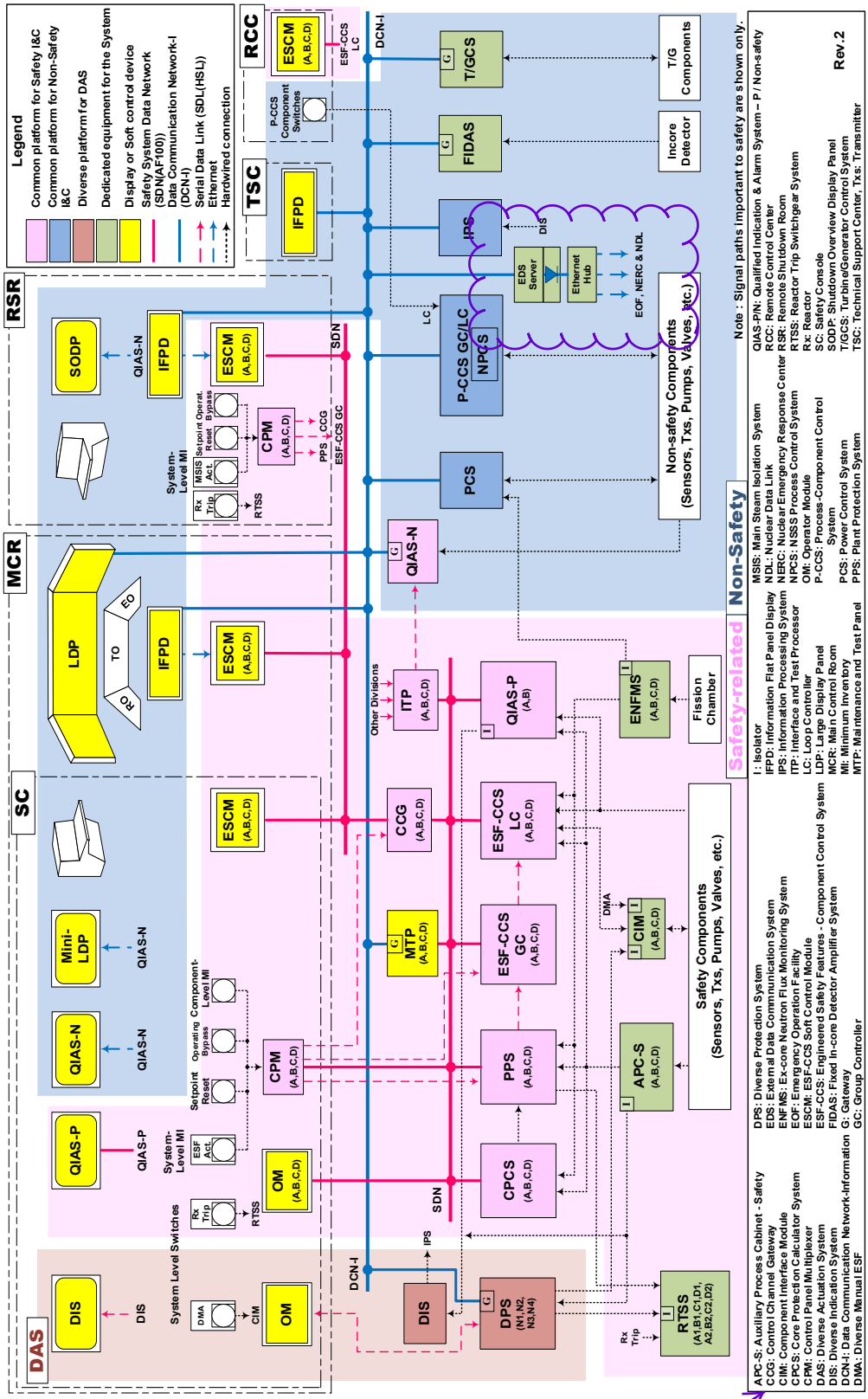

Figure 4-1 APR1400 I&C System Overview Architecture

"A"

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.

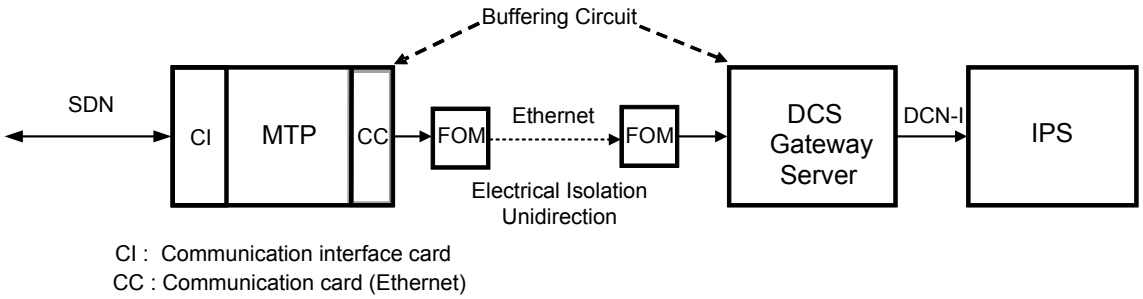

Figure 4-24 Data Communication from MTP to IPS

4.6.2.6 Communication of ESCM

TS

4.6.2.7 Communication to External Interface

TS

TS

4.7 Safety HSI System

TS

4.7.1 Safety Control HSI

RAI 45-7883-Question 07.09-2_Rev.5
RAI 45-7883-Question 07.09-2_Rev.6

Page intentionally blank

Page intentionally blank

CSS	containment spray system
CVCS	chemical and volume control system
CWP	CEA withdrawal prohibit
DAS	diverse actuation system
DBE	design basis event
DC	direct current
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
DRCS	digital rod control system
DVI	direct vessel injection
EDESS	emergency diesel engine starting system
EDG	emergency diesel generator
EMI	electromagnetic interference
ENFMS	ex-core neutron flux monitoring system
EOF	emergency operations facility
EOP	emergency operating procedure
EPRI	Electric Power Research Institute
ERDS	emergency response data system
ERF	emergency response facility
ESCM	ESF-CCS soft control module
ESF	engineered safety features
ESFAS	engineered safety features actuation system
ESF-CCS	engineered safety features-component control system

EDS External Data communication system

MTP	maintenance and test panel
NA	not applicable
NIMS	NSSS integrity monitoring system
NPCS	NSSS process control system
NRC	Nuclear Regulatory Commission
NSSS	nuclear steam supply system
OM	operator module
OSC	operational support center
P&ID	
PA	postulated accident
PC	personal computer
P-CCS	process-component control system
PCS	power control system
PF	penalty factor
PLC	programmable logic controller
PLCS	pressurizer level control system
PM	processor module
POSRV	pilot operated safety relief valve
PPCS	pressurizer pressure control system
PPS	plant protection system
PRV	process representative value
PS	processing section
PSCEA	part-strength CEA
PZR	pressurizer
QA	quality assurance
QIAS	qualified indication and alarm system
QIAS-N	qualified indication and alarm system – non-safety
QIAS-P	qualified indication and alarm system – P
RAM	random access memory
RCC	remote control center

NDL	nuclear data link
NERC	nuclear emergency response center

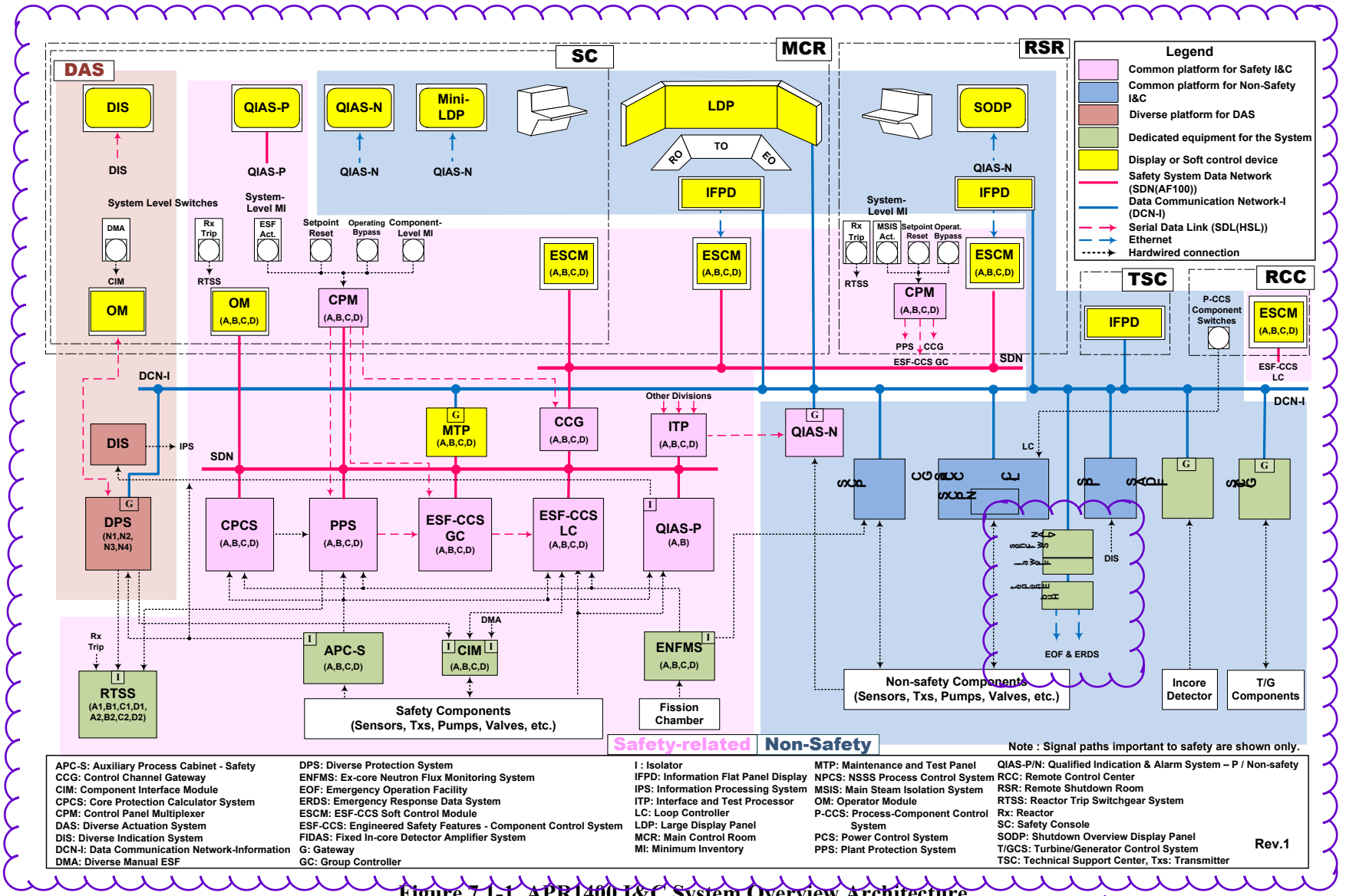

Figure 7.1-1 APR1400 I&C System Overview Architecture

Replace “C” on the following page

APR1400 DCD TIER 2

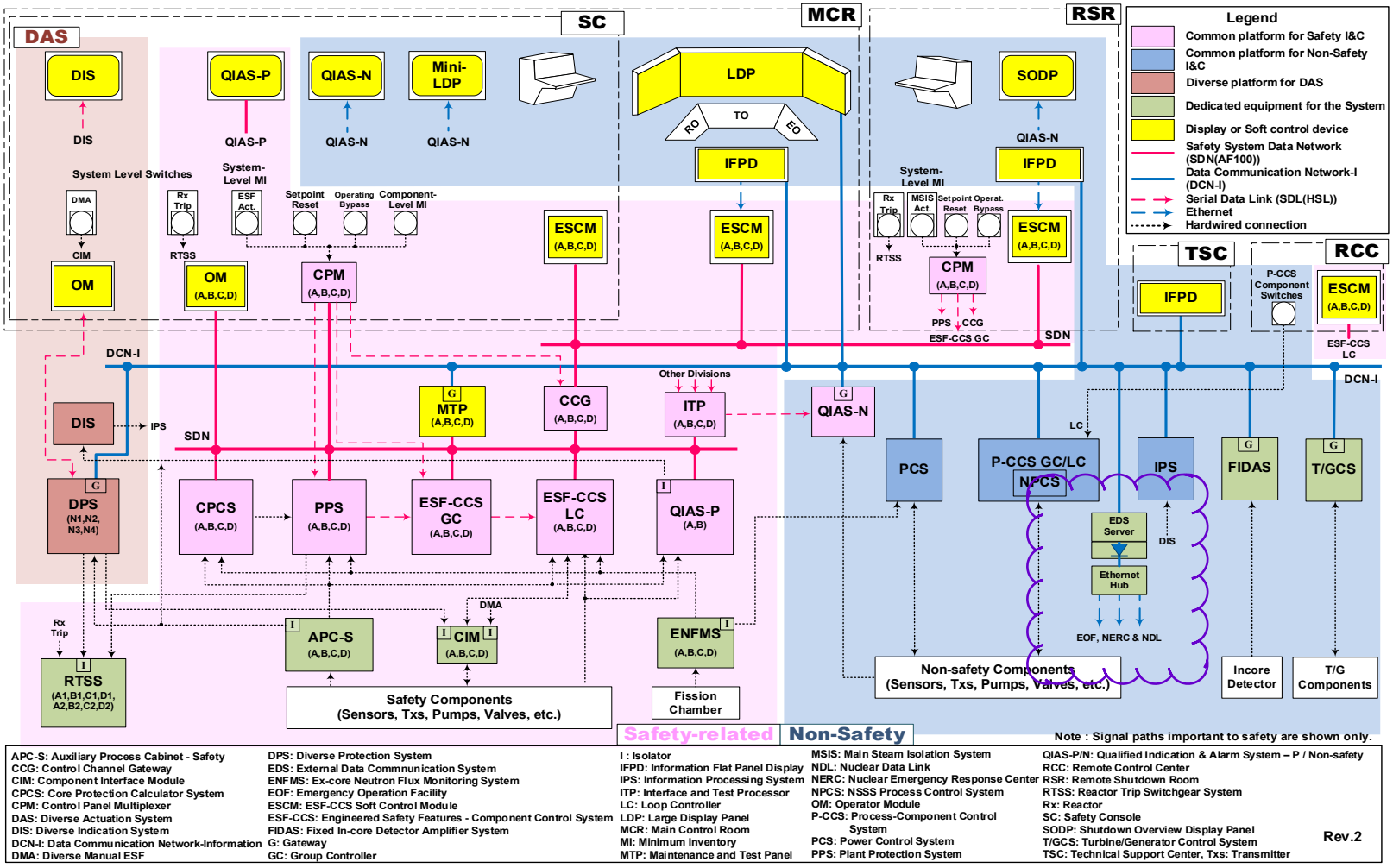

Figure 7.1-1 APR1400 I&C System Overview Architecture

"C"

D/G	diesel generator
DIS	diverse indication system
DMA	diverse manual ESF actuation
DPS	diverse protection system
DRCS	digital rod control system
DVI	direct vessel injection
EDG	emergency diesel generator
EEPROM	Electrically Erasable Programmable Read-Only Memory
EMC	electromagnetic compatibility
EMI	electromagnetic interference
ENFMS	ex-core neutron flux monitoring system
EOP	emergency operating procedure
ESCM	ESF-CCS soft control module
ESF	engineered safety features
ESFAS	engineered safety features actuation system
ESF-CCS	engineered safety features – component control system
FIDAS	fixed in-core detector amplifier system
FLC	FPGA-based logic controller
FPD	flat panel display
FPGA	field programmable gate array
FWCS	feedwater control system
GDC	general design criteria
GL	generic letter
GTG	gas turbine generator
HDL	hardware description language
HFE	human factors engineering
HJTC	heated junction thermocouple
HSI	human-system interface
I&C	instrumentation and control
ICC	inadequate core cooling
IEEE	Institute of Electrical and Electronics Engineers
IFPD	information flat panel display
IPS	information processing system
IRWST	in-containment refueling water storage tank
ITP	interface and test processor

EDS External Data communication system

ITS	important-to-safety
KHNP	Korea Hydro & Nuclear Power Co., Ltd.
LC	loop controller
LCL	local coincidence logic
LDP	large display panel
LOCA	loss of coolant accident
LOOP	loss of offsite power
M/A	manual/auto
MCR	main control room
MG Set	motor generator set
MI	minimum inventory
MS	main steam
MSIS	main steam isolation signal
MTP	maintenance and test panel
N/A	not applicable
NAPS	nuclear application programs
NIMS	NSSS integrity monitoring system
NPCS	NSSS process control system
NR	narrow range
NRC	U.S. Nuclear Regulatory Commission
NSSS	Nuclear Steam Supply System
OM	operator module
PA	postulated accident
P-CCS	process - component control system
PCS	power control system
PLC	programmable logic controller
PLCS	pressurizer level control system
POSRV	pilot operated safety relief valve
PPCS	pressurizer pressure control system
PPS	plant protection system
QIAS-N	qualified indication and alarm system – non-safety
QIAS-P	qualified indication and alarm system – p
RCP	reactor coolant pump
RCS	reactor coolant system
RFI	radio frequency interference

NDL	nuclear data link
NERC	nuclear emergency response center

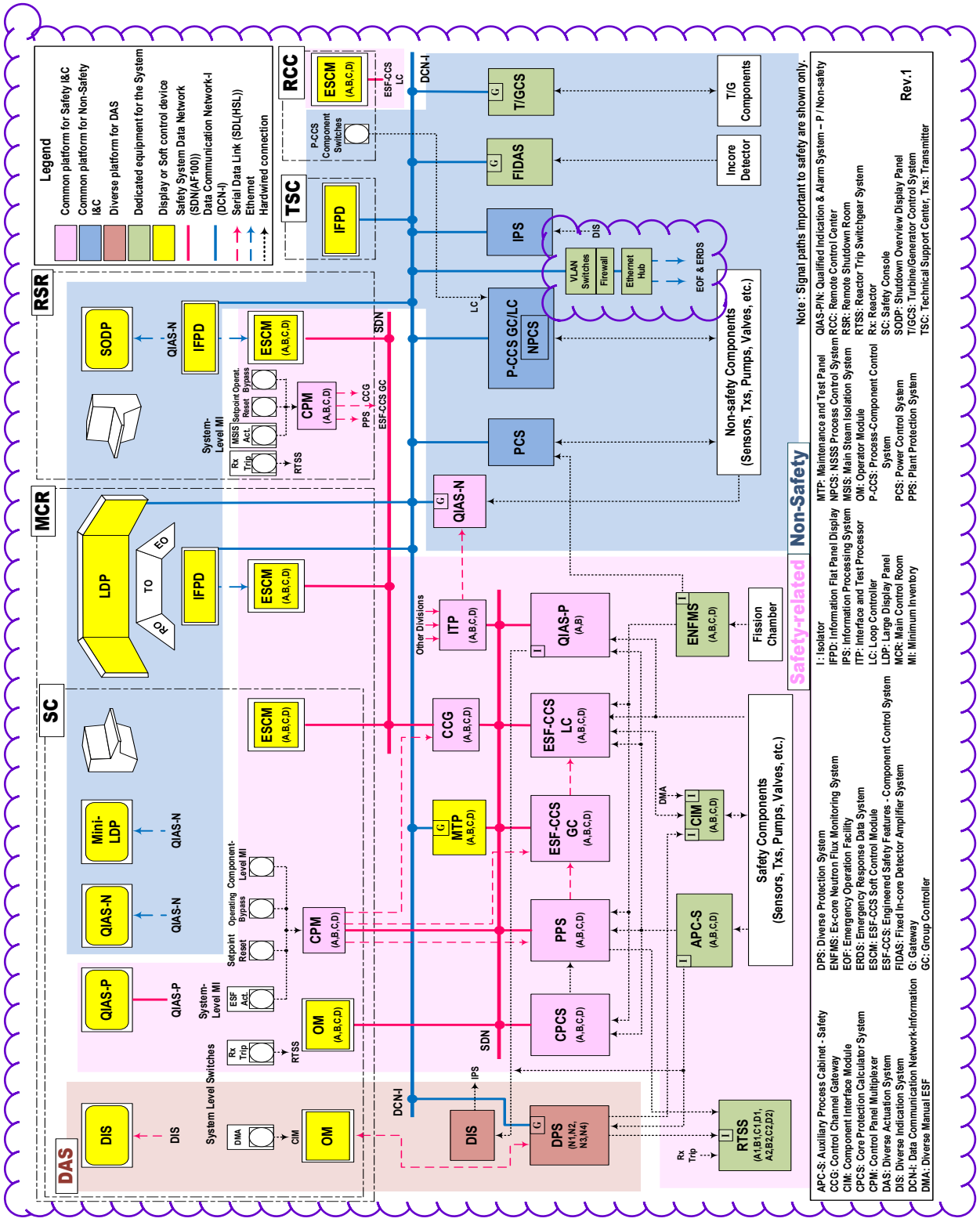

Figure 4-1 Architecture Overview of the APR1400 I&C Systems

Replace with "D" on the following page

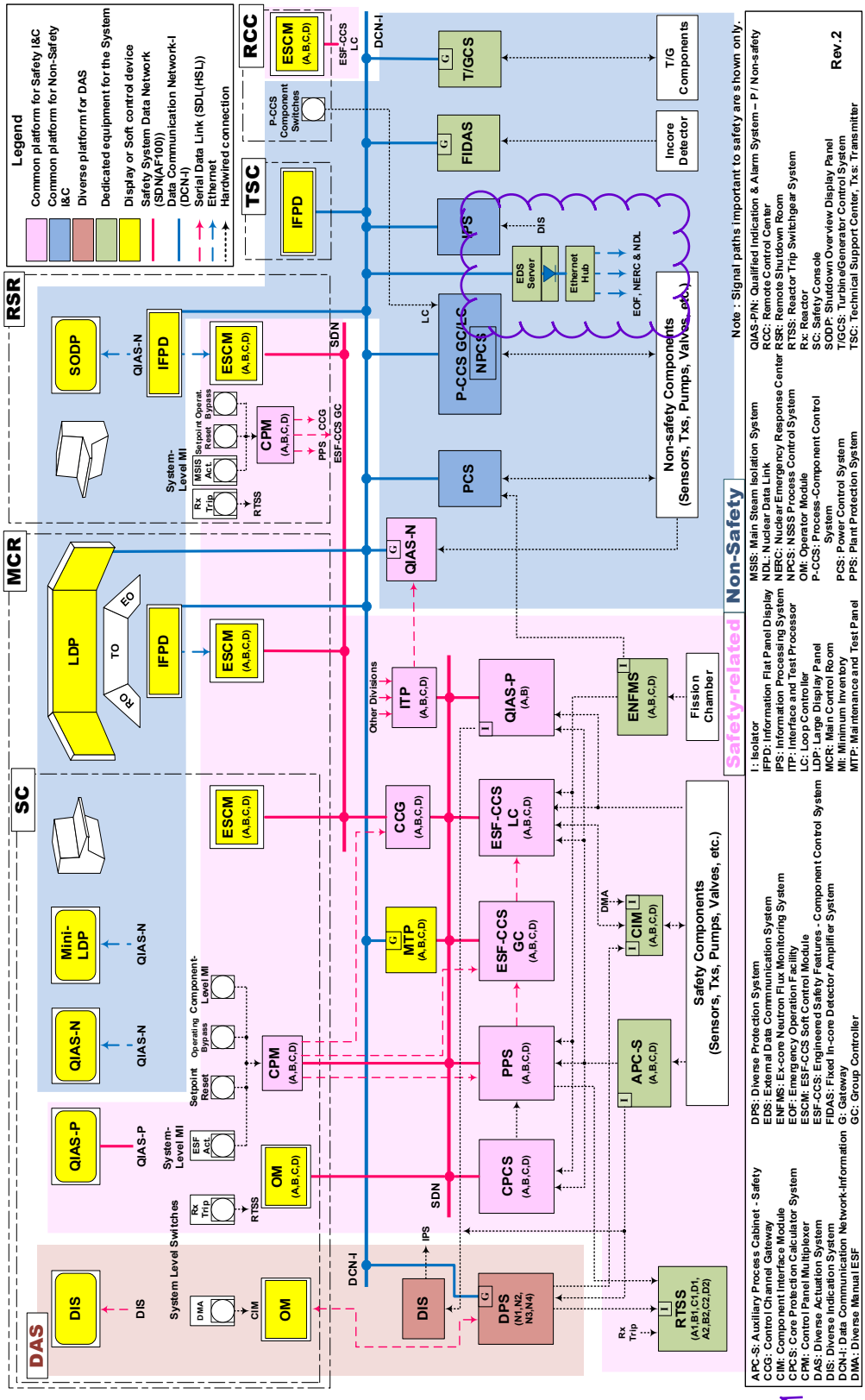

Figure 4-1 Architecture Overview of the APR1400 I&C Systems

"D"

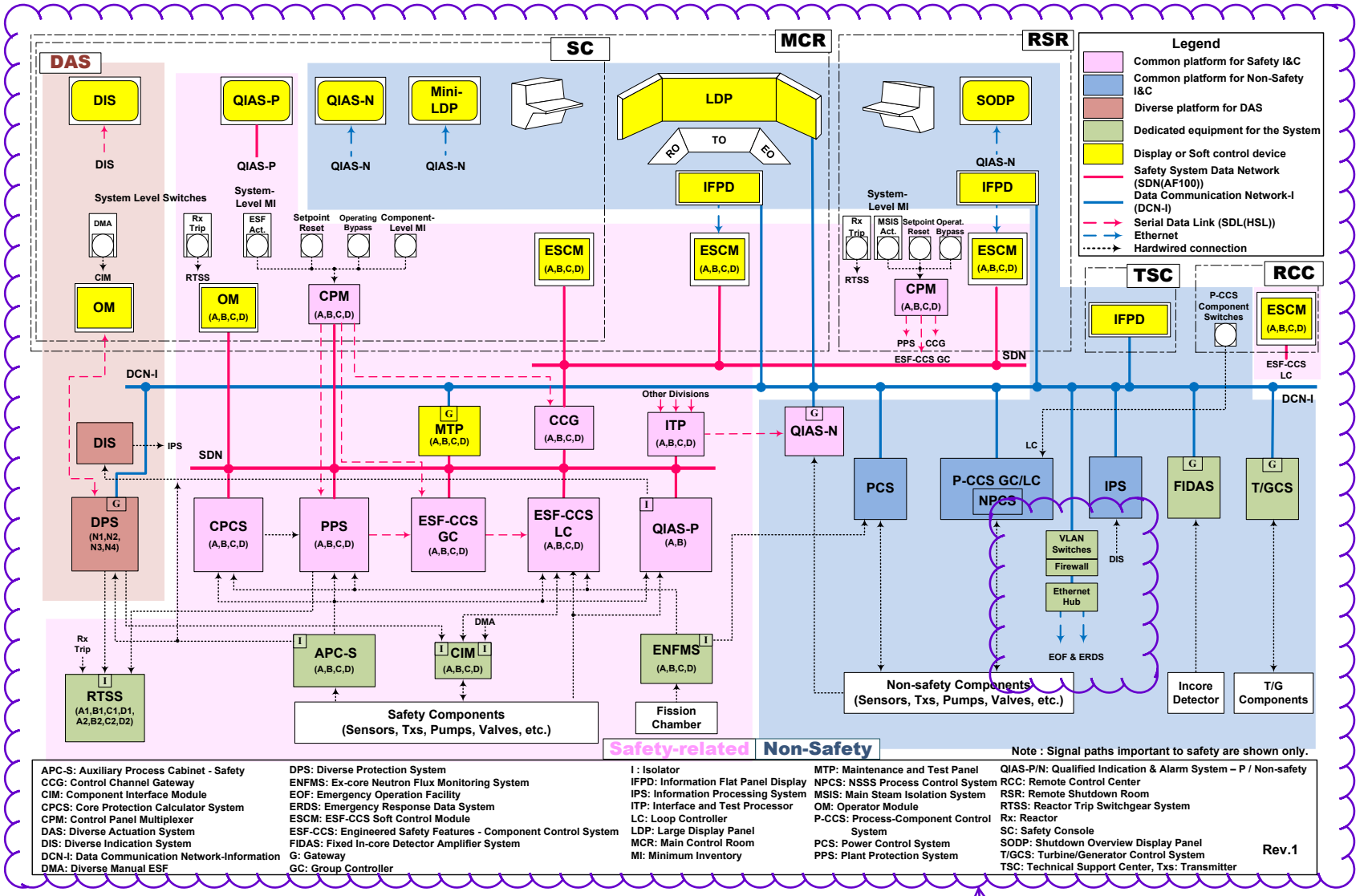

Figure 4-1 Overview of APR1400 I&C System Architecture

Replace "E" on the following page

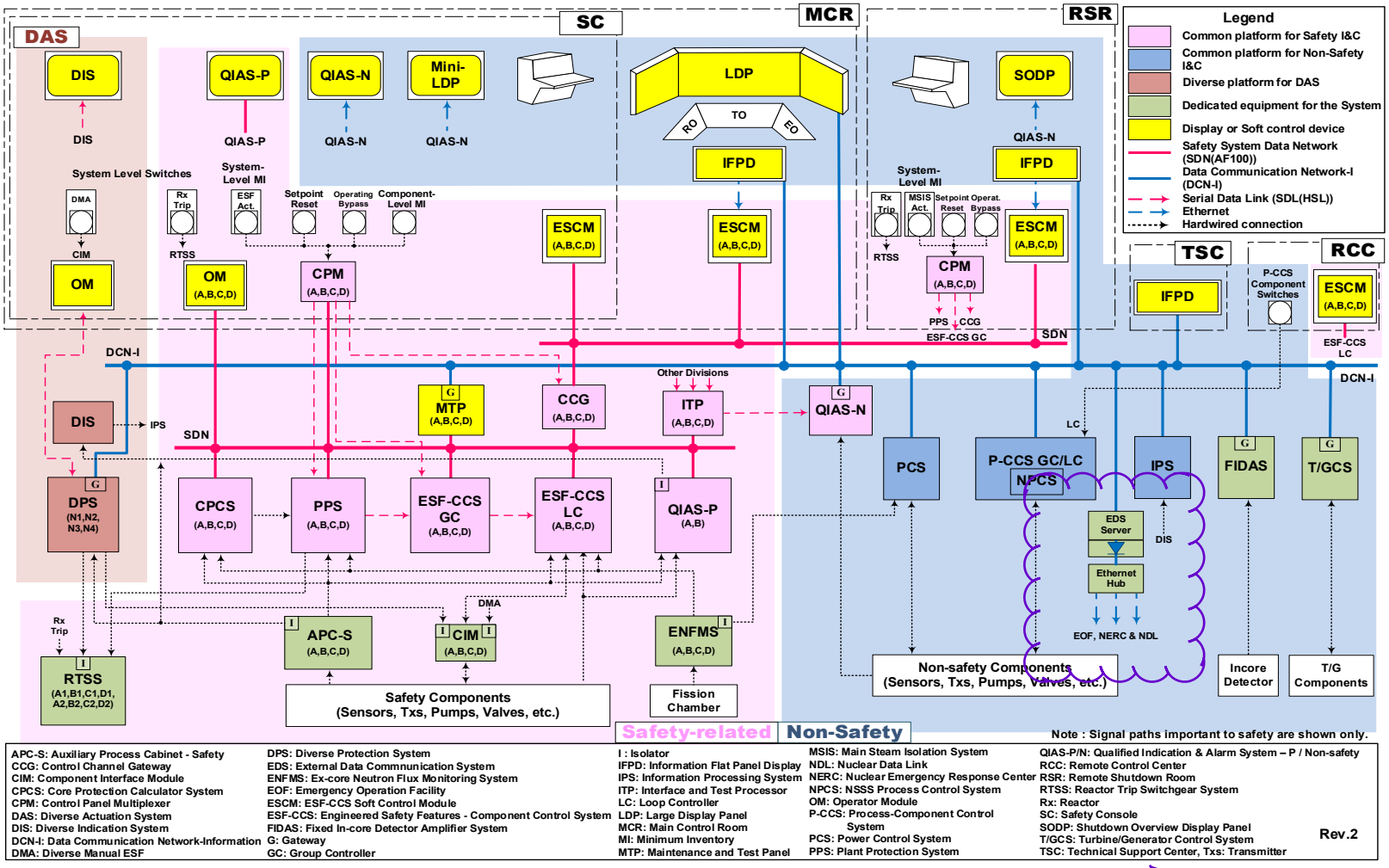

Figure 4-1 Overview of APR1400 I&C System Architecture

"E"

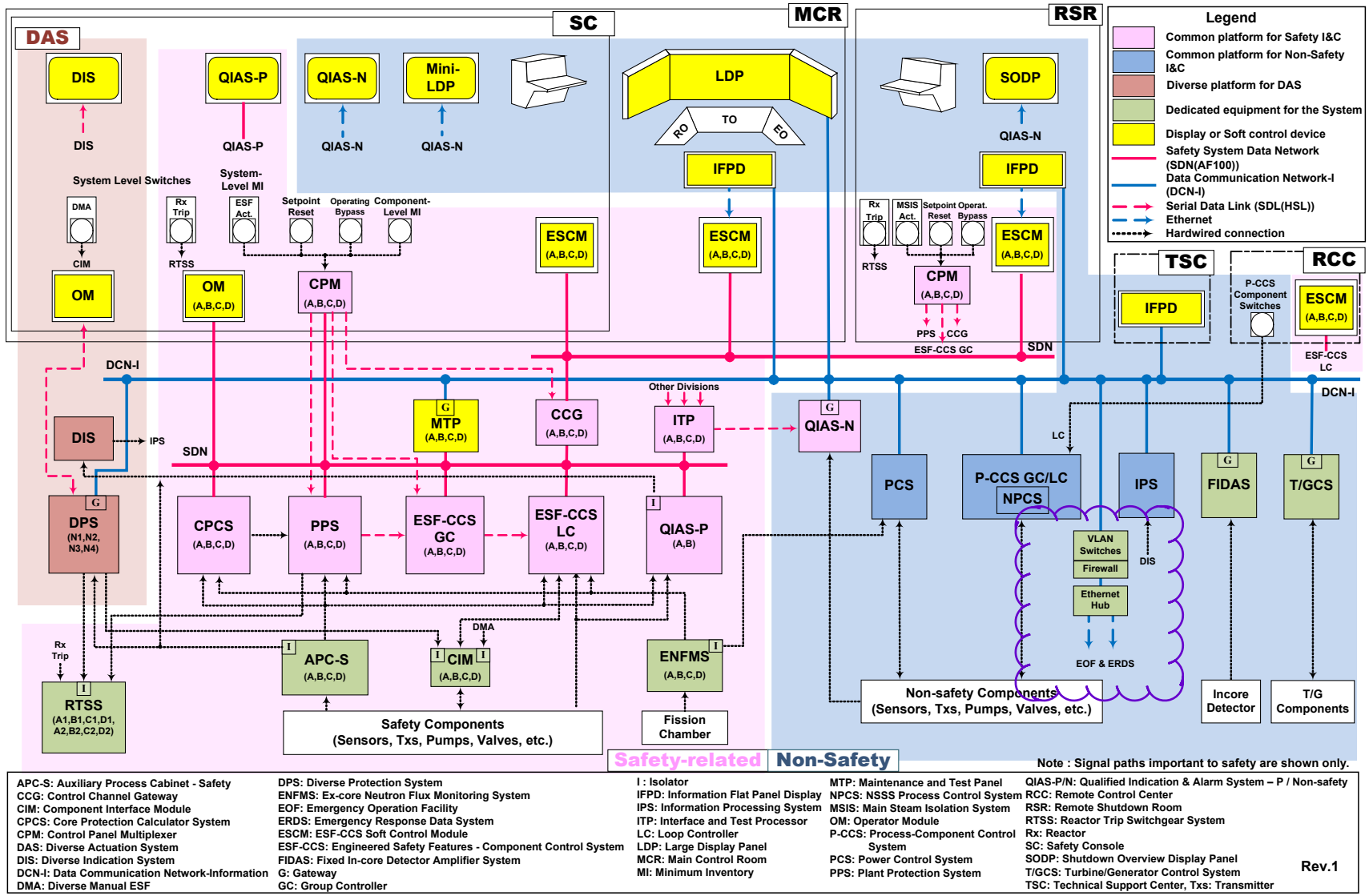

Figure 4.1-1 Credible Failure Boundary of Control System CCF

Replace "F" on the following page

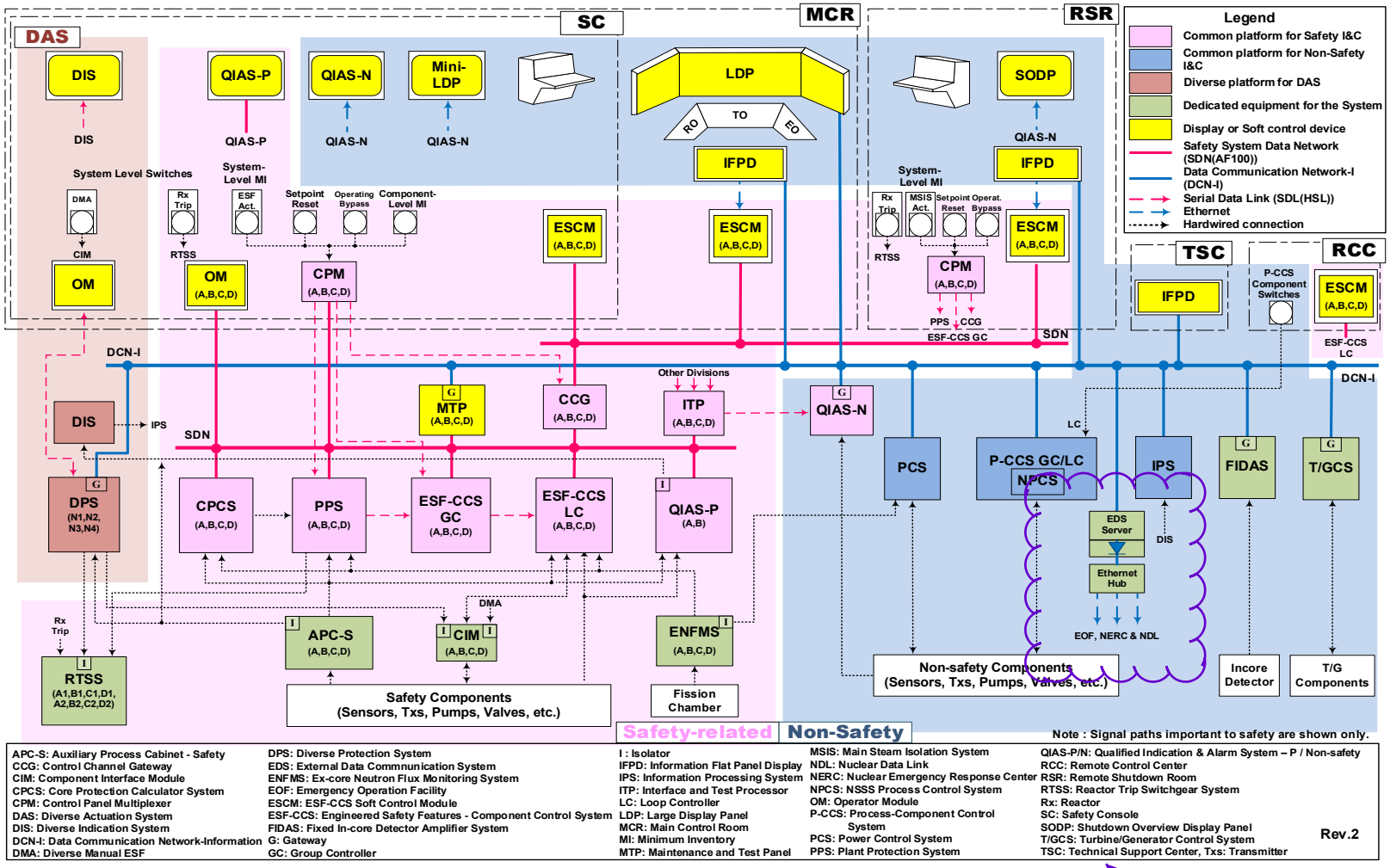

Figure 4.1-1 Credible Failure Boundary of Control System CCF

"F"