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.:	**274-8277**
SRP Section:	**07.01 - Instrumentation and Controls - Introduction**
Application Section:	**Section 7.1, 7.3, and 10.2**
Date of RAI Issue:	**10/27/2015**

Question No. 07.01-34

Provide additional descriptions and clarifications to the response to RAI 43-7887, Question 07.01-18 to demonstrate how the safety-related portion of the radiation monitoring system (RMS) meets the independence requirements and quality requirements of IEEE Std 603-1991.

10 CFR 50.55a(h)(3) states, in part, that an application filed on or after May 13, 1999, for design certifications must meet the requirements for safety systems in IEEE Std. 603-1991 and the correction sheet dated January 30, 1995. Clause 5.3, "Quality," of IEEE Std. 603-1991 requires components and modules to 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. IEEE Std 603-1991, Clause 5.6.3, requires the safety system design to be such that credible failures in and consequential actions by other systems, as documented in Clause 4.8 of the design basis, shall not prevent the safety systems from meeting the requirements of this standard. IEEE Std. 603-1991, Clause 5.6.3.1 states, in part, “Isolation devices used to effect a safety system boundary shall be classified as part of the safety system.”

In RAI 43-7887, Question 07.01-18, the staff requested for the applicant to demonstrate how standalone system, such as the safety-related portion of the Radiation Monitoring System (RMS) meet the requirements of IEEE Std 603-1991. In the response to this RAI, the applicant states that the RMS consists of two channels, the Safety Related Divisionalized Cabinet (SRDC) and the non-safety related RMS computer cabinet, as shown in Figure 7.3-23. The safety portion of the RMS consists of the radiation element, the local unit, and the SRDC. The divisional SRDC transmits the engineered safety feature actuation system (ESFAS) initiation signals to the dedicated ESFAS measurement channels, as described in Subsection 7.3.1.1. The safety portion of the RMS is part of the engineered safety feature (ESF) system as described in the Subsection 7.1.1.3. Therefore, the safety portion of the RMS is a part of ESF system and designed to comply with ESF System applicable criteria in the APR1400 FSAR Tier 2, Table 7.1-1, “Regulatory Requirements Applicability Matrix.” The ESF system, including the

safety portion of the RMS, complies with the requirements of IEEE Std 603-1991, Clauses 5.1, 5.3, 5.5, and 5.6, as described in Subsection 7.3.3.2, is addressed in the Appendix A, “Conformance to IEEE Std 603-1991” of Technical Report, APR1400-Z-J-NR-14001, Rev. 0 “Safety I&C System." Based on the staff’s review of APR1400 FSAR Tier 2, Sections 7.3.1.1 and 7.1.1.3, and Appendix A of the Safety I&C System Technical Report, the staff finds that additional information is needed to clarify the design description of the RMS as described below:

a. APR1400 FSAR Tier 2, Section 7.3.1.1, states the balance of plant (BOP) ESFAS receives process variable signals from the safety portion of the RMS, manual ESF system-level actuation switches, and manual channel bypass switches. The BOP ESFAS consists of 1-out-of-2 logic taken twice except for the Fuel handling area emergency ventilation actuation signal (FHEVAS), which has one 1-out-of-2 logic. APR1400 FSAR Tier 2, Figure 7.3-23, shows the RMS measurement channel functional diagram, but design descriptions or reference to this figure were not provided in FSAR Tier 2, Section 7.3. Based on this figure, it is not clear how many divisions are in the RMS SRDC. In addition, it is not clear whether the RMS computer cabinet is safety-related or non-safety. If the RMS processor in the computer cabinet is non-safety, then how is it isolated from the SRDC processor to meet the independence requirements of IEEE Std. 603-1991, Clause 5.6.3? If the RMS processor is safety-related, how is it meeting independence requirements of IEEE Std. 603-1991, Clause 5.6.3 when transmitting information to the IPS and QIAS-N?

b. Appendix A of the Safety I&C System Technical Report, Section A.5.3, "Quality," states the platform to be used for the safety I&C system is qualified as described in WCAP-16097-P-A, “Common Qualified Platform Topical Report”, Rev. 3, February 2013. However, APR1400 FSAR Tier 2, Section 7.1 under "Safety Systems," states the safety-related portion of the RMS is implemented on an independent platform that is different from the Common Q platform. Further, Technical Report APR1400-Z-J-NR-14003, Rev. 0, “Software Program Manual,” does not appear to address standalone safety-related systems such as the RMS. As such, it is unclear how the requirements of IEEE Std 603-1991, Clause 5.3, are met for the safety-related portion of the RMS.

c. Clarify in the APR1400 FSAR that the RMS is the only standalone safety-related I&C system.

Response – (Rev. 1)

a. DCD Tier 2, Section 7.3.1.1 will be revised to provide a detailed design description and reference to Figure 7.3-23.

   Figure 7.3-23 is to be revised to reflect the latest system functional configuration. The radiation monitoring system (RMS) processor receives the electrically isolated radioactivity measurement signal directly from the local unit, rather than from the safety related divisionalized cabinet (SRDC) processor.

   The revised figure is a simplified block diagram which provides a functional overview of the RMS. Although the number of divisions for the SRDC can be inferred from the previous heading written above the SRDC, where it states “safety channel ‘A’ (B similar),” a note has been added to clearly state the SRDC cabinet has redundant

divisions. The figure can be viewed for clarity in conjunction with Figures 7.3-9 (FHEVAS), 7.3-10 (CPIAS) and 7.3-11(CREVAS). Also, Section 7.3.1.7 of DCD Tier 2 will be revised to state the SRDC cabinet has redundant divisions.

The RMS computer cabinet is non-safety related; Figure 7.3-23 is to be revised accordingly for clarity. Those measurement signals originating from the safety related detector channels that are transmitted to the non-safety RMS processor are electrically isolated using an IEEE Std 384 Class 1E qualified isolator per Clause 6.2.2, at each local unit. This satisfies the independence requirement between safety systems and other systems per IEEE Std 603-1991, Clause 5.6.3.

Since the isolation is done at the local unit, no isolation is needed for those signals sent to the IPS and QIAS-N. The revision to Figure 7.3-23 shows the connection from the RMS processor to the IPS and QIAS-N through a fiber-optic converter. The fiber-optic converter does not provide isolation, but provides data communication paths via fiber-optic signal transmission.

b. The safety portion of RMS is not addressed in the Safety I&C System TeR. As stated in Section 2 of the Safety I&C System TeR, the report provides the system description, design features and software design process of 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).

   The SPM TeR is intended to provide generic guidance for the software engineering process for digital computer-based instrumentation and control (I&C) systems. The SPM TeR does not address a specific system or software but describes general software processes for all I&C systems. Even though the safety portion of RMS is not specifically addressed in the SPM TeR, the general software processes described in the SPM TeR are applied to the safety portion of the RMS.

   As the RMS supplier and platform have not been determined for the APR1400 DC project, KHNP cannot provide detailed platform information, such as qualification and software design of the SRDC. However, KHNP's purchase specification for the reference plants, Shin-Kori 3&4 and upon which the APR1400 specification will be based, requires that the SRDC be supplied by a 10 CFR 50, Appendix B qualified supplier. The hardware of the SRDC is qualified to Class 1E, and the software of the SRDC will meet the requirements of NRC RG 1.152, Rev. 3 and IEEE Std. 7-4.3.2-2003.

   DCD Tier 2, Sections 7.3.3.2 and 7.3.3.3 will be revised to state compliance of the SRDC to IEEE Std. 603-1991 and IEEE Std. 7-4.3.2-2003.

c. As indicated in the response to RAI 43-7887 Question 07.01-18, there are no other standalone safety-related I&C systems other than ENFMS, APC-S, the SRDC of the RMS, and the CIM. DCD Tier 2, Section 7.1 describes the following :

   "The following safety I&C systems are implemented on independent platforms that are diverse from the safety-qualified PLC platform: ex-core neutron flux monitoring system (ENFMS) (see Subsection 7.2.1.1.c), auxiliary process cabinet – safety (APC-S) (see

Subsection 7.2.1), safety portion of radiation monitoring system (RMS) (refer to Section 11.5 and Subsection 12.3.4) and component interface module (CIM) (see Subsection 7.3.1.11)."

Impact on DCD

DCD Tier 2, Subsections 7.3.1.1, 7.3.1.7, 7.3.2.3, 7.3.3.2, 7.3.3.3, 7.3.5, and Figure 7.3-23 will be revised, as indicated in the attachment associated with this response.

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

There is no impact on any Technical, Topical, or Environmental Report.

(CIM), which performs signal prioritization. The CIM transmits signals to the final actuated device (e.g., switchgear, motor control center, solenoids).

The ESF-CCS receives signals from the master transfer switches to disable all main control room (MCR) controls and enable remote shutdown room (RSR) controls.

safety related divisionalized cabinet (SRDC)

7.3.1.1 Engineered Safety Features Actuation System Measurement Channels

The ESFAS measurement channels perform continuous monitoring of each selected plant variable and transmit analog signals to bistables.

of the RMS instrumentation

The ESFAS measurement channels receive signals from the PPS and the ~~safety portion~~ of the RMS. Detailed description ~~for the safety portion of the RMS~~ is described in Section 11.5 and Subsection 12.3.4.

Undervoltage signals received from the electrical panel detect a loss of voltage on the Class 1E 4.16 kV buses.

Deleted and inserted "A" on next page

A measurement channel for the PPS is shown in Figure 7.2-2. A measurement channel for the RMS is shown in Figure 7.3-23. ~~It consists of a sensor/transmitter, current loop resistors, loop power supply, and fiber optic isolated outputs for the IPS and QIAS-N.~~

A measurement channel is physically separated and electrically isolated from other channels.

7.3.1.2 Engineered Safety Features Actuation System Bistable and Coincidence Logic

The bistable processors (BPs) are in the PPS cabinet. The ESFAS bistable logic in the BP compares the analog signal from the sensors with predetermined fixed or variable setpoints. If the input signal exceeds the setpoint, the bistable logic produces trip signals that are transmitted to the coincidence logic.

For the nuclear steam supply system (NSSS) ESFAS, there are two redundant BPs in each channel. The outputs of the BPs are designated as follows: A1 and A2 in channel A, B1 and

RAI 274-8277 - Question 07.01-34

RAI 274-8277 - Question 07.01-34_Rev.1

A

The RMS measurement channel consists of a radiation element, a local unit, an SRDC processor, an RMS processor, and a fiber optic transmitter. The radiation element includes a radiation sensor and a signal transmitter. The local unit distributes the radiation signal to the safety related SRDC processor and non-safety RMS processor. When the radiation signal exceeds the radiation setpoint value, the SRDC processor sends a BOP ESFAS initiation signal to the ESF-CCS GC. The radiation signal is displayed on the IPS and the QIAS-N in the MCR. The radiation signal originating from the safety related radiation element that is transmitted to the non-safety RMS processor is electrically isolated using a Class 1E qualified isolator, at the local unit.

The radiation element and the local unit are installed in the radiation monitor described in Subsections 11.5 and 12.3.4.1.

b. Manual test interlock

The manual test function is performed when the function enable key switch is activated.

7.3.1.7 Redundancy

The ESF-CCS consists of following redundant features:

a. Four divisions of the GCs

b. Four divisions of the LCs

c. Four divisions of the 2-out-of-4 coincidence logic in the GCs for the NSSS ESFAS

d. Two divisions of the 1-out-of-2 logic in the GCs for the BOP ESFAS

e. Two 1-out-of-2 logics in each division for the BOP ESFAS except the FHEVAS

f. Two GCs in each division

g. Four redundant ac power supplies

h. Four redundant dc power supplies

There are four redundant divisions for each parameter from the process sensors to the initiation logic in the PPS for the NSSS ESFAS.

There are two redundant divisions for each parameter from the process sensors to the actuation logic in the GC for the BOP ESFAS.

Each ESF-CCS division actuates the ESF components assigned in that division.

The ESF system meets the single failure criterion and can be tested during operation.

The ESFAS coincidence logic in the LCL is changed to 2-out-of-3 logic when a division is removed for testing or maintenance without affecting system availability.

The SRDC is redundant, having divisions A and B.

in bypass for testing and the single failure of the different channel belonging to other division occurs at the same time under the radiation release accident, the 1-out-of-1 logic of the available division can be actuated by the remaining operating radiation monitor. The single failure criterion is met by changing the logic from 1-out-of-2 to 1-out-of-1 in the channel bypass.

In addition, the purpose of the bypass mode of the BOP ESFAS is to test a measurement channel. For BOP ESFAS design, double sets of two channels (A and B) are provided for measurement channels except the FHEVAS. Even if one measurement channel is placed in test mode, the other measurement channel is available.

7.3.2.2 Quality of Components and Modules

The ESF system is implemented using Class 1E components.

7.3.2.3 Independence

The SRDC meets the independence requirement between safety systems and other systems of IEEE Std 603.

The locations of the sensors for the ESFAS and the points at which the sensing lines are connected to the process loop have been selected to provide physical separation of the divisions within the system, thereby precluding a situation in which a single event could remove or negate a protective action and safety function.

The cabling routing and sensing lines from sensors comply with NRC RG 1.75 (Reference 6) and NRC RG 1.151 (Reference 7). Cables for each division are physically separated. The I&C cables are routed separately from the power cables.

The ESFAS initiation logic is located in four PPS cabinets and two RMS cabinets, and the ESF actuation devices are controlled from four ESF-CCS cabinets. The geographical separation and electrical isolation between these cabinets reduces the possibility of a CCF.

The outputs of each division are isolated from each other. The loss of one division does not cause loss of the system function.

7.3.2.4 Diversity and Defense-in-Depth

The diversity and defense-in-depth features for the ESF-CCS are implemented by the DPS and DMA switches. The control signals from the ESF-CCS, DPS, DMA switches, and FPC

The FMEA assumes that one bistable trip channel is bypassed for maintenance.

The FMEA results demonstrate that:

a. Any single failure does not prevent a system-level ESFAS function due to four division redundancy.

b. Any single failure is detected by diagnostic or periodic test.

The FMEA for the ESFAS function from sensor to the LCL is included in Table 7.2-7. Table 7.3-8 describes the FMEA for the ESF-CCS.

7.3.3.2 Conformance with IEEE Std. 603

Conformance with IEEE Std. 603 is addressed in the Safety I&C System Technical Report.

7.3.3.3 Conformance with IEEE Std. 7-4.3.2

The SRDC will be supplied by a 10 CFR Part 50, Appendix B qualified supplier.

Conformance with IEEE Std. 7-4.3.2 is addressed in the Safety I&C System Technical Report.

~~The SRDC is designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with ASME NQA-1. (Reference 30)~~ The hardware of the SRDC ~~is~~ will be designed and tested in accordance with the requirement of IEEE Std. 323.

7.3.3.4 Analysis for Additional Postulated Failure

The analysis for additional postulated failures is as follows:

a. Loss of cooling water to vital equipment: The APR1400 has four divisions of safety cooling water, corresponding to the four divisions of safety ESF equipment. These four divisions are controlled by the ESF-CCS. Therefore, loss of a single division of cooling water does not prevent accomplishing the safety function.

b. Loss of plant instrument air: There is no reliance on plant instrument air for any safety functions.

c. Loss of power source: All of the subsystems in the safety system are provided power from redundant power sources. Therefore, loss of a single power source does not prevent accomplishing the safety function. The loss of a power source can result in a transient condition. A transient condition is considered in the safety analysis described in Chapter 15.

The software of the SRDC ~~meets~~ will meet the requirements of NRC RG 1.152 (Reference 31) and IEEE Std. 7-4.3.2.

20. IEEE Std. 344-2004, "IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, 2004.

21. Regulatory Guide 1.180, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related instrumentation and Control Systems," Rev. 1, U.S. Nuclear Regulatory Commission, October 2003.

22. IEC 61000-4-2, "Electromagnetic Compatibility – Testing and Measurement Techniques – Electrostatic Discharge Immunity Test," International Electrotechnical Commission.

23. IEC 61000-4-5, "Electromagnetic Compatibility-Testing and Measurement Techniques – Surge Immunity Test," International Electrotechnical Commission.

24. IEEE Std. 352-1987, "IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems," Institute of Electrical and Electronics Engineers, 1987.

25. IEEE Std. 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, 1991.

26. IEEE Std. 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, 2003.

27. IEEE Std. 379-2000, "IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems," Institute of Electrical and Electronics Engineers, 2000.

28. APR1400-Z-J-NR-14013-P, "Response Time Analysis of Safety I&C System," KHNP, November 2014.

29. 10 CFR Part 50, Appendix A, "General Design Criteria for Nuclear Power Plants," U.S. Nuclear Regulatory Commission.

~~30. ASME NQA-1,"Quality Assurance Requirements for Nuclear Facility Applications," The American Society of Mechanical Engineers, 2008 Edition with 2009 Addenda.~~

31. Regulatory Guide 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," Rev. 3, U.S. Nuclear Regulatory Commission, July 2011.

Replace this figure with attached figure A.

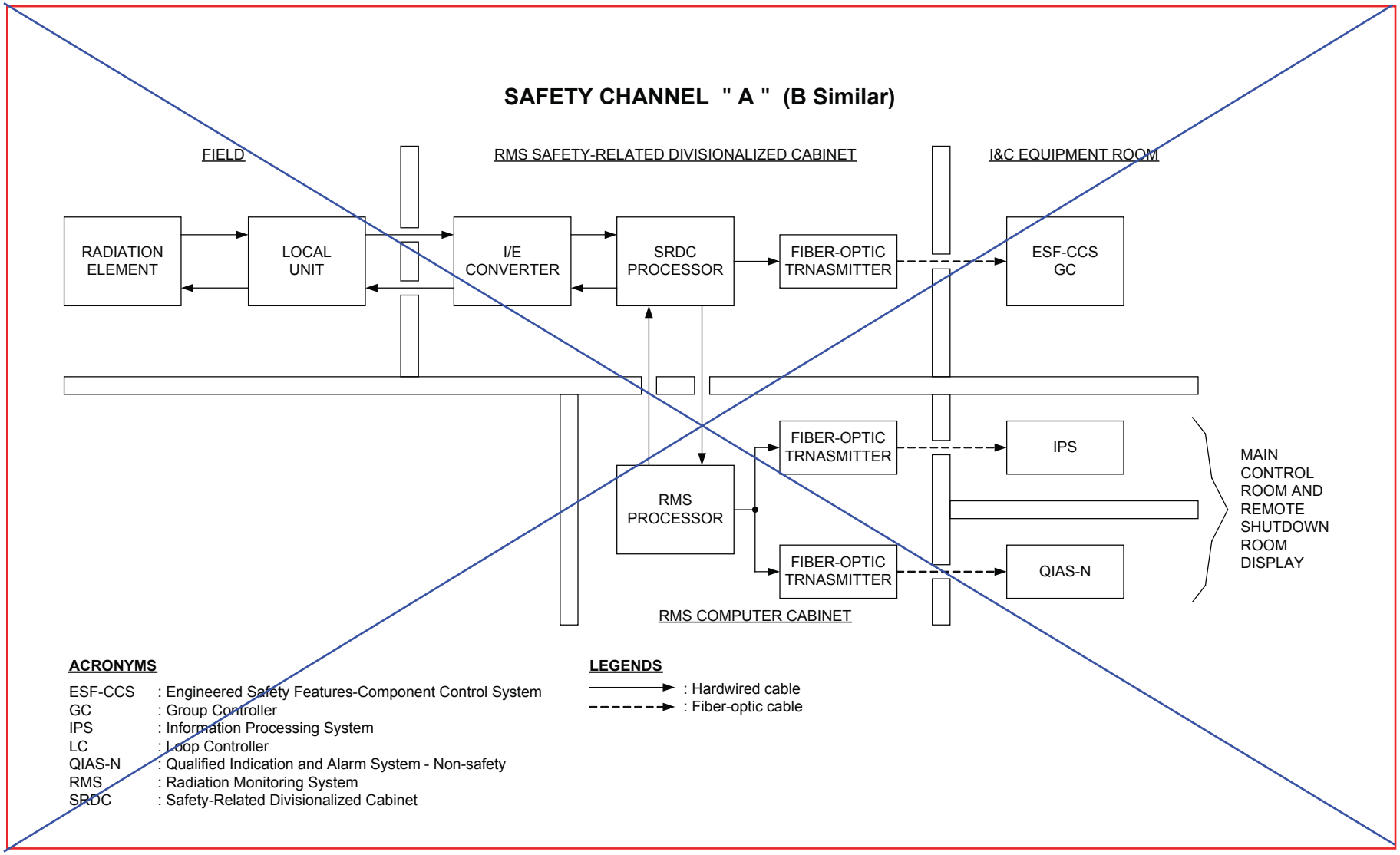
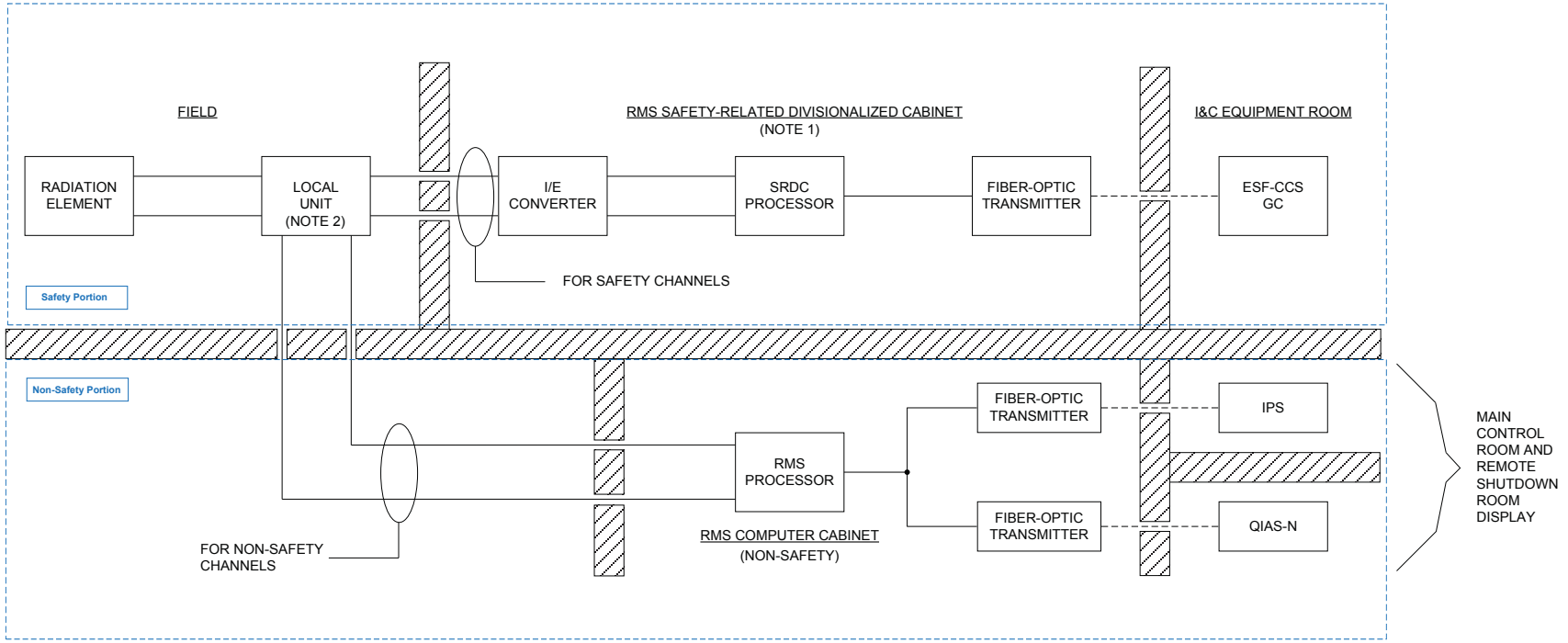


Figure 7.3-23 Radiation Monitoring System Measurement Channel Functional Diagram

A



ACRONYMS

ESF-CCS : Engineered Safety Features-Component Control System
GC : Group Controller
IPS : Information Processing System
LC : Loop Controller
QIAS-N : Qualified Indication and Alarm System - Non-safety
RMS : Radiation Monitoring System
SRDC : Safety-Related Divisionalized Cabient

LEGENDS

———— : Hardwired cable
– – – – – – – – : Fiber-optic cable

NOTES

1. THE SRDC CABINET IS REDUNDANT,HAVING DIVISIONS A AND B.
2. ISOLATORS ARE INCLUDED.