Revision	Approved by	Number of Pages
000		53
Approval Date	26/10-17	

General Nuclear System Ltd.

UK HPR1000 GDA Project

Document Reference:	**HPR/GDA/PSR/0008**

Preliminary Safety Report

Chapter 8

Instrumentation & Control

DISTRIBUTION LIST

Recipients	Cross Box
GNS Executive	☐
GNS all staff	☐
GNS and BRB all staff	☒
CGN	☒
EDF	☒
Regulators	☒
Public	☐

SENSITIVE INFORMATION RECORD

Section Number	Section Title	Page	Content	Category

Table of Contents

8.1 List of Abbreviations and Acronyms

ACP	Auxiliary Control Panel
ACPR	Advanced Chinese Pressurized Reactor
ALARP	As Low As Reasonably Practicable
ATWS	Anticipated Transient Without Scram
ASG	Emergency Feedwater System [EFWS]
BOP	Balance of Plant
CCF	Common Cause Failure
CI	Conventional Island
CIC	Component Interface Cabinet
COWP	Compact Operator Workplace
DAC	Diverse Actuation Cabinet
DBC	Design Basic Condition
DCS	Digital Control System
DEC	Design Extension Condition
DHP	Diverse Human interface Panel
DTC	Data Transmission Cabinet
ECP	Emergency Control Panel
ESFAC	Engineered Safety Feature Actuation Cabinet
ESFAS	Engineered Safety Feature Actuation System
FC	Function Category
GDA	Generic Design Assessment
GME	Turbine Supervisory System [TSS]
GRE	Turbine Governing System [TGS]
GSE	Turbine Protection System [TPS]
GW	Gateway
HAF	Chinese Nuclear Safety Regulations
HCP	Hard Control Panel

HMI	Human Machine Interface
HPR1000 (FCG3)	Hua-long Pressurized Reactor under construction at Fangchenggang nuclear power plant unit 3
HVAC	Heating, Ventilation and Air Conditioning system
IAEA	International Atomic Energy Agency
I&C	Instrumentation and Control
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
KCC	Nuclear Accident Emergency Management System [NAEMS]
KDA	Severe Accident I&C System [SA I&C]
KDS	Diverse Actuation System [DAS]
KIC	Plant Computer Information and Control System [PCICS]
KNS	Real-time Information Monitoring System [RIMS]
KPR	Remote Shutdown Station System [RSSS]
KRS	Site Radiation and Meteorological Monitoring System [SRMMS]
KRT	Plant Radiation Monitoring System [PRMS]
KSC	Main Control Room System [MCRS]
LDP	Large Display Panel
MCM	Main Computerized control Mean
MCR	Main Control Room
M-NET	Management Network
NI	Nuclear Island
NPP	Nuclear Power Plant
OWP	Operator Workplace
PAMC	Post-Accident Monitoring Cabinets
PAMS	Post-Accident Monitoring System
PLC	Programmable Logic Controller
PSAS	Plant Standard Automation System
PWR	Pressurized Water Reactor

RGL	Rod Position Indication and Rod Control System [RPICS]
RIC	In-core Instrumentation System [IIS]
RPC	Reactor Protection Cabinet
RPN	Nuclear Instrumentation System [NIS]
RPS	Reactor Protection System
RSS	Remote Shutdown Station
RTS	Reactor Trip System
SAC	Safety Automation Cabinet
SAS	Safety Automation System
SBO	Station Black Out
SCID	Safety Control and Information Device
SFC	Single Failure Criterion
SHP	Severe accident Human interface Panel
S-NET	System Network
SPC	Signal Pre-processing Cabinet
SSCs	Structures, Systems and Components
SSR	Specific Safety Requirements
TGCS	Turbine Generator Control System
TSC	Technical Support Center
UK HPR1000	The UK Version of the Hua-long Pressurized Reactor
UPS	Uninterrupted Power Supply
VDA	Atmospheric Steam Dump System [ASDS]
VDU	Visual Display Unit

System codes (XXX) and system abbreviations (YYY) are provided for completeness in the format (XXX [YYY]), e.g. Turbine Supervisory System (GME [TSS]).

8.2 I&C Introduction

This chapter supports the following high level objective: the design and intended construction and operation of the UK Version of the Hua-long Pressurized Reactor (UK HPR1000) will protect the public by providing multiple levels of defense to fulfil the fundamental safety functions (reactivity control, fuel cooling and confinement of radioactive material).

This chapter will demonstrate the following: the Instrumentation & Control systems support the Structures, Systems and Components (SSCs) in performing their required duties, and enable the detection of potentially dangerous faults or conditions to allow appropriate safety actions.

The safety design of Hua-long Pressurized Reactor under construction at Fangchenggang nuclear power plant unit 3 (HPR1000 (FCG3)) is based on the theory of "Deterministic safety assessment as the main means, probability safety assessment as an auxiliary means" as the overall design concept. On the basis of the safety requirements of determinism, Probabilistic Safety Assessment is used to build the failure model of I&C systems. It is a verification analysis process for the I&C system design, as one part of the safety analysis of overall safety objective of the plant, to support the overall safety objective improvement.

The high level claims as following demonstrate how HPR1000 (FCG3) Instrumentation and Control (I&C) supports the As Low As Reasonably Practicable (ALARP) targets:

- The HPR1000 (FCG3) I&C design scheme satisfies the requirements in related codes and standards. It also satisfies the safety requirements and function requirements of HPR1000 (FCG3) power plant.
- The I&C platforms and equipment adopted in HPR1000 (FCG3) meet related I&C function requirements.
- The I&C systems support the SSCs in performing their required duties, and enable the detection of potentially dangerous faults or conditions to allow appropriate safety actions.

The UK HPR1000 I&C will be designed based on I&C design of HPR1000 (FCG3). However, the design for the UK HPR1000 for the Generic Design Assessment (GDA) has not been declared and consequently no detailed UK HPR1000 design information is available at this time, the detailed information will be presented in later stages. So this chapter only describes Hua-long Pressurized Reactor under construction at HPR1000 (FCG3). The UK HPR1000 I&C design will be based on the HPR1000 (FCG3), as described in chapter 1.

This chapter provides a summary of the I&C systems important to safety included in the HPR1000 (FCG3) design, together with the approach to safety Function Category (FC), I&C system safety classification, the design principles and related standards. The

following systems to support the overall objectives will be introduced in this chapter:

- Reactor Protection System (RPS).
- Post-Accident Monitoring System (PAMS).
- Safety Automation System (SAS).
- Plant Standard Automation System (PSAS).
- Diversity Driven System (KDS [DAS]).
- Severe Accident I&C System (KDA [SA I&C]).
- Other I&C systems (Nuclear Instrumentation System (RPN [NIS]), In-core Instrumentation System (RIC [IIS]), Rod Position Indication and Rod Control System (RGL [RPICS]), Plant Radiation Monitoring System [RMS], Turbine Generator Control System (TGCS), Site Radiation and Meteorological Monitoring System KRS [SRMMS], etc.).
- Balance of Plant (BOP) I&C systems.
- Human Machine Interface (HMI).

8.2.1 Background

HPR1000 (FCG3) is an evolutionary, advanced Pressurized Water Reactor (PWR) nuclear power technology developed according to Chinese Nuclear Safety Regulations (HAF), International Atomic Energy Agency (IAEA) Specific Safety Requirements (SSR), and the post-Fukushima safety requirements. The I&C systems for the HPR1000 (FCG3) are designed in accordance with relevant international standards including Institute of Electrical and Electronics Engineers (IEEE), International Electrotechnical Commission (IEC) and the latest IAEA guidance. The I&C systems adopt proven technology and have evolved from mature designs that have been implemented by other reactor types of China General Nuclear Power Corporation such as the Advanced Chinese Pressurized Reactor 1000 (ACPR1000). For example, a Diverse Actuation System (KDS [DAS]) has been introduced (in ACPR1000) to provide diverse means of protection in case of software Common Cause Failure (CCF) in the RPS. The KDA [SA I&C] with a 12-hour battery back-up power supply has been introduced (in ACPR 1000) to take the lessons learned from the Fukushima accident.

The HPR1000 (FCG3) I&C functions are mainly implemented in four different I&C platforms, which are FirmSys platform, HOLLiAS-N platform, SpeedyHold platform and FitRel platform. These platforms have passed a rigorous qualification process based on relevant international standards. They have been applied in many other Nuclear Power Plant (NPP) units in China. For instance, FirmSys platform has been applied to 6 ACPR1000 units (Hong Yan He Units 5 & 6, Yang Jiang Units 5 & 6 and Tian Wan Units 5 & 6) and two HTR units (Shi Dao Wan units 1&2), HOLLiAS-N platform has been applied to 17 units with good operational records.

8.2.2 Structure of the Document

Chapter 8 presents the main design of the I&C system of HPR1000 (FCG3). By introducing the general structure, function requirements, design basis and safety evaluation of I&C system, it is indicated that the design of the I&C system of the NPP conforms to the safety-related laws, codes and standards.

Chapter 8 mainly contains the following contents:

- Sub-chapter 8.3 design principles for I&C.
- Sub-chapter 8.4 general architecture of I&C systems.
- Sub-chapter 8.5 general description of FC1 I&C systems.
- Sub-chapter 8.6 general description of FC2 I&C systems.
- Sub-chapter 8.7 general description of FC3&NC I&C systems (PSAS).
- Sub-chapter 8.8 general description of severe accident I&C system.
- Sub-chapter 8.9 general description of diverse actuation system.
- Sub-chapter 8.10 general description of control room system.
- Sub-chapter 8.11 PSR Conclusions.
- Sub-chapter 8.12 references.

8.2.3 I&C Function

The HPR1000 (FCG3) I&C design adopts Digital Control System (DCS) which includes F-SC1 DCS and F-SC3&NC DCS. However, conventional analogue technology and other diverse technology are adopted as a diversified method for safety purposes.

The I&C systems involves three main safety functions:

- Control of reactivity.
- Removal of heat from the reactor and from the fuel store.
- Confinement of radioactive material.

by means of the following actions:

- Monitor the plant to provide the necessary information, during normal operation, anticipated operating incidents and accidents.
- Maintain the operating parameters of process systems or equipment within the stipulated limits of the operating condition.
- Initiate protection actions, engineered safety measures and other post-accident mitigation measures to ensure the power plant reach a controlled and safe shutdown state and to limit radioactive release to the environment in abnormal

conditions or accidents.

8.3 Design Principles for I&C

8.3.1 Single Failure Criterion

Single Failure Criterion (SFC) is applied to a system so that it is capable of performing its safety tasks with the presence of any single failure. The SFC has been taken into account in the design of FC1/FC2 systems by ensuring a sufficient degree of redundancy, adequate independence/diversity and physical and electrical separation. The SFC is applied to FC1/FC2 systems in HPR1000 (FCG3) project, including the Reactor Trip System (RTS), the Engineered Safety Feature Actuation System (ESFAS), the SAS and the PAMS.

8.3.2 Redundancy Criterion

Redundancy design provides alternative (identical or diverse) SSCs, so that anyone can perform the required function regardless of the state of operation or failure of any other.

Considering the SFC and the system functional design requirement，the FC1/FC2 systems adopt reasonable redundancy design in HPR1000 (FCG3). For example, the RTS is equipped with four independent protection channels (channel I, II, III, IV), and the ESFAS and SAS are both equipped with three independent trains (train A, B and C).

In addition, some FC3 systems such as KDA [SA I&C] and Plant Computer Information and Control System (KIC [PCICS]) also adopt redundancy design.

8.3.3 Independence Criterion

Independence criterion requires equipment to possess both of the following characteristics:

1) The ability to perform its required function is unaffected by the operation or failure of other equipment.

2) The ability to perform its function is unaffected by the occurrence of the effects resulting from the postulated initiating event for which it is required to function.

The safety I&C system design of HPR1000 (FCG3) meets the independence criterion by means of physical separation, electrical isolation and communication isolation.

a) Physical separation

The four independent channels of the RTS are respectively located in four rooms corresponding to different fire-resistance zones. The redundant trains of the ESFAS, SAS and PAMS are also respectively located in rooms corresponding to different fire-resistance zones to meet the requirements of physical separation.

In the same train or channel, separation between FC1/FC2 I&C systems and FC3/NC I&C systems, is realized by distance, or by barriers. If the separation cannot be performed

in some exceptional situations, the qualification class of F-SC3/NC equipment should be enhanced to prevent it from affecting F-SC1/F-SC2 equipment.

b) Electrical isolation

Data exchange between different safety systems and between FC1/FC2 and FC3/NC systems uses both network and hardwired links. For network links, fiber optic cables are used for electrical isolation. For hardwired links, relays or other isolation modules are used.

c) Communication isolation

Data communication isolation between different channels or trains in FC1/FC2 I&C systems, or between FC1/FC2 I&C systems and FC3/NC I&C systems is provided. As a result, failures in the communication links cannot cause the loss of safety functions. What's more, a failure in one communication network does not affect the functions of another network in redundant configuration.

Protection systems and control systems must not interfere with one another. Interconnections between functions of different categories are implemented to ensure that failure in a lower category function cannot affect the higher category functions unless specific justification is provided.

8.3.4 Diversity Criterion

Diversity means the existence of two or more different ways or means of achieving a specified objective. Diversity is specifically provided as a defense against CCF. It may be achieved by providing systems that are physically different from each other or by functional diversity, where similar systems achieve the specified objective in different ways.

Diversity in the design of the I&C systems of HPR1000 (FCG3) includes functional diversity, signal diversity, equipment diversity and different design schemes, to reduce the risk of CCFs, for example:

- I&C functions are performed in four different I&C platforms.
- The RPS measures and processes, where possible, two diverse process variables for each reactor trip function under Design Basic Condition -2 (DBC-2).
- When RPS becomes unavailable due to CCFs of software, the KDS [DAS] can perform the needed functions.
- Conventional operation equipment with manual trip and engineered safety features actuation are adopted.

8.3.5 Fail Safe Criterion

FC1/FC2 I&C systems in HPR1000 (FCG3) are designed in accordance with fail safe criterion. The system output can be placed in safe state or proved acceptable state when

components fail or lose the power source.

When the trip channel fails, and if the remaining trip channels cannot meet the SFC, reactor trip signal will be generated to realize safe shutdown. While the fail-safe position of the ESFAS is generally maintained at the current position.

8.3.6 Periodic Test Requirement

In HPR1000 (FCG3), the FC1/FC2 I&C systems are designed to permit periodic testing in order to confirm their ability to perform their required functions. Periodic tests for instrument channels, processing equipment and actuators can be respectively carried out in different stages, but there shall be certain overlapping to ensure overall completeness. During the periodic test, it will not hinder executing the safety functions.

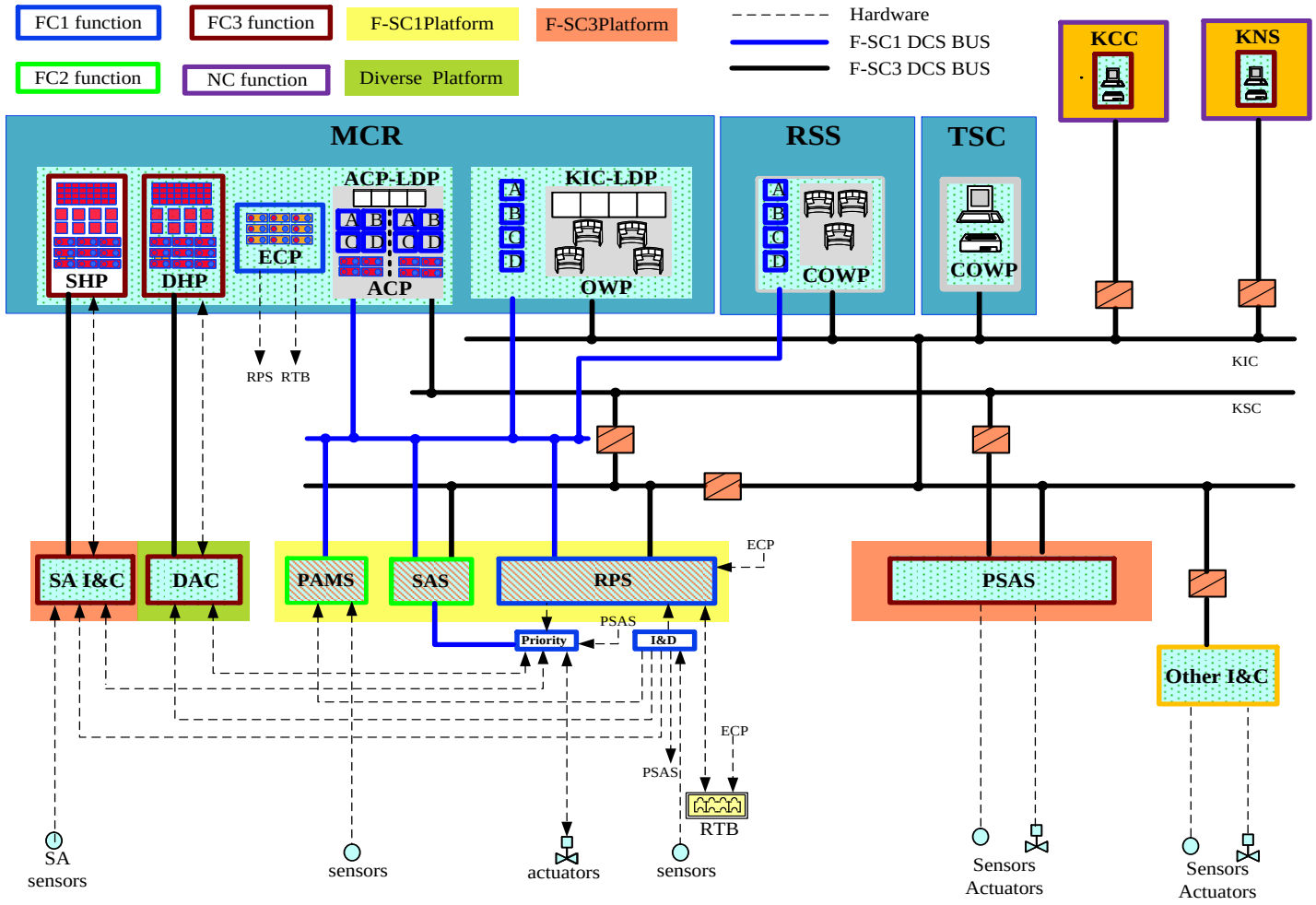
The periodic test requirement for the FC3/NC I&C systems depends on the specific functional requirements.

8.4 General Architecture of the I&C Systems

In HPR1000 (FCG3) design, I&C systems are used to implement reactor protection, plant operation and control functions, based on four platforms: FirmSys, HOLLiAS-N, SpeedyHold and FitRel. Detailed information about I&C overall architecture based on I&C platforms will be sent in a separate file. The I&C functions are classified into four categories: FC1, FC2, FC3 and NC. The qualification and quality assurance requirements for software and hardware of I&C platforms should meet the requirements of related codes and standards.

8.4.1 Periodic Test Requirement

The overall structure of the digital I&C adopted by HPR1000 (FCG3) is as shown in F-8.4-1.



I&D: Isolation and Distribution

F-8.4-1 Overall I&C Structure Chart

8.4.2 I&C Level Introduction

The vertical structure of I&C consists of four levels:

- Process system interface level (level 0).
- Automatic control and protection level (level 1).
- Operation and information management level (level 2).
- Plant information management level (level 3).

8.4.2.1 Process System Interface Level (level 0)

This level is composed of sensors, actuators and other local equipment on site.

8.4.2.2 Automatic Control and Protection Level (level 1)

This level provides functions including signal acquisition and pre-processing, logic processing, control arithmetic calculation, data communication, etc.. This level includes RPS, PAMS, SAS, PSAS, KDS [DAS], KDA [SA I&C], other I&C systems and the BOP I&C systems. RPS, SAS and PAMS belong to F-SC1 DCS. PSAS belongs to F-SC3&NC DCS. Interfaces between systems in different safety classes are separated by communication isolation for network links and by electrical isolation for hardwired links.

a) RPS

The RPS is to cope with design basis accidents. When protection parameters reach or exceed set points, the system triggers reactor trip and triggers the engineered safety features and other post-accident mitigation measures to ensure that the power plant reaches a controlled state. The RPS consists of the RTS and the ESFAS.

- RTS

  The RTS acquires and processes the signals to achieve automatic reactor trip function and send the relevant parameters and other information via network to control rooms for indication and alarm.

  The RTS includes four redundant independent channels, and each channel consists of two groups. To achieve function diversity, the reactor trip parameters will be allocated to the two groups, in order to prevent CCF. Each group is able to trigger reactor trip signal.

- ESFAS

  The ESFAS implements the control functions of engineered safety feature and supporting systems. It transmits related parameters and other information to control rooms via network to control rooms for indication and alarm.

  The ESFAS comprises three trains of redundant Engineered Safety Feature Actuation cabinets (ESFACs). Each train of ESFAC receives the trigger signals from

four RTS channels to actuate system-level engineered safety features based on two-out-of-four voting logic. The triggering signals for engineered safety feature actuation are sent to the SAS by network and sent to the Component Interface Cabinets (CICs) by hardwire.

The RPS also includes the Signal Pre-processing Cabinets (SPCs), CICs and Data Transmission Cabinets (DTCs). The SPC is the interface between the Reactor Protection Cabinet (RPC) and plant sensors, which performs signal pre-processing, separation and distribution functions. The CIC is used as the interface between the ESFAC and actuators for signal priority management. The DTC is used to perform data transmission function.

b) SAS

The SAS comprises of three trains of Safety Automation Cabinets (SACs). It implements the control function required to bring the power plant from controlled state to safe shutdown state.

c) PAMS

The PAMS performs the post-accident monitoring function, including two trains of redundant and independent Post-Accident Monitoring Cabinets (PAMCs). It monitors the primary and secondary loop parameters, such as pressure, temperature, flowrate and the water levels in the pressurizer and steam generators under accident and post-accident conditions.

d) PSAS

PSAS monitors and controls the plant in normal operational conditions. In addition, PSAS can maintain the main power plant parameters within the normal operational range to avoid triggering a reactor trip or engineered safety features actuation during operation transients.

e) KDS [DAS]

The KDS [DAS] is designed to bring the NPP to a final state in the event of software CCF in RPS and SAS with a concurrent high-frequency initiating event. The KDS [DAS] uses another technology which is different from the protection system, to make it diverse from the protection system. The KDS [DAS] provides diverse tripping by cutting the power supply of control rod drive mechanism.

f) KDA [SA I&C]

The KDA [SA I&C] performs the Design Extension Condition-B (DEC-B) functions needed in the event of a total loss of power (loss of off-site power, emergency diesel generators and Station Black Out (SBO) diesel generators).

g) Other I&C system

The other I&C systems include the following systems:

- Nuclear Instrumentation System (RPN [NIS])

The RPN [NIS] provides neutron detectors to continuously monitor the changes of the reactor power level and power distribution. The detectors of RPN [NIS] are installed outside the reactor pressure vessel to measure the neutron flux.

- In-core instrumentation system (RIC [IIS])

The RIC [IIS] provides measurement data like reactor core neutron flux distribution, fuel assembly outlet coolant temperature, and pressure vessel water level. The assemblies are installed inside the reactor pressure vessel.

- Rod Position Indication and Rod Control System (RGL [RPICS])

The RGL [RPICS] is used to insert and withdraw the control or shutdown rod control cluster assemblies, and to monitor the position of each control rod assembly. The RGL [RPICS] is composed of the rod control system and the rod position indication system. The rod control system is to adjust the core reactivity by control rod control cluster assemblies automatically or manually. The rod position indication system is to provide the measured position for each rod control cluster assemblies.

- Plant Radiation Monitoring System (KRT [RMS])

The KRT [RMS] includes the process radiation monitoring subsystem, area radiation monitoring subsystem, effluent radiation monitoring subsystem and post-accident monitoring subsystem.

- Turbine Generator Control Systems (TGCS)

The TGCS is composed of Turbine Governing System (GRE [TGS]), Turbine Protection System (GSE [TPS]), Turbine Supervisory System (GME [TSS]), and Generator Excitation and Voltage Regulation System (GEX [GEVRS]), which respectively achieve the turbine control, protection, monitoring and generator regulations etc..

- Site Radiation and Meteorological Monitoring System (KRS [SRMMS])

The KRS system continuously monitors site area environmental γ radiation data and meteorological parameters, and collects the samples of liquid effluents and various environmental media.

h) BOP I&C system

The BOP I&C generally adopts Programmable Logic Controller (PLC) to achieve their control functions. Normally few signals exchanged with the DCS by hardwire or network interfaces.

8.4.2.3 Operation and Information Management Level (level 2)

The Operation and information management level is designed on the basis of digital

human interfaces. Its functions include information support, diagnosis, equipment control, operation log and so on. It comprises equipment deployed in the Main Control Room (MCR), the Remote Shutdown Station (RSS), and the Technical Support Center (TSC). Please refer sub-chapter 8.10 for details.

8.4.2.4 Plant Information Management Level (level 3)

This level includes the Real-time Information Monitoring System (KNS [RIMS]) and Nuclear Accident Emergency Management System (KCC [NAEMS]).

This level is mainly responsible for non-real-time functions and comprehensive information processing of the whole plant and receiving some necessary information of the plant through network interface equipment to help managers (plant managers, superior administrative authorities, national emergency center or relevant safety authorities) get knowledge of the status of the plant. The transmission of information is unidirectional. The operation and information management network is connected to the plant level network or the remote network by gateways, to provide relevant on-site and off-site units and departments with main information on the nuclear power unit operation. Specific function and specification design shall be subject to the plant management requirements.

8.4.3 Categorization of I&C Functions and Equipment

I&C equipment which is important to safety should be consistent with their safety function categories. That is, SSCs that fulfil safety category 1 functions (FC1) should be function class 1 items (F-SC1). SSCs that fulfil safety category 2 functions (FC2) should be function class 2 items (F-SC2). SSCs that fulfil safety category 3 functions (FC3) should be function class 3 items (F-SC3). Please refer to sub-chapter 4.7 for safety classification principle. If an I&C equipment fulfils multiple functions, its classification depends on the function with the highest category. The correlation between function category and equipment classification is shown in the following table.

T-8.4-1 Correlation Between Function Category and Equipment Classification

Function Category	FC1	FC2	FC3	NC
Equipment Classification	F-SC1	F-SC2	F-SC3	NC

In actual equipment selection, a safety function at a lower safety category can be realized in equipment at higher safety classification. Functions category, safety classification and seismic category of the I&C systems of HPR1000 (FCG3) are shown in the following table.

T-8.4-2 System Function and Equipment Classification

Systems Code	Name	Function Category	Equipment Classification	Seismic Category
PSAS	Plant Standard Automation System	FC3/NC	F-SC3/NC	seismic category 1 (SSE1), seismic category 2 (SSE2) and NO
RTS	Reactor Trip System	FC1	F-SC1	Seismic category 1 (SSE1)
ESFAS	Engineered Safety Feature Actuation System	FC1	F-SC1	Seismic category 1 (SSE1)
SAS	Safety Automation Unit	FC2	F-SC1	Seismic category 1 (SSE1)
PAMS	Post-Accident Monitoring System	FC2	F-SC1	Seismic category 1 (SSE1)
DAS	Diverse Actuation System	FC3	F-SC3	Seismic category 1 (SSE1)
SA I&C	Severe Accident I&C System	FC3	F-SC3	Seismic category 1 (SSE1)

8.4.4 I&C Defense in Depth

The I&C Defense in Depth structure of HPR1000 (FCG3) consists of 5 independent defense levels.

a) Level 1 – prevention line: PSAS

The prevention line detects and corrects transient events or system failures that deviate from normal operating to prevent emergency events from causing accidents.

b) Level 2 – main defense line: RPS + SAS

The main defense line is to enable accident mitigation measures to mitigate the consequences of DBC 2-4 accidents so as to avoid severe accidents and radioactive substance leakage. The RPS is to perform all FC1 functions for ensuring a controlled state. The SAS is to perform the safety functions from the controlled state to safe shutdown state.

c) Level 3 – diverse defense line: DAS

The diverse defense line is to bring the NPP to the final state following the software CCF in RPS and SAS with a concurrent high-frequency initiating event.

d) Level 4 – severe accident defense line: SA I&C

The severe accident defense line performs the DEC-B functions needed in the event of a total loss of power (loss of off-site power, emergency diesel generators and SBO diesel generators).

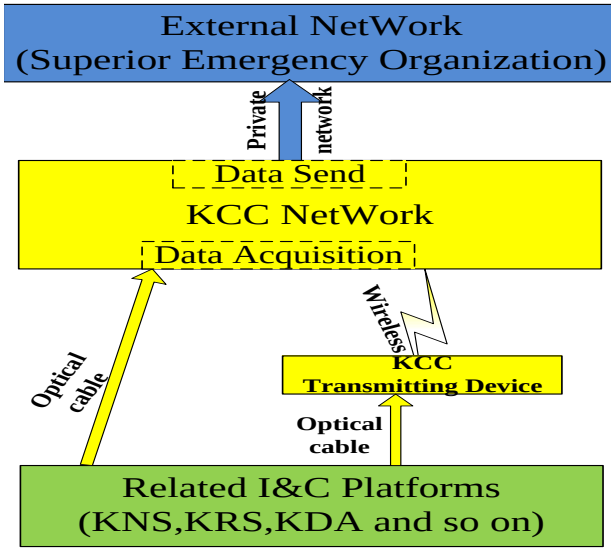
e) Level 5 – emergency response line: KCC [NAEMS]

The emergency response line is to mitigate the consequences of radioactive release that could potentially result from accidents.

The KCC [NAEMS] is deployed in on-site emergency control center. KCC [NAEMS] collects the plant operating parameters, equipment state parameters and environmental radiation monitoring data from the KNS [RIMS], KRS [SRMMS], KDA [SA I&C] and so on. As shown in F-8.4-2, KCC [NAEMS] provides the information and technical support for the on-site emergency management. On the other hand, it is able to send information to the superior nuclear emergency organizations, and assist the off-site emergency response.

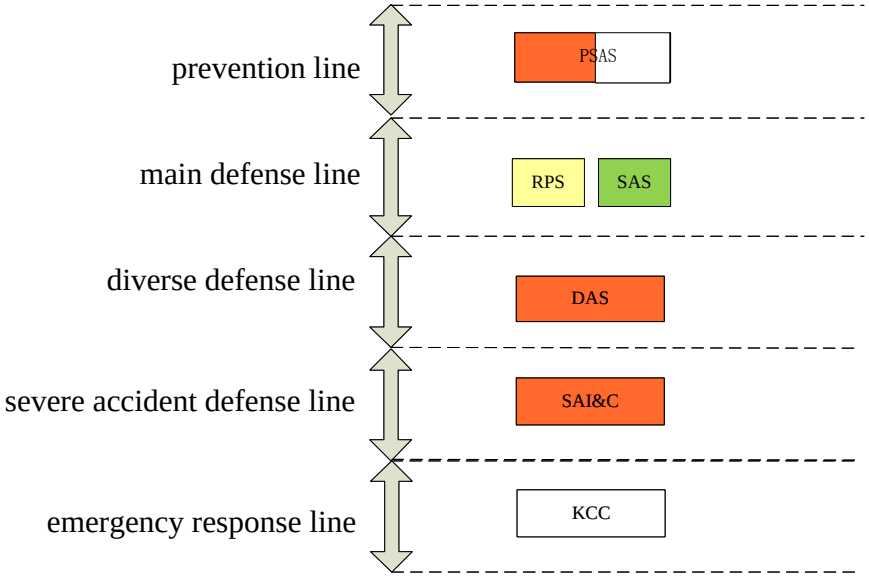
In order to assure the system availability in emergency situation, the important equipment are available under seismic condition. These equipment are also powered by diesel generator in on-site emergency control center, to keep them available for 7 days during emergency event.

What's more, in the situation when optical fiber link is interrupted and cannot be recovered, KCC [NAEMS] can also get the needed important plant information by wireless link.



F-8.4-2 Overview of the KCC [NAEMS] Architecture

The I&C Defense in Depth level is shown in F-8.4-3.



F-8.4-3 I&C Defense in Depth Level

8.4.5 I&C Equipment Layout

Specific factors such as physical separation, transportation, installation, maintenance convenience, and expandability have been taken into account in I&C equipment layout.

Separated and independent Heating, Ventilation and Air Conditioning systems (HVAC) are equipped for different I&C rooms. The basic layout schemes are as follows:

a) DCS equipment layout

The DCS equipment in HPR1000 (FCG3) are arranged in different buildings: the NI DCS equipment are mainly arranged in the NI safeguard buildings and nuclear auxiliary buildings while the CI and BOP DCS equipment are mainly arranged in the turbine buildings and CI electrical buildings.

b) Other I&C equipment layout

Other I&C equipment (such as RPN and RIC) is respectively deployed in corresponding safeguard buildings. TGCS cabinets are deployed in CI buildings.

c) BOP control system layout

The BOP control systems are deployed in corresponding local control rooms or buildings.

8.4.6 I&C Equipment Power Supply

The power supply of different I&C equipment is configured based on the safety classification, functional requirement and availability of the equipment.

In general, redundant power supply (with 2-hour Uninterrupted Power Supply (UPS)) is configured for I&C equipment. Special power supply (with 12-hour UPS) is provided for

the equipment required in severe accidents. I&C equipment in different buildings or trains are power supplied by different electric systems in corresponding buildings or trains.

8.4.7 Seismic Requirement

The seismic category of I&C equipment is determined according to its functions, and the seismic category principle of HPR1000 (FCG3) is described in sub-chapter 4.7.6.

The seismic category of F-SC1, F-SC2 and partial F-SC3 items is SSE1.

The seismic category of non-SSE1 equipment should be SSE2 if any internal hazards resulting from an earthquake could cause an unacceptable effect on SSE1 equipment.

The seismic category of other equipment is NO.

8.4.8 I&C Equipment Qualification

The equipment qualification of F-SC3 and NC I&C equipment is in accordance with general industry standards.

The standards of equipment qualification of F-SC1 and F-SC2 I&C equipment are shown in the following table.

T-8.4-3 Standards of Equipment Qualification

Test Classification	Standards	Items	Rev
Overall	IEC 61513	Instrumentation and control systems important to Safety-General requirement	2011
	IEC60780	Nuclear power plants Electrical equipment of the safety system Qualification	1998
Environmental test	IEC60068-2-1	Environmental testing for electric and electronic products----Part 2 Test method Test A:Clod	2007
	IEC60068-2-2	Environmental testing for electric and electronic products----Part 2 Test method Test A:Dry hot	2007

Test Classification	Standards	Items	Rev
	IEC60068-2-30	Environmental testing for electric and electronic products----Part 2 Test method Test Db：Damp heat, cyclic	2005
	IEC60068-2-6	Environmental testing for electric and electronic products----Part 2 Test method Test Fc: Vibration(sinusoidal)	1995
	IEC60068-2-6	Environmental testing for electric and electronic products ---- Part 2 Test method Test N:Change of temperature	2009
	EPRI TR-107330	generic requirements specification for qualifying a commercially available PLC for safety-related applications in nuclear power plants	1996
Electromagnetic compatibility	RG1.180	Guidelines for Evaluating Electromagnetic and Radio ---- Frequency Interference in Safety-Related Instrumentation and Control Systems	2003
	IEC62003	Nuclear Power Plant ---- Instrumentation and Control Important to Safety ---- Requirements for Electromagnetic Compatibility Testing	2009
Seismic qualification test	IEC60980	Seismic qualification of electrical equipment of the safety system for nuclear power plants	1988
Software Verification and Validation	IEC60880	Nuclear power plants ---- Instrumentation and control systems important to safety –Software aspects for computer-based systems performing category A functions	2006

Test Classification	Standards	Items	Rev
	IEC62138	Nuclear power plants ---- Instrumentation and control important for safety ---- Software aspects for computer-based systems performing category B or C functions	2004

8.4.9 I&C Cyber Security Requirements

I&C systems (both hardware and software) for the HPR1000 (FCG3) shall be designed so that they are free from vulnerabilities that may affect the reliability of the system. Vulnerabilities are considered to be deficiencies in the design that may allow inadvertent, unintended, or unauthorized access or modifications to the safety system.

Cyber security design of I&C systems of HPR1000 (FCG3) refers to the requirements in RG 1.152, RG 5.71, IEC 62645 and relative codes and standards in China.

Cyber security of I&C system adopts technical and managing measures to achieve the security aim. Cyber security will be considered in the lifetime of the I&C system.

8.4.10 Reliability

The reliability of DCS functions depends on the implementation of the deterministic design requirements and the intrinsic reliability required for DCS systems and equipment which perform these functions.

The reliability required for DCS system and equipment is based on the following approaches:

- For hardware, the reliability of the function is estimated in a quantitative way such as the failure rate of DCS components and a failure mode analysis.
- For software, the reliability of the function is estimated in a qualitative way, such as the evaluation of the design complexity, the development quality and relevant experience feedback, etc..

Redundancy and fault tolerance measures should be taken to guarantee the execution of automatic actions in case of the plant availability decrease. For example, the main control and monitoring functions need to be allocated in different processors.

8.5 General Description of FC1 I&C Systems

8.5.1 Safety Requirements

The RPS is subject to safety requirements applicable to FC1 I&C systems, due to its management of those protection functions including: reactor trip, engineering safety features actuation functions and so on.

8.5.1.1 Safety Functions

The RPS contributes to ensuring three main safety functions:

- Control of reactivity.
- Removal of heat from the reactor and from the fuel store.
- Confinement of radioactive material.

8.5.1.2 Design Requirements

a) Single failure criterion

The RPS should satisfy the SFC which requires a sufficient degree of redundancy. In addition the RPS fulfils the following specific design rules:

- A single failure and all the failures caused by the single failure should not disable the safety features.
- The redundant channels and trains are physically and electrically separated from each other to guarantee the availability of the left redundancy in case of a loss of one channel or train.

b) Emergency power supply

The power supply of RPS is backed-up by an uninterruptible power system and the emergency diesel generators. The I&C functions of RPS are kept available in case of the loss of the external power supply.

c) Qualification

Qualification of RPS equipment must demonstrate the functional availability under the specified environmental conditions. Detailed qualification requirements are listed in sub-chapter 8.4.8.

d) Hazards

The I&C equipment of the RPS must be protected against the damaging effects resulting from internal or external hazards defined in chapter 18 and 19.

8.5.1.3 Periodic test

The safety classified I&C features should be subject to a combination of self-diagnosis and periodic tests to detect the failures or performance degrading of the system or devices. Tests frequency is defined based on the reliability analysis of the tested part. The RPS is designed to allow periodic tests.

8.5.2 Role of the System

The RPS mainly implements safety classified I&C functions such as automatic, manual and monitoring functions.

The RPS mainly fulfils the following I&C Functions:

- Automatic reactor trip and turbine trip.
- Automatic start of ESFAS and control of related supporting systems.
- Providing alarms and plant data for detection of situations which require operator's manual actions.
- Generation of permissive signals.
- Manual actuation of FC1/FC2 I&C Functions.

8.5.3 Design Basis

8.5.3.1 Redundancy

Redundant channels of RTS and trains of ESFAS are necessary to satisfy SFC during maintenance, and reduce the risk of spurious actuation.

8.5.3.2 Independence

The RPS is designed not to be affected by the other I&C systems with a lower safety classification and each part of the RPS is also designed not to be affected by the lower safety classification parts of the RPS. The following criteria shall be met:

- Independency between RPS and the other I&C systems.
- Independency between redundant channels and trains of the RPS.
- Independency between the equipment of different safety classification in RPS.
- Independency between diverse protection functions.

8.5.3.3 Diversity

The design of the RPS complies with the diversity principle.

The RPS is backed up by a diverse I&C system which is presented in sub-chapter 8.9.

In addition, two diverse protection variables for reactor trip where as far as possible is designed for each DBC-2 event.

8.5.3.4 Availability Requirements

In case of an equipment failure in one channel or train, the safety features required for the DBC events are still available and the risk of spurious actuation of actuators should be minimized as far as possible.

8.5.3.5 Environment Requirements

The components of RPS are qualified to be able to operate in the normal environment conditions and to remain functional under the post-accident conditions.

8.5.3.6 Completion of Protective Action

The safety systems shall be designed so that, once triggered automatically or manually, the intended sequence of protective actions shall continue until they are completed. Deliberate operator action shall be required to put the safety systems back to normal state.

8.5.3.7 Human Machine Interface Requirements

The RPS is equipped with an engineering HMI to enable safe and effective commissioning, maintenance, periodic tests and configuration.

The RPS is also equipped with operational HMI, which is described in sub-chapter 8.10.

8.5.4 System Description and Operation

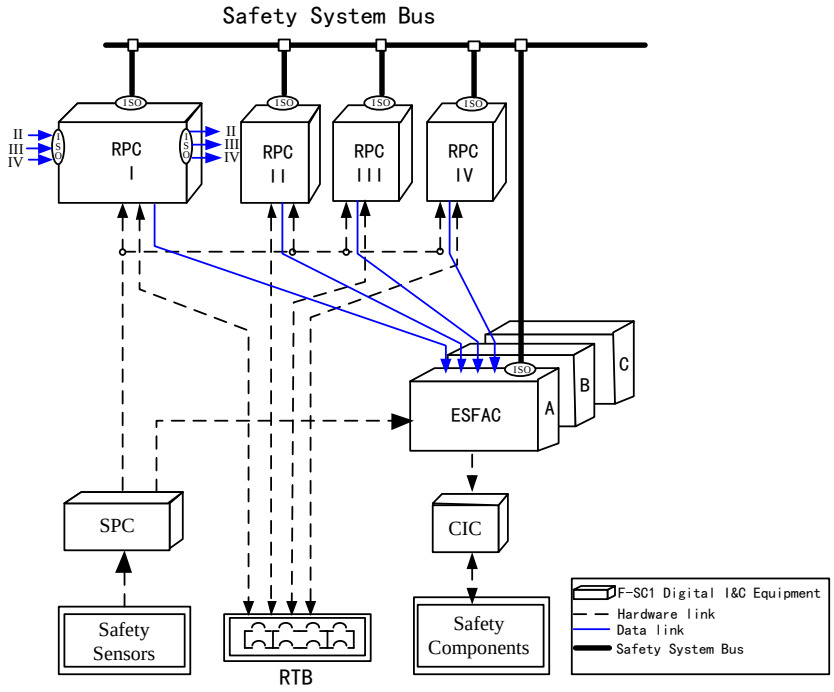
The RPS implements those I&C functions required to bring the plant to the controlled state after DBC2-4 events, and to maintain the state as long as possible. The main FC1 classified I&C Functions implemented by RPS includes:

- Reactor trip: to enable all rods to fall into the reactor core under gravity.
- ESFAS I&C functions: to actuate the engineered safety features such as safety injection, containment isolation and so on.
- ESFAS closed loop control I&C functions: FC1 closed loop controls such as regulation of main steam relief control valves in Atmospheric Steam Dump System (VDA [ASDS]), flow limitation control valves in Emergency Feedwater System (ASG [EFWS]) and so on.
- Permissive signals: The RPS generates permissive signals to authorize the protection channel according to the plant state.

The RPS also performs some FC2 functions such as FC2 manual controls including memory reset, manual actuation and so on.

As shown in F-8.5-1，RPS mainly includes the following digital I&C system components:

- RPCs: RPCs consist of a four-fold redundant structure, four protection channels: IP, IIP, IIIP, and IVP.
- ESFACs: ESFACs consist of a three-fold structure: train A, train B and train C.
- SPCs: SPCs consist of 4 independent channels.
- CICs: CICs perform component-level control logic, including local operation and priority management logic for safety actuators.



F-8.5-1 Architecture of RPS

The RPS exchanges information with the following systems:

- The HMI: for plant operation and monitoring by the operators.
- The SAS: for the function authorization management in the post accidents.
- The PSAS: for some information indication, control function interlocks and periodic tests data transfer.
- The "external" systems (I&C cabinets for the diesels, RPN, Turbine I&C etc.): for the function management of those external systems.

8.5.5 Preliminary Design Substantiation

8.5.5.1 Equipment Classification

The equipment of the RPS is classified as F-SC1. For detailed information, please refer to sub-chapter 8.4.3.

8.5.5.2 Seismic Category

The equipment of the RPS complies with the requirements of SSE1. For detailed information, please refer to sub-chapter 8.4.7.

8.5.5.3 Power Supply

Refer to sub-chapter 8.4.6.

8.5.5.4 Environment Requirements

RPS has the capability to work under the environmental conditions in the I&C rooms of the safeguard building.

8.5.5.5 Maintenance

By-pass function is provided which allows the RPS to be maintained online, in order to meet the SFC.

8.5.5.6 Periodic Test

The periodic test of RPS can be subdivided into several test segments. The test segments are carried out in an overlap manner to ensure the periodic test can cover the entire scope of RPS.

8.6 General Description of FC2 I&C Systems

8.6.1 Safety Automation System (SAS)

8.6.1.1 Safety Requirements

The SAS is subject to safety requirements applicable to FC2 I&C systems. The SAS performs the processing functions of automatic and manual actions, together with the associated monitoring functions, to bring the reactor from controlled state to safe shutdown state.

a) Safety functions

The safety functions of SAS are as the following:

- Control of reactivity.
- Removal of heat from the reactor and from the fuel store.
- Confinement of radioactive material.

b) Design requirements

- Single failure criterion

SAS is designed to meet the SFC.

The SAS will require physical and electrical independence of the equipment.

- Emergency power supply

Emergency diesel generators are equipped as backed-up power supplies for SAS. In addition, the SAS must be supplied by an uninterruptible power supply at the suitable voltage, so that it carries out its I&C functions without interruption when the external power supply is lost.

- Qualification under operating conditions

The SAS equipment located in safeguard buildings remain operational in all plant conditions, including the accident conditions. Detailed qualification requirements are listed in sub-chapter 8.4.8.

- Hazards

The I&C equipment of the SAS must be protected against the damaging effects resulting from internal or external hazards defined in chapter 18 and 19.

c) Periodic test

For SAS, periodic tests are designed to confirm the ability to perform their required functions.

8.6.1.2 Role of the System

The role of the SAS is to perform safety functions to bring the reactor from controlled state to safe shutdown state, and other FC2 functions.

The following I&C functions are performed by SAS:

- Processing of data processing.
- Processing of application calculations.
- Processing of monitoring signals.

8.6.1.3 Design Basis

a) Availability requirements

The main availability requirements for the SAS are composed of the reliability and the maintainability of the system. Redundant design is adopted to promote the reliability of the system, while maintenance methods and tests are facilitated to enhance the availability.

b) Performance requirements

For SAS, the performance requirements of the I&C functions in terms of response time and accuracy as derived from the functional requirements must be fulfiled.

c) Environment requirements

The components of SAS are qualified to be able to operate in the normal environment conditions and to remain functional under the post-accident conditions.

d) Human Machine Interface requirements

The SAS is equipped with engineering HMIs to enable safe and effective commissioning, maintenance, periodic tests and configuration.

The SAS is also equipped with operational HMI, which is described in sub-chapter 8.10.

8.6.1.4 System Description and Operation

The SAS will achieve manual and automatic control of FC2 functions upon actuation of the corresponding process system, which is triggered by the RPS. Interfaces provided among Level 2 and the SAS are to control and monitor process systems required for safe shutdown state.

The structure and composition of SAS are decided by following the functional requirements. The set of requirements affects the allocation of I&C processing tasks to the various components within the SAS.

The SAS exchanges information with the following:

- The HMI: for plant operation by the operators.
- The PSAS and RPS: for the plant data acquisition, logic processing and actuator control.

8.6.1.5 Preliminary Design Substantiation

a) Equipment classification

The SAS comprises three trains of redundant SACs. F-SC1 DCS is adopted to realize the function of SAS. Please refer to sub-chapter 8.4.3 for detailed information.

b) Seismic category

The equipment of the SAS complies with the requirements of SSE1.

c) Power supply

Redundant power supply (with 2-hour UPS) is configured for SAS.

d) Environment requirements

SAS has the capability to work under the environmental conditions in the I&C rooms of the safeguard building.

e) Periodic test

SAS periodic test mainly aims at verifying the whole control loop, both automatic control loop and manual control loop included.

8.6.2 Post- Accident Monitoring system (PAMS)

8.6.2.1 Safety Requirements

PAMS mainly provides post-accident process parameter information and system state information to help the operators to:

- Execute the prearranged manual operation functions.
- Realize the state of NPP and the safety systems, and take appropriate actions to

deal with the abnormal events.

- Ensure NPP to reach and maintain safe shutdown state.

8.6.2.2 Role of the System

PAMS is mainly designed to perform monitoring functions for post-accident condition. It can monitor operation status for process systems that need to run during accident condition and post-accident condition, to help operators execute emergency operating procedures.

8.6.2.3 Design Basis

PAMS mainly executes FC2 functions. Referred to IEEE 497 (2010), the requirements such as single failure, CCF, independence and separation, isolation, information ambiguity calibration and testability are considered in the system design.

The variable definition, variable types and variable selection principles take reference from IEEE 497 (2010). These principles and types are the main sources of post-accident monitoring information.

8.6.2.4 System Description and Operation

PAMS receives parameters for display from RPC by network or from site by hardwire. The related parameters after the voter block in PAMC cabinet will be sent to the appropriate equipment for display, such as SCID, ACP-VDU, hardware equipment and trend recorder. The safety classification of these display equipment is consistent with their safety function categories. For example, the classification of SCID is F-SC1, because the FC1 and FC2 information are displayed on the SCID.

8.6.2.5 Preliminary Design Substantiation

PAMS is composed of two redundant independent trains, which are implemented by F-SC1 equipment. The overall architecture of PAMS is demonstrated in Figure F-8.4-1. The PAMS functions are mainly implemented by PAMC.

PAMC performs functions on voting and calculating of Type A, Type B, Type C variables. It receives signals from RPC, SAC or RIC via different routes (such as peer-to-peer transmission, network, hardware), and sends variables to ACP and KIC [PCICS] for display after voting and calculating.

Type D and Type E variables are not sent into PAMC for voting and calculating. They are sent from RPC, SAC or PSAC to ACP-VDU and KIC [PCICS] for display via network.

Type A, Type B, Type C variables which are configured with redundant A/B dual-channel are sent to PAMS A/B train respectively.

For Type A, Type B, Type C variables which are acquired from three loops, the signal of each loop are sent to both PAMS A and B trains for display. For those from the four protection channels, the signal of each channel are sent to both PAMS A and B trains, and

display after voting and calculating.

8.7 General Description on the FC3 & NC I&C Systems (PSAS)

8.7.1 Safety Requirements

The PSAS is subject to safety requirements applicable to FC3 I&C systems, due to its management of FC3 I&C Functions.

8.7.2 Role of the System

The PSAS performs FC3 and NC functions, including Nuclear Island (NI) process control, Conventional Island (CI) process control and some BOP control functions.

The general objective of plant control system is as the following:

a) Establish and maintain power balance when the plant runs in a steady state.

b) Suppress the operating transients to avoid trip of units and re-establish a steady operational state of the units.

c) Provide necessary monitoring information for the operators.

8.7.3 Design Basis

a) Availability requirements

The main availability requirements for the PSAS are composed of the reliability and the maintainability of the system. Redundant design is adopted to promote the reliability of the system, while maintenance methods and tests are facilitated to enhance the availability.

b) Performance requirements

The PSAS must fulfil the performance requirements of the I&C functions in terms of response time and accuracy as derived from the functional requirements.

c) Environment requirements

The environmental conditions that the PSAS must tolerate are defined by the temperature and relative humidity of the rooms.

d) Human Machine Interface requirements

The PSAS is equipped with an engineering HMI to enable safe and effective commissioning, maintenance, periodic tests and configuration.

8.7.4 System Description and Operation

8.7.4.1 System Description

PSAS system mainly consists of F-SC3 classified cabinets which are arranged in different rooms.

The PSAS executes the following key functions: reactor power control, reactor coolant temperature control, pressurizer pressure control, pressurizer level control, steam generator level control, and steam dump control.

Besides the functions above, the PSAS executes the control and monitoring functions including primary auxiliary systems, plant cooling water systems, HVAC systems, partial electrical systems, and so on.

8.7.4.2 System Operation

The commands from operators in MCR and feedback signals from site equipment are received by PSAS. Site operating commands will be produced after logic processing in cabinets, whilst signals acquired in site will be processed in PSAS and sent to operating station in MCR for display.

8.7.5 Preliminary Design Substantiation

8.7.5.1 Equipment Classification

The classification of the PSAS is F-SC3. Safety classification principles presented in sub-chapter 4.7 should be applied.

8.7.5.2 Seismic Category

The FC3 part of the PSAS complies with the requirements of SSE1, the NC part of the PSAS (NI part) complies with the requirements of SSE2, and the NC part of the PSAS (CI part) complies with the requirements of NO.

8.7.5.3 Power Supply

The cabinets of PSAS are equipped with redundant uninterruptible power supplies.

8.7.5.4 Environment Requirement

The equipment of PSAS shall meet the environmental conditions of I&C rooms in the safeguard building, such as requirements of pressure, temperature and humidity.

8.7.5.5 Maintenance

The PSAS is maintainable.

8.8 Severe Accident I&C System (SA I&C)

8.8.1 Safety Requirements

The KDA [SA I&C] is designed to perform DEC-B mitigating and monitoring functions. The detailed information of DEC-B is described in chapter 13.

8.8.2 Role of the System

The KDA [SA I&C] performs the DEC-B functions needed in the event of a total loss of power (loss of offsite power, emergency diesel generators and SBO diesel generators).

8.8.3 Design Basis

8.8.3.1 Function Classification

The KDA [SA I&C] processes FC3 I&C function according to the principles specified in sub-chapter 4.7.

8.8.3.2 Periodic Test

The KDA [SA I&C] is designed to allow periodic test.

8.8.3.3 Hazards

The KDA [SA I&C] should be available under seismic condition.

8.8.4 System Description

8.8.4.1 System Structure and Composition

The KDA [SA I&C] is composed of two parts:

- Severe Accident I&C Cabinets (divided into train A and train B).
- Severe accident Human interface Panel (SHP) in MCR.

KDA [SA I&C] Cabinets mainly perform the following functions:

- Signal acquisition.
- Logic processing.
- Output control orders, alarms and indication information.
- Signal exchange and communication with other I&C systems.

The SHP is located in the MCR, and includes conventional display, operation equipment and Visual Display Unit (VDU). It provides manual control for the actuators that are needed in mitigation of severe accidents. The SHP also displays the parameters and alarms related to severe accident.

8.8.4.2 Layout

The KDA [SA I&C] cabinets are located in Safeguard Buildings, while the SHP is located in MCR.

8.8.4.3 System Interfaces

a) Input

The input signals of the KDA [SA I&C] include:

- Signals of severe accident dedicated sensors and feedback signals of severe accident dedicated actuators.
- Sensors and actuators feedback signals isolated and distributed by SPC.

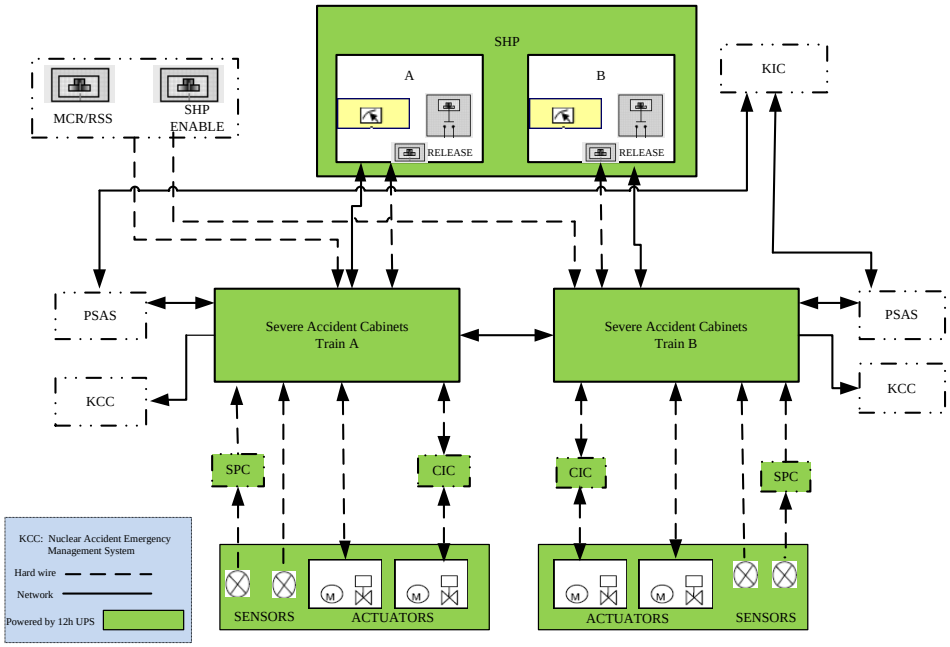
- Manual control commands from KIC [PCICS].
- SHP permission signals from MCR enable switch and RSS mode switches.

b) Output

The output signals of the KDA [SA I&C] include:

- Control commands to the actuators.
- Control commands to CIC.
- Severe accident monitoring signals to KIC [PCICS].
- Monitoring signals to KCC [NAEMS].

F-8.8-1 is the KDA [SA I&C] system architecture and interfaces diagram.



F-8.8-1 KDA [SA I&C] System Architecture and Interfaces Diagram

8.8.5 Preliminary Design Substantiation

8.8.5.1 Equipment Classification

The equipment classification of KDA [SA I&C] is F-SC3 according to the principles specified in sub-chapter 4.7.

8.8.5.2 Seismic Category

The equipment of the KDA [SA I&C] complies with the requirements of SSE1.

8.8.5.3 Power Supply

To deal with the total loss of power condition, the KDA [SA I&C] is powered by 12-hour UPS systems.

8.8.5.4 Environment Requirements

The environmental conditions that the KDA [SA I&C] must tolerate are defined by the temperature and relative humidity of the rooms. Sensors must satisfy the qualification of severe accident.

8.8.5.5 Maintenance

The KDA [SA I&C] is maintainable.

8.8.5.6 Periodic Test

The KDA [SA I&C] can be periodically tested, with online self-diagnosis capability. There shall be certain overlapping to ensure overall completeness.

8.9 General Description of Diverse Actuation System

8.9.1 Safety Requirements

8.9.1.1 Safety Functions

The KDS [DAS] is able to mitigate the consequences of Anticipated Transient Without Scram (ATWS) which is caused by the CCF of RPS and SAS, and to reach the final state of the NPP. In addition, specific measures are taken in KDS [DAS] to mitigate the consequences in case of an ATWS due to mechanical blockage of the rods.

The KDS [DAS] contributes to ensuring the three main safety functions:

- Control of reactivity.
- Removal of heat from the reactor and from the fuel store.
- Confinement of radioactive material.

8.9.1.2 Design Requirements

a) Function classification

The KDS [DAS] processes FC3 I&C function according to the principles specified in sub-chapter 4.7.

b) Single failure criterion

The SFC is not required for KDS [DAS].

c) Emergency power supply

The KDS [DAS] must be capable of operating in the event of loss of offsite power. Therefore KDS [DAS] must be equipped with UPS. The power supply provided to KDS [DAS] should be diverse from the power supply of RPS.

d) Qualification under operating conditions

The equipment of KDS [DAS] must be operational in both normal and extreme

environmental conditions. Detailed qualification requirements are listed in sub-chapter 8.4.8.

e) Hazards

The KDS [DAS] must not be affected by earthquake.

f) Periodic test

The KDS [DAS] can be periodically tested, with online self-diagnosis capability.

8.9.2 Role of the System

The KDS [DAS] is designed to bring the NPP to a final state in the event of software CCF in RPS and SAS with a concurrent high-frequency initiating event.

The KDS [DAS] mainly fulfils the following functions:

- Provide diverse actuation functions.
- Provide diverse manual actuation functions for shutdown and engineered safety actuation functions.
- Provide diverse indications for plant parameters.

8.9.3 Design Basis

8.9.3.1 Separation

The KDS [DAS] and digital protection system are mutually independent.

8.9.3.2 Availability Requirements

The KDS [DAS] must be available to operate in the event of software CCF in RPS and SAS with a concurrent high-frequency initiating event.

The availability requirements are linked to the main reliability and the maintainability of KDS [DAS].

8.9.3.3 Performance Requirements

The KDS [DAS] must meet the performance requirements in terms of response time.

8.9.3.4 Environmental Requirements

The environmental requirements of KDS [DAS] are stipulated by the relative humidity and the temperature of the room where KDS [DAS] equipment are located.

8.9.4 System Description and Operation

8.9.4.1 System Structure and System Composition

The KDS [DAS] consists of the Diverse Human interface Panel (DHP) and Diverse Actuation Cabinets (DAC).

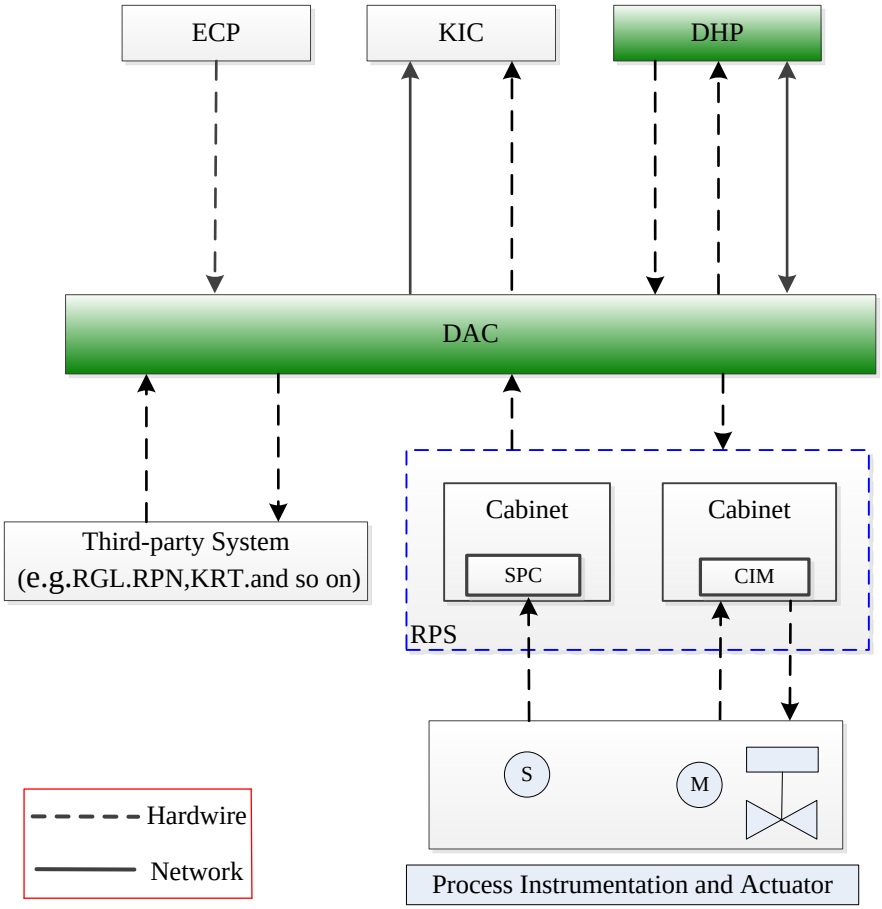
- The DAC includes acquisition, logic processing and output circuits that implement diverse automatic shutdown and engineered safety actuation functions.
- The DHP includes operation equipment, indicators, lights and alarms that are used to realize system-level manual actuation functions and necessary equipment-level manual actuation functions, as well as safety parameters monitoring function.

8.9.4.2 Layout

The DAC is located in the I&C rooms of the safeguard buildings, while the DHP is located in the MCR.

8.9.4.3 System Interface

For the system interface with external systems please see F-8.9-1.



F-8.9-1 System Interface for KDS [DAS]

8.9.5 Preliminary Design Substantiation

8.9.5.1 Equipment Classification

The equipment classification of KDS [DAS] is F-SC3 according to the principles specified in sub-chapter 4.7.

8.9.5.2 Seismic Category

The equipment of the KDS [DAS] complies with the requirements of SSE1.

8.9.5.3 Power Supply

The KDS [DAS] is designed with redundant power supplies, one of which is diverse from the power supplies of RPS.

8.9.5.4 Environment

The KDS [DAS] has the capability to work under the environmental conditions in the I&C rooms of the safeguard building.

8.9.5.5 Maintenance

The KDS [DAS] is maintainable.

8.9.5.6 Periodic Test

The KDS [DAS] can be periodically tested, with online self-diagnosis capability. There shall be certain overlapping to ensure overall completeness.

8.10 Control Room System

8.10.1 Introduction

Control room system includes MCR, RSS, and TSC as the monitoring and control centers of the plant. MCR, RSS and TSC are equipped with adequate HMI, with the purpose of providing supervision and control to the plant, so as to provide guarantee for the effective and safe operation of the plant. Control room system consists of KIC [PCICS], Main Control Room System (KSC [MCRS]) and Remote Shutdown Station System (KPR [RSSS]). KIC [PCICS] provides the computerized control means for monitoring and control of the plant in all conditions. KSC [MCRS] provides key monitoring and control means for the plant. KPR [RSSS] provides adequate HMI to maintain the plan in safe status when MCR is unavailable.

8.10.2 Design Principle

The HMI design of control room system is based on the following principles:

- Human factors engineering principles are fully considered, so that personnel and the systems can perform best. A best allocation of all functions shall be applied to realize the highest safety and best availability of the human supervision on the plant. The design must particularly focus on the characteristics of the personnel and the human factors engineering principles to provide perfect and effective HMI.
- Experiences and feedbacks on the human factors engineering involved in the design and operation of control room system gained from domestic and overseas plants are taken full advantage.

- The layout of the control rooms incorporates the requirements on work space and passage for the operation, maintenance and test personnel, and should match the basic ergonomic data.
- The control rooms are designed as a whole to comply with the human factors engineering and environment requirement, and provide suitable work environment and work space for the operators.
- The HMI of control room system provides easily assimilated and understood information to help the operators to make a decision efficiently and accurately.

8.10.3 Design Requirements

The design of control room system provides adequate monitoring and control to the whole plant under all operating conditions, whether normal or abnormal.

The analysis of personnel task requirements, system requirements, regulatory requirements and other requirements are performed in earlier stages of the design process to identify design inputs for the HMI.

A set of HMI principles, philosophies, standards, guidelines and conventions is derived and applied to the HMI design.

Tests and evaluations of concepts and detailed design features will be conducted during the process of developing HMIs to support design decisions.

The design of the control rooms has been developed taking into account all of the roles and activities taking place in or affecting the control rooms, including:

- The unit shift team's roles and activities.
- Avoidance of disturbance and interference to monitoring and control activities.
- Communication devices.
- Support facilities, such as printers, and document cabinets.

8.10.4 Function and Layout

8.10.4.1 MCR

MCR is the monitoring and control center of the plant. It consists of necessary HMI equipment, such as Operator Workplaces (OWPs), Large Display Panels (LDPs) of KIC [PCICS] (KIC-LDP), Emergency Control Panel (ECP), Auxiliary Control Panels (ACPs), LDPs of ACP (ACP-LDP), DHP, SHP, etc., for monitoring and controlling the plant in all conditions. The process monitoring and control means in the MCR are supplied by the HMI of KIC [PCICS] and KSC [MCRS].

a) OWP and KIC-LDP

OWP and KIC-LDP is the HMI equipment of KIC [PCICS] in MCR. OWP and KIC-LDP

is the Main Computerized control Mean (MCM) for the monitoring and control of the plant. KIC [PCICS] is composed of OWPs, Compact Operator Workplaces (COWPs), LDPs, NI servers, CI servers, calculation servers, historical servers, maintenance station, engineering station, configuration station, gateways, network switches, power cabinets, printers, and so on. Most of KIC [PCICS] system equipment is configured redundantly. The redundant parts are powered by train A and B respectively.

The OWPs in MCR include NI-OWP (NI Operator Workplace), CI-OWP (CI Operator Workplace), US-OWP (Unit Supervisor Workplace), and SE-OWP (Safety Engineer Workplace). Each OWP in MCR has five VDUs and four Safety Control and Information Device (SCIDs).These SCIDs execute part function of RPS system. The KIC-LDPs include four large liquid crystal displays and provide plant overview displays. These OWPs and KIC-LDPs are equipped for the operators to operate, monitor and control the plant in all plant conditions, except in a time of evacuation of the MCR due to hazardous situations and other similar events.

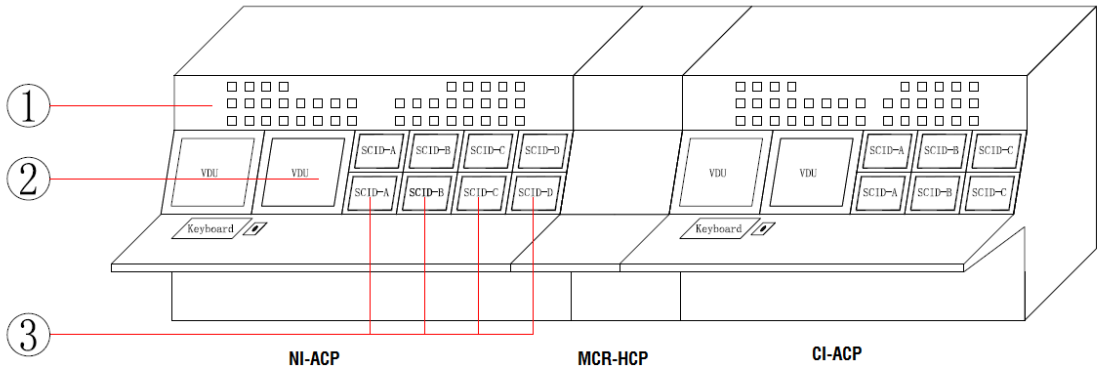
b) ACP

ACP is the HMI equipment of KSC [MCRS] in MCR. ACP is the backup means of MCM for the monitoring and control of the plant, which could provide sufficient controls and information for the operators when KIC [PCICS] system is unavailable or in scheduled maintenance. KSC [MCRS] is mainly composed of ACP, real-time servers, historical servers, maintenance station, engineering station, configuration station, power cabinets, printers, and so on. Most of KSC [MCRS] system equipment is configured redundantly. The redundant part is powered by train A and B respectively.

The main function of the ACP is to provide the shift team with sufficient controls and information to help:

- To maintain the unit in “steady power operation state” or transition to fallback mode (with ECP) in case of unavailability of KIC in DBC-1.
- To make the unit reach “safe shutdown State” (through “controlled state”) with ECP in case of unavailability of KIC in DBC2-4.
- To monitor and control the unit in case of unavailability of KIC caused by planned maintenance during normal shutdown on RIS/RHR mode, maintenance cold shutdown mode, refueling cold shutdown mode, reactor completely discharged mode, in the meantime, operation which could change the state of the plant shall not be carried out.

ACP consists of NI-ACP, MCR-Hard Control Panel (HCP), CI-ACP, US-ACP, and ACP-LDP in MCR. NI/CI-ACP is divided into three parts: Conventional part, VDU part, and SCID part.



F-8.10-1 Layout of ACP

① Conventional part: There are some important hard wired instruments on NI/CI-ACP, including alarm windows, parameter indicators and so on.

② VDU part: The VDUs of NI/CI-ACP are based on SpeedyHold platform. These VDUs of NI/CI-ACP are used for the display, record and operation of F-SC3/NC functions, and used for the display and record of FC1/FC2 functions.

③ SCID part: The SCIDs of NI/CI-ACP are based on FirmSys platform. These SCIDs are used for the display and operation of FC1/FC2 functions and execute part function of RPS system.

US-ACP is equipped with two VDUs and only has monitoring function.

ACP-LDPs include four large liquid crystal displays hung on the wall. The function of ACP-LDP is to assist the shift team in monitoring the general status of the plant.

MCR-HCP is equipped with KIC/ACP mode switches and indicators to transfer the control function between KIC and ACP. The safety screens for the display and record of PAMS parameters are also installed on MCR-HCP.

c) ECP

ECP is a panel placed between NI-OWP and CI-OWP with some conventional devices. A few hardwired controls and indicators are implemented on the ECP for a limited number of functions, which shall be rapidly accessible to the operators (e.g. reactor trip, safety injection and turbine trip). The ECP will always be active as long as the MCR is available.

d) DHP

The DHP is the HMI equipment of the KDS [DAS] in MCR. DHP provides the manual control, alarm and indication functions to prevent postulated software CCF in the RPS.

The main functions of DHP are:

- To provide system-level actuation for diverse reactor trip and engineered safety

actuation functions, and a small set of equipment-level actuation.

- To provide information display for monitoring and alarms of key safety parameters, and status indication of systems and equipment.

e) SHP

The SHP is the HMI equipment of KDA [SA I&C] in MCR. SHP is used to perform the mitigation functions for the identified severe accidents coincident with total power loss.

The main functions of SHP are:

- To provide manual control function in severe accidents.
- To provide parameter monitoring function in severe accidents.

The HMI equipment of DCS in MCR will be used in different conditions of the plant:

- OWP and LDP of KIC [PCICS] are used in all conditions (including normal conditions, accidental conditions and severe accidental conditions).
- ACP (including NI-ACP, CI-ACP, US-ACP and ACP-LDP) is used in case of the failure of KIC [PCICS]. And ACP can be used for DBC accidents.
- DHP of KDS [DAS] is used in case of the failure of RPS with DBC accidents
- SHP of KDA [SA I&C] is used together with ACP in DEC-A (except the CCF of RPS) and DEC-B accidental (severe accident) conditions with the failure of KIC [PCICS].
- ECP is available in MCR until the control function of the plant has been transferred to RSS (except reactor trip and turbine trip).

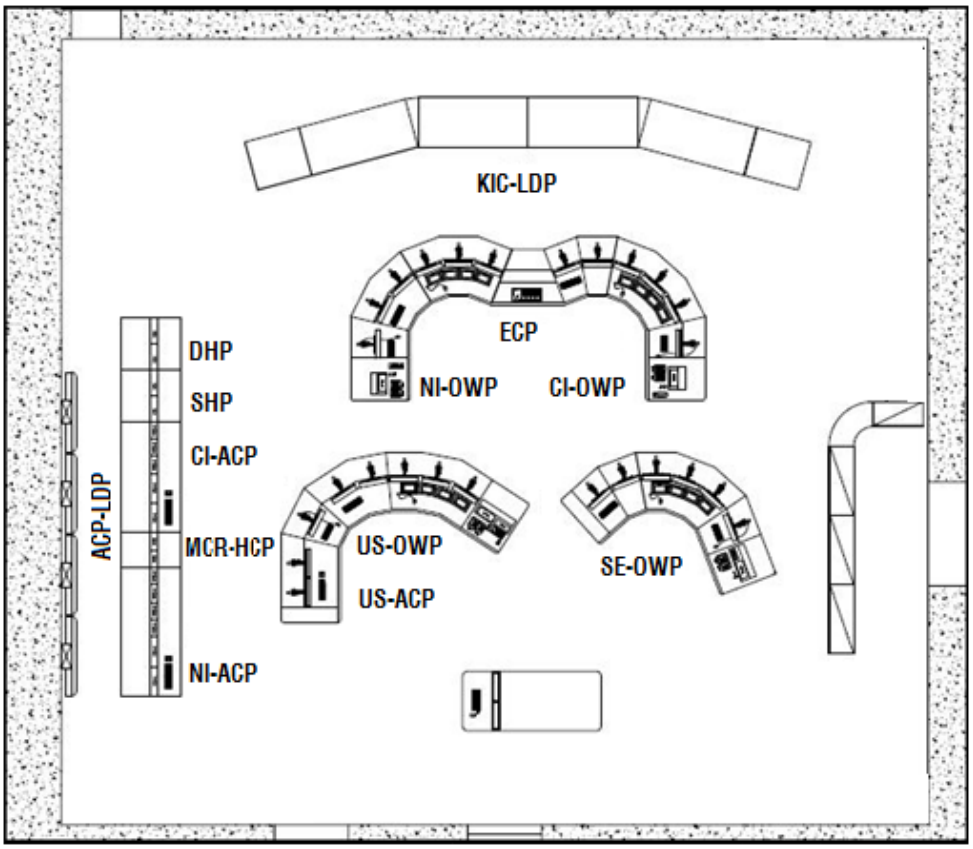
The safety class of HMI equipment in MCR is provided by the following table.

T-8.10-1 Information on HMI Equipment in MCR

Equipment		**Platform**	**Safety Class**
MCR-OWP	VDU part	HOLLiAS-N	F-SC3
	SCID part	FirmSys	F-SC1
KIC-LDP	/	HOLLiAS-N	NC
NI-ACP CI-ACP	VDU part	SpeedyHold	F-SC3
	SCID part	FirmSys	F-SC1

Equipment		Platform	Safety Class
	Conventional part	/	F-SC2/F-SC3
US-ACP	/	SpeedyHold	F-SC3
ACP-LDP	/	SpeedyHold	NC
MCR-HCP	PAMS-SCID	FirmSys	F-SC1
	KIC/ACP Mode Switches	/	F-SC2
ECP	/	/	F-SC1
SHP	/	SpeedyHold	F-SC3
DHP	/	SpeedyHold	F-SC3

The layout of MCR is shown in F-8.10-2.



F-8.10-2 Layout of MCR

8.10.4.2 RSS

RSS is the auxiliary control point of MCR. If MCR is unavailable due to an independent external or internal hazard, RSS enables the operators to perform adequate operations, to bring the plant into a safe shutdown status. It encompasses three COWPs offering the same functions as OWPs located in the MCR.

Each RSS-COWP is equipped with four VDUs and four SCIDs. The seismic category of RSS-COWP is seismic category 1.

There are MCR/RSS mode switches to transfer the control between MCR and RSS. The train A and train C MCR/RSS mode switches are installed in RSS-HCP in RSS. The train B and train D (only for channel IV) RSS mode switches are installed in a box outside RSS. The location of the MCR/RSS mode switches is on the safe evacuation path from MCR to RSS which is protected against damage.

8.10.4.3 TSC

TSC, near to MCR, is used by the technical support team. There is a COWP offering the same information as OWPs located in the MCR (without control function). TSC-COWP only has four VDUs. It is used by the technical support team in case of an accident to establish additional staff analyzing the plant conditions and supporting the post-accident management.

8.11 PSR Conclusions

8.11.1 Conclusions

The foundation on which the UK HPR1000 I&C systems will be developed meets the specific objectives defined to support the high level objectives defined in chapter 1.

This chapter presents the design principles of the I&C systems, and describes the general architecture and different safety classes of the I&C as well as the main HMIs for the HPR1000 (FCG3). This chapter provides confidence that the I&C systems to be developed for UK HPR1000 will be able to demonstrate compliance with UK regulatory requirements. The comparison of HPR1000 (FCG3) Instrumentation & Control Overall Architecture with IEC 61513 has been nearly finished, which will be issued soon. The comparison with IEC61226 is still ongoing which will be finished in next stage.

The main areas that require further analysis to design the UK HPR1000 I&C systems have been identified and these will be developed at appropriate stages in, and beyond, GDA.

8.11.2 Comparison between HPR1000 (FCG3) Design and the UK SAP&TAG Requirements

It is proposed that the I&C systems of UK HPR1000 will adopt similar design as the HPR1000 (FCG3). Based on the analysis of the comparison between the HPR1000 (FCG3) design and the UK TAG & SAP requirements, a few areas have been identified

which might require further discussion and analysis during or beyond GDA with the main items listed below:

a) The GAP between Secondary Protection System（SAP&TAG）and DAS [KDS]

As mentioned in TAG (NS-TAST-GD-046 Computer Based Safety Systems), in order to meet the risk reduction requirement, secondary protection system must be provided. However more requirements related to Secondary Protection System is not given in this TAG.

In HPR1000 (FCG3), DAS [KDS] which is based on FPGA (Field Programmable Gate Array) technology provides the functions required to mitigate software CCF in RPS and SAS with a concurrent high-frequency initiating event. Based on the safety classification principles, the DAS [KDS] is FC3. More detailed information about DAS [KDS] is described in the sub-chapter 8.9 of PSR report. The DAS [KDS] should be discussed in future.

b) Use of Smart Devices

CGN is aware that there are more strict requirements to the use of Smart devices in UK context. In HRP1000, so far as practicable, the use of smart device shall be avoided for safety or safety related functions.

When the use is unavoidable for the UK HPR1000, justifications to prove that the smart devices are suitably qualified to meet the designed reliability claims must be provided. It is necessary to consider an appropriate qualification process.

c) Safety classification of I&C

In HPR1000 (FCG3), the overall classification principle of the plant safety functions is based on the IAEA SSG-30. In IAEA SSG-30, the function that is designed to reduce the actuation frequency of the reactor trip or engineered safety features in the event of a deviation from normal operation, including those designed to maintain the main plant parameters within the normal range of operation of the plant is assigned to safety category 3.

In IEC 61226, which is the source of NS-TAST-GD-094, the control functions which are the only means to maintain the main process variables within the limits assumed in the safety analysis is assigned to category B.

This difference will be discussed in future.

d) Statistical testing consideration for demonstrating the reliability of computer-based safety systems

Statistical testing is highly recommended as an approach for demonstrating the numerical reliability of computer-based safety systems in SAP-2014. And also in TAST-GD-046_R4, it is pointed out that the number of dynamic tests should be informed by statistical testing considerations. Consideration should be given to the feasibility of generating a statistical

estimation of system reliability.

In HPR1000 (FCG3), system availability and unavailable factors of safety function are given through probabilistic safety assessment. Dynamic testing is used to demonstrate the functional and performance requirements are satisfied, without statistical testing considerations, for the demonstration of the reliability of computer-based safety systems.

8.12 References

[1] IAEA, Safety of Nuclear Power Plants Design, IAEA SSR-2/1, Version 1, 2016.

[2] ONR, Safety Assessment Principles for Nuclear Facilities, Version 0, 2014.

[3] ONR, Safety Systems, NS-TAST-GD-003, Version 7, 2014.

[4] ONR, Computer Based Safety Systems, NS-TAST-GD-046, Version 4, 2013.

[5] IEC, Nuclear power plants - Instrumentation and control systems important to safety - General requirement, IEC 61513, Version 2, 2011.

[6] IEC, Nuclear power plants - Instrumentation and control system important to safety - Separation, IEC 60709, Version 2, 2004.

[7] IEC, Nuclear power plants - Instrumentation and control systems important for safety - Requirements for electrical supplies, IEC 61225, Version 2, 2005.

[8] IEC, Nuclear power plants - Instrumentation and control important to safety software aspects for computer-based systems performing category A functions, IEC 60880, Version 2, 2006.

[9] IEC, Nuclear power plants - Instrumentation and control important to safety software aspects for computer-based systems performing category B and C functions, IEC 62138, Version 1, 2004.

[10] IEC, Nuclear power plants - Electrical equipment of safety system - Qualification, IEC 60780, Version 2, 1998.

[11] IEC, Recommended practices for seismic qualification of electrical equipment of the safety system for nuclear, IEC 60980, Version 1, 1989.

[12] IEC, Nuclear power plants - Control rooms - Design, IEC 60964, Version 2, 2009.

[13] IEC, Nuclear power plants - Control rooms - Supplementary control points for reactor shutdown without access to the main control room, IEC 60965, Version 2, 2009.

[14] IEC, Nuclear power plants - Design of control rooms - Functional analysis and assignment, IEC 61839, Version 2, 2000.

[15] IAEA, IAEA Safety Standards: Safety Classification of Structures, Systems and

Components in Nuclear Power Plants, IAEA SSG-30, 2014 edition, May 2014.

[16] IEEE, Standard Criteria for Safety Systems for Nuclear Power Generating Stations, IEEE 603, 2009 edition, 2009.