Revision	Approved by	Number of Pages
000		122
Approval Date	12/11/2018	

General Nuclear System Ltd.

UK HPR1000 GDA Project

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

Title:

Pre-Construction Safety Report

Chapter 8

Instrumentation and Control

This document has been prepared on behalf of General Nuclear System Limited (GNS) with the support of China General Nuclear Power Corporation (CGN) and Électricité de France S.A. (EDF).

Although due care has been taken in compiling the content of this document, neither GNS, CGN, EDF nor any of their respective affiliates accept any liability in respect to any errors, omissions or inaccuracies contained or referred to in it.

DISTRIBUTION LIST

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

MODIFICATION RECORD

Revision	Section	Page	Modification
000	ALL	ALL	First Issue

TABLE OF CONTENTS

8.1 List of Abbreviations and Acronyms 4

8.2 Introduction 8

8.2.1 Background and Evolution 8

8.2.2 Main Technologies and Platforms 10

8.2.3 Interfaces with Other Chapters 11

8.2.4 ALARP 14

8.2.5 Scope 14

8.2.6 Overview of I&C Safety Case 16

8.2.7 Structure of Chapter 8 17

8.3 Applicable Codes and Standards 18

8.3.1 HPR1000 (FCG3) Standards Architecture 18

8.3.2 IAEA and IEC Standards Series 18

8.3.3 Correspondence between Chinese Standards and IAEA/IEC Standards 19

8.3.4 Applicable Standards in UK HPR1000 22

8.4 I&C Claim Architecture 25

8.4.1 I&C High Level Claims Development Process 25

8.4.2 I&C Claims Architecture 27

8.5 Overall I&C Architecture 31

8.5.1 Introduction 31

8.5.2 Claims of Overall I&C Architecture 31

8.5.3 Description of Overall I&C Architecture 31

8.5.4 Layout and Interconnections 40

8.5.5 Defence in Depth 41

8.5.6 Targets of Numeric Reliability for I&C Systems 44

8.5.7 The Safety Features of I&C Systems 45

8.6 F-SC1 Centralised I&C System 52

8.6.1 Introduction 52

8.6.2 Claims for Safety Functions 52

8.6.3 Claims for Safety Features 52

8.6.4 System Function Description 52

8.6.5 System Architecture 53

8.6.6 System Design Description 55

8.7 F-SC2 Centralised I&C System 58

8.7.1 Introduction 58

8.7.2 Claims for Safety Functions 58

8.7.3 Claims for Safety Features 58

8.7.4 System Function Description 58

8.7.5 System Architecture 60

8.7.6 System Design Description 61

8.8 F-SC3 Centralised I&C Systems 63

8.8.1 Plant Standard Automation System (PSAS) 63

8.8.2 Severe Accident I&C System (KDA [SA I&C]) 67

8.8.3 Diverse Actuation System (KDS [DAS]) 70

8.9 Non-classified Centralised I&C System 74

8.10 Non-centralised I&C Systems 74

8.11 Instrumentation and Actuators 77

8.11.1 Instrumentation 77

8.11.2 Actuators 77

8.12 I&C Support Systems 78

8.12.1 Electrical Power System 78

8.12.2 HVAC 80

8.13 Control Room Systems 81

8.13.1 Introduction 81

8.13.2 Claims for Safety Functions 81

8.13.3 Claims for Safety Features 81

8.13.4 Main Control Room System (KSC [MCRS]) 81

8.13.5 Plant Computer Information and Control System (KIC [PCICS]) 87

8.13.6 Remote Shutdown Station System (KPR [RSSS]) 90

8.13.7 HMIs in Control Rooms 91

8.14 System Development and Justification 97

8.14.1 System Development 97

8.14.2 System Justification 98

8.14.3 I&C Platforms 99

8.14.4 Smart Devices 104

8.15 Commissioning 105

8.16 EMIT and Ageing 105

8.16.1 Examination, Maintenance, Inspection and Testing 105

8.16.2 Ageing Degradation 106

8.17 ALARP Assessment 107

8.17.1 General Description 107

8.17.2 Presenting the HPR1000 I&C Design Evolution 108

8.17.3 Identifying and Analysing the UK RGP and OPEX 108

8.17.4 Analysing the Insight from the PSA 109

8.17.5 Identifying Gaps 109

8.17.6 Undertaking an Options Analysis 109

8.17.7 Selecting an Optimal Solution and Implementation to Close the Gaps and Giving the ALARP Justification 110

8.18 Concluding Remarks 110

8.19 References 110

Appendix 8A I&C Systems Function Claims 113

8.1 List of Abbreviations and Acronyms

AC	Alternating Current
ACP	Auxiliary Control Panel
ACPR1000	Advanced Chinese Pressurised Reactor
ALARP	As Low As Reasonably Practicable
ARE	Main Feedwater Flow Control System [MFFCS]
ASG	Emergency Feedwater System [EFWS]
ASP	Secondary Passive Heat Removal System [SPHRS]
ATWS	Anticipated Transient Without Scram
BLX	Conventional Island Electrical Building
BMX	Turbine Generator Building
BNX	Nuclear Auxiliary Building
BOP	Balance of Plant
BSC	Basis of Safety Case
BWX	Radioactive Waste Treatment Building
CAE	Claims, Arguments, Evidence
CCF	Common Cause Failure
CCMC	Core Cooling Monitoring Cabinet
CGN	China General Nuclear Power Corporation
CI	Conventional Island
CIC	Component Interface Cabinet
CIM	Component Interface Module
COWP	Compact Operator Workplace
CPLD	Complex Programmable Logic Device
CPR1000	Chinese Pressurised Reactor
CPR1000^{+}	Chinese Improved Pressurised Reactor
CPU	Central Processing Unit
CTEC	China Techenergy Co., Ltd
CVI	Condensate Vacuum System [CVS]
DAC	Diverse Actuation Cabinet
DBC	Design Basic Condition

DC	Direct Current
DCL	Main Control Room Air Conditioning System [MCDACS]
DEC-A	Design Extension Condition A
DEC-B	Design Extension Condition B
DEL	Safety Chilled Water System [SCWS]
DHP	Diverse Human interface Panel
DiD	Defence in Depth
DTC	Data Transmission Cabinet
DVL	Electrical Division of Safeguard Building Ventilation System [EDSBVS]
ECP	Emergency Control Panel
ECS	Extra Cooling System [ECS]
EDG	Emergency Diesel Generator
EHR	Containment Heat Removal System [CHRS]
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
EMIT	Examination, Maintenance, Inspection and Testing
ESFAC	Engineered Safety Feature Actuation Cabinet
FPGA	Field Programmable Gate Array
GDA	Generic Design Assessment
GW	Gateway
HAF	Chinese Nuclear Safety Regulation
HCP	Hardwired Control Panel
HDL	Hardware Description Language
HF	Human Factors
HFE	Human Factors Engineering
HMI	Human Machine Interface
HPR1000	Hua-long Pressurised Reactor
HPR1000 (FCG3)	Hua-long Pressurised Reactor under construction at Fangchenggang nuclear power plant unit 3
HVAC	Heating, Ventilation and Air Conditioning
I&C	Instrumentation and Control

I/O	Input/Output
IAEA	International Atomic Energy Agency
ICBM	Independent Confidence Building Measure
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]
KPR	Remote Shutdown Station System [RSSS]
KRT	Plant Radiation Monitoring System [PRMS]
KSC	Main Control Room System [MCRS]
LDP	Large Display Panel
LOOP	Loss of Offsite Power
MCM	Main Computerised Control Means
MCR	Main Control Room
MHSI	Medium Head Safety Injection
MSIV	Main Steam Isolation Valve
NC	Non-classified
NI	Nuclear Island
NPP	Nuclear Power Plant
OPEX	Operating Experience
OWP	Operator Workplace
PCSR	Pre-Construction Safety Report
PE	Production Excellence
PIE	Postulated Initiating Event
PLC	Programmable Logic Controller
PMC	Fuel Handling and Storage System [FHSS]
PS	Protection System
PSA	Probabilistic Safety Assessment
PSAC	Plant Standard Automation Cabinet

PSAS	Plant Standard Automation System
RBS	Emergency Boration System [EBS]
RCP	Reactor Coolant System [RCS]
RCPB	Reactor Coolant Pressure Boundary
RCV	Chemical and Volume Control System [CVCS]
RGL	Rod Position Indication and Rod Control System [RPICS]
RGP	Relevant Good Practice
RHR	Residual Heat Removal
RIC	In-core Instrumentation System [IIS]
RIS	Safety Injection System [SIS]
RPC	Reactor Protection Cabinet
RPN	Nuclear Instrumentation System [NIS]
RPV	Reactor Pressure Vessel
RSS	Remote Shutdown Station
RTB	Reactor Trip Breaker
SAC	Safety Automation Cabinet
SAP	Safety Assessment Principle (UK)
SAS	Safety Automation System
SBO	Station Black Out
SCC	Safety Control Cabinet
SCID	Safety Control and Information Device
SDM	System Design Manual
SE	Safety Engineer
SFC	Single Failure Criterion
SHP	Severe accident Human interface Panel
S-NET	System Network
SPC	Signal Pre-processing Cabinet
SPM	Signal Pre-processing Module
SSCs	Structures, Systems and Components
SSE	Safe Shutdown Earthquake
TAG	Technical Assessment Guide (UK)

TBD	To Be Determined
TEG	Gaseous Waste Treatment System [GWTS]
TGCS	Turbine Generator Control System
TR	Topic Report
TSC	Technical Support Centre
UK HPR1000	UK version of the Hua-long Pressurised Reactor
UPS	Uninterruptible Power Supply
US	Unit Supervisor
V&V	Verification and Validation
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. Diverse Actuation System (KDS [DAS]).

8.2 Introduction

The object of Pre-Construction Safety Report (PCSR) Chapter 8 is to provide engineering substantiation that the design of the Instrumentation and Control (I&C) systems delivers the necessary nuclear safety, in an appropriate manner, depending on the safety function category and safety classification for the UK version of the Hua-long Pressurised Reactor (UK HPR1000).

This sub-chapter introduces the evolution and background of the UK HPR1000 I&C systems. It describes the main technology and gives an overview of the I&C safety case and scope of the I&C systems and Generic Design Assessment (GDA).

As Low As Reasonably Practicable (ALARP) is a convenient means to express the legal duty to reduce risks so far as reasonably practicable. This sub-chapter gives the general description of ALARP and Sub-chapter 8.17 provides the strategy of ALARP.

The structure of this chapter and its relationship with other chapters are also introduced.

8.2.1 Background and Evolution

The Hua-long Pressurised Reactor (HPR1000), developed by China General Nuclear Power Corporation (CGN), is derived from improvements of the Chinese Pressurised Reactor (CPR1000), Chinese Improved Pressurised Reactor (CPR1000^{+}) and Advanced Chinese Pressurised Reactor (ACPR1000). The construction and operation experience of the HPR1000 are described in Chapter 2.

I&C technology has evolved from analogue electronics to digital processing

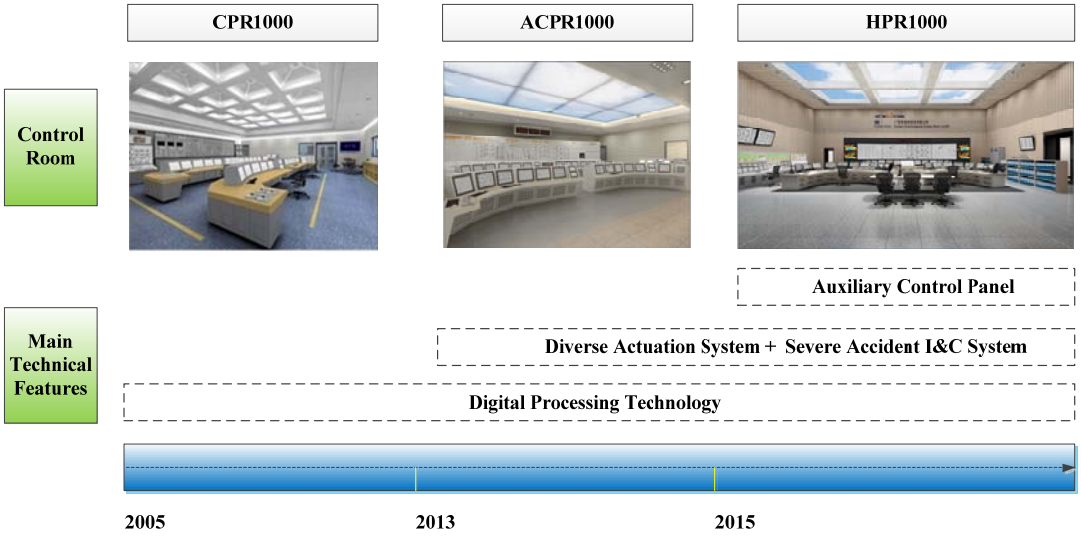
technology which is the major improvement in the CPR1000 power plant. This current generation technology can enhance the safety and functional performance of I&C systems.

In the ACPR1000 power plant, the Diverse Actuation System (KDS [DAS]) and the Severe Accident I&C System (KDA [SA I&C]) are adopted as the significant modifications in the I&C systems design. The KDS [DAS] is able to mitigate the consequences of Design Basic Conditions (DBCs) with the concurrent Common Cause Failure (CCF) of Protection System (PS) and Safety Automation System (SAS) and it brings the Nuclear Power Plant (NPP) to its final state.

Taking account of learning from the Fukushima accident, the KDA [SA I&C] is used to perform Design Extension Condition B (DEC-B) management and monitoring functions required in the event of a total loss of the Alternating Current (AC) power supply.

In the HPR1000, the continuous optimisations are implemented in the KDS [DAS] and KDA [SA I&C] design, and three divisions for the Engineered Safety Feature Actuation Cabinet (ESFAC) are designed corresponding to the I&C systems design. The Auxiliary Control Panel (ACP) is the major improvement corresponding to the ACPR1000 I&C systems design.

The evolution and main technical features of the HPR1000 I&C systems are shown in Figure F-8.2-1.



F-8.2-1 Evolution and Main Technical Features of HPR1000 I&C Systems

The design of the UK HPR1000 I&C systems starts from the Hua-long Pressurised Reactor under construction at Fangchenggang nuclear power plant unit 3 (HPR1000 (FCG3)) design and is updated based on the modifications reflecting the requirements of UK context and Relevant Good Practice (RGP). It is recognised that there are some

gaps between the HPR1000 (FCG3) design and UK RGP. CGN will analyse these gaps by using ALARP methodology and implement necessary improvements to close the gaps after ALARP analysis.

8.2.2 Main Technologies and Platforms

The I&C systems of the UK HPR1000 mainly adopt digital processing technology to perform protection, control, monitoring and alarm functions. The digital control systems provide the adequate and reliable measures to maintain all plant parameters within the specified operational limits, prevent abnormal transients or accidents and mitigate the consequences after accidents.

The main platforms based on digital processing technology include:

a) FirmSys is used for F-SC1 and F-SC2 systems;

b) SpeedyHold is used for F-SC3 systems;

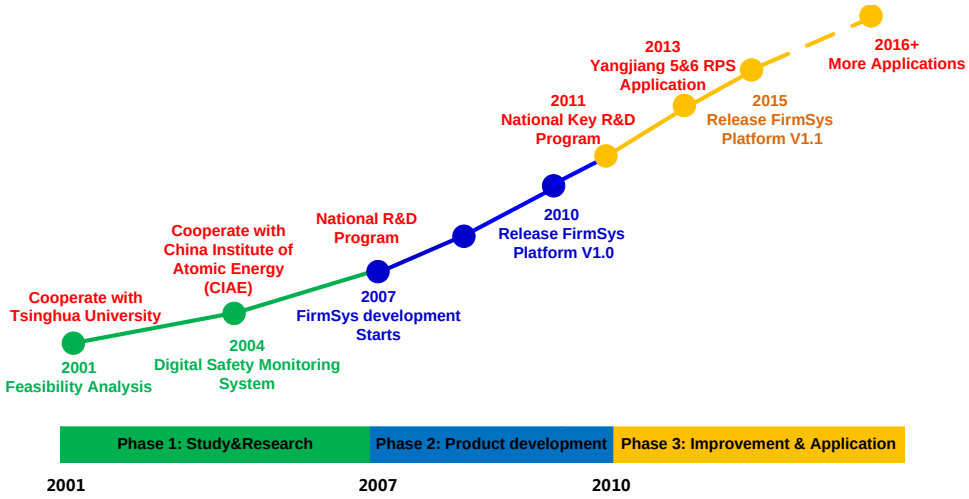
c) HOLLiAS-N is used for F-SC3 and Non-classified (NC) systems.

The FirmSys platform is developed and produced by China Techenergy Co., Ltd (CTEC). It is a safety class I&C platform, which can be applied to safety I&C systems. The development of the FirmSys platform follows China and international nuclear safety codes, regulations and relevant industry standards.

The evolution and main development milestones of FirmSys are shown in Figure F-8.2-2.

The FirmSys platform development was started in 2007. Version 1.0 was released in 2010, and then along with the applications, FirmSys had been continuously improved. Version 1.1 was released in 2015.

FirmSys has been applied to ACPR1000 plants (Yangjiang NPP unit 5 and 6 safety control and protection system and Hongyanhe NPP unit 5 and 6 safety control and protection system) and is applied to the HPR1000 (FCG3) (safety control and protection system).



F-8.2-2 Evolution and Main Development Milestones of FirmSys

The HOLLiAS-N platform is developed and produced by Hollysys company, and has been used as the F-SC3 and NC platform in more than 17 NPP units in China.

The SpeedyHold platform is developed and produced by CTEC. It is a general computer based I&C platform which adopts technology different from HOLLiAS-N and is applied to the KDA [SA I&C] in the HPR1000 (FCG3).

Besides digital processing technology, a platform based on Field Programmable Gate Array (FPGA) technology is adopted for the KDS [DAS]. This platform is FitRel used for F-SC3 systems. A gap of the KDS [DAS] between the current technology and UK context has been identified.

8.2.3 Interfaces with Other Chapters

The I&C systems design requirements are derived from the plant safety design basis, including the functional requirements and the design principles. The input requirements for the I&C systems is linked to other chapters, and the interfaces are listed in Table T-8.2-1.

T-8.2-1 Interfaces between Chapter 8 and Other Chapters

PCSR Chapter	Interface
Chapter 1 Introduction	Chapter 1 provides the fundamental objective, Level 1 claims and Level 2 claims. Chapter 8 provides claims and arguments to support Level 2 claim 3.3 that are addressed in Chapter 1.
Chapter 2 General Plant Description	Chapter 8 provides a further description of the I&C systems mentioned in Chapter 2.

PCSR Chapter	Interface
Chapter 4 General Safety and Design Principles	Chapter 4 presents the general safety and design principles which are the input of I&C system design. Chapter 8 demonstrates that the principles have been implemented in the design.
Chapter 6 Reactor Coolant Systems	Chapter 6 provides control function requirements that are fulfilled by I&C systems in Chapter 8.
Chapter 7 Safety Systems	Chapter 7 provides control function requirements that are fulfilled by I&C systems in Chapter 8.
Chapter 9 Electric Power	Chapter 9 presents the design information of electrical power systems which support the functions of I&C systems in Chapter 8. Chapter 8 presents the I&C functions to support of electrical power systems in Chapter 9. Chapter 8 also presents the definition and the general justification approach of smart devices used in safety classified I&C systems, which are also applicable to the smart devices used in safety classified electrical power systems presented in Chapter 9.
Chapter 10 Auxiliary Systems	Chapter 10 provides control function requirements that are fulfilled by I&C systems. Chapter 8 provides design substantiation relevant to the control functions in Chapter 10.
Chapter 11 Steam and Power Conversion System	Chapter 11 provides control function requirements that are fulfilled by I&C systems in Chapter 8. Chapter 8 provides design substantiation relevant to these control functions in Chapter 11.
Chapter 12 Design Basis Condition Analysis	Chapter 8 provides the substantiation of I&C systems which are taken into consideration the fault analysis in Chapter 12.

PCSR Chapter	Interface
Chapter 13 Design Extension Conditions and Severe Accident Analysis	Chapter 13 presents the analysis of design extension conditions. Chapter 8 demonstrates that the requirements have been implemented in the I&C design.
Chapter 14 Probabilistic Safety Assessment	Chapter 8 provides design inputs for the Probabilistic Safety Assessment (PSA) analysis and fault trees modelling in Chapter 14. Chapter 14 is used to identify the vulnerabilities in system design to improve the system reliability.
Chapter 15 Human Factors	Chapter 15 provides the principles and methodology of human factor integration that are considered in I&C systems design. Chapter 8 provides the specific design of I&C systems, which is taken into account for further estimate in the Human Factors (HF) area.
Chapter 18 External Hazards	Chapter 18 provides the types of external hazards considered in the UK HPR1000. Chapter 8 considers these types of external hazards and demonstrates that the protection measures against external hazards have been implemented in the design.
Chapter 19 Internal Hazards	Chapter 19 provides the types of internal hazards considered in the UK HPR1000. Chapter 8 considers these types of internal hazards and demonstrates that the protection measures against internal hazards have been implemented in the design.
Chapter 20 MSQA and Safety Case Management	The organisational arrangements and quality assurance arrangements set out in Chapter 20 are implemented in the design process and in the production of Chapter 8.

PCSR Chapter	Interface
Chapter 30 Commissioning	Chapter 8 provides the I&C system design information for commissioning arrangements and requirements in Chapter 30.
Chapter 31 Operational Management	Chapter 31 provides the arrangement of Examination, Maintenance, Inspection and Testing (EMIT), ageing and degradation procedure. Chapter 8 provides I&C systems design substantiation relevant to EMIT, ageing and degradation.
Chapter 33 ALARP Evaluation	The ALARP approach presented in Chapter 33 has been applied in Chapter 8 to perform the ALARP demonstration for I&C systems design, which supports the overall ALARP demonstration addressed in Chapter 33.

8.2.4 ALARP

In UK context, there is a fundamental requirement for the requesting party to set out its process to reduce risks to the level, which is ALARP. This requires that all measures are taken during the design and operation process to minimise radiation doses to workers or members of the public. During the I&C systems design, ALARP is used to demonstrate and evaluate the architecture, systems and platforms.

Chapter 33 presents the methodology of the ALARP evaluation for UK HPR1000 design. Further information is described in Sub-chapter 33.4.

Chapter 8 follows this method and Sub-chapter 8.17 gives the general description of ALARP for I&C systems design.

8.2.5 Scope

8.2.5.1 Scope of I&C Systems

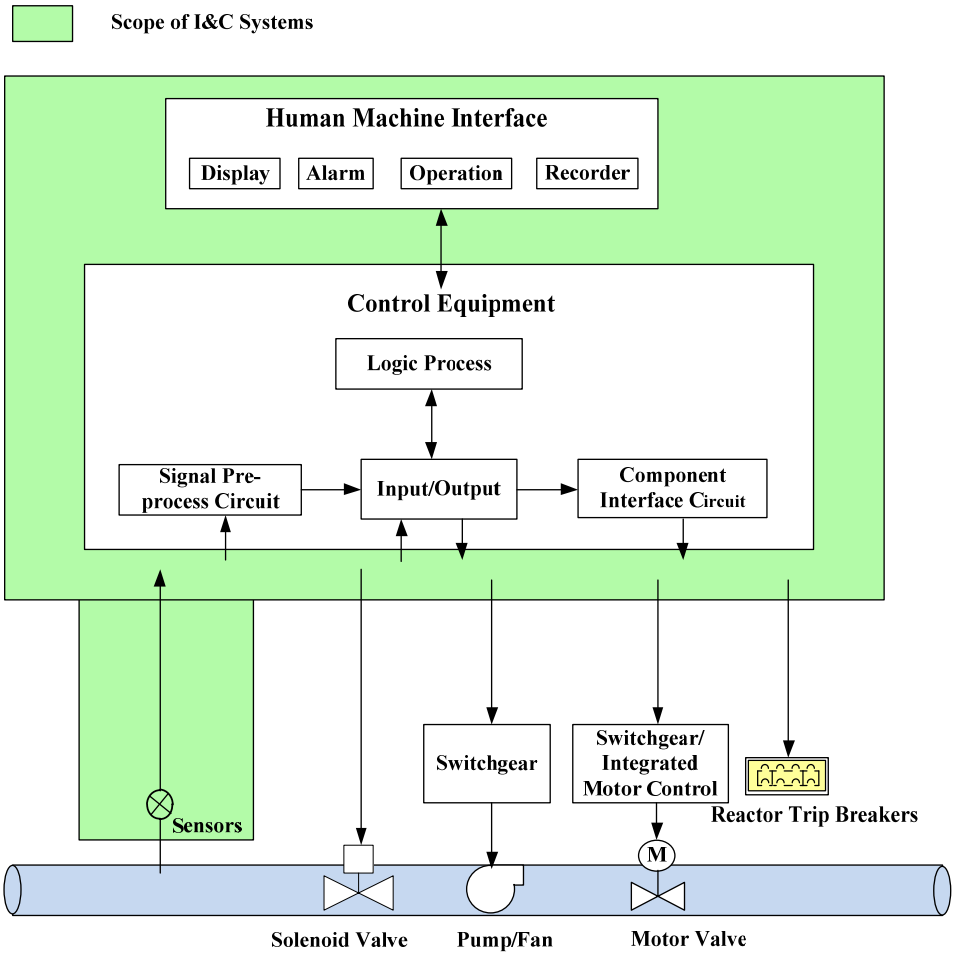
This sub-chapter introduces information about the architecture, systems and platforms contributing to nuclear safety. The scope of I&C systems is defined in Figure F-8.2-3. It covers:

a) Sensors;

b) Actuators;

c) Control equipment;

d) Human Machine Interface (HMI).



F-8.2-3 Scope of I&C Systems

The systems and equipment of the HMIs are described in this chapter and the information of HF of I&C systems is described in Chapter 15.

8.2.5.2 GDA Scope

This sub-chapter identifies general information about the scope of I&C systems during the GDA process. It mainly includes the overall I&C architecture, systems and platforms. The following information is included in the GDA scope:

a) The equipment layout of the Centralised I&C systems and associated building information;

b) The I&C systems which directly contribute to Defence in Depth (DiD);

c) The qualification and substantiation of platforms for Centralised I&C systems;

d) The requirements of installation, testing, commissioning and maintenance.

Only the F-SC1, F-SC2 and F-SC3 systems and equipment mentioned above are provided during the GDA process. The degree of information provided is

proportionate to the classification of the systems, e.g. more information is provided for a higher classification.

For the newly-developed I&C platform, the methodology and strategy of platform qualification are included in the GDA scope.

The Non-centralised I&C systems, smart devices and sensors will be undertaken during the post GDA phase subject to the equipment selection and purchasing. Only selection principles and key properties will be included in the GDA scope.

Centralised I&C systems, which include the PS, SAS, KDS [DAS], KDA [SA I&C], Plant Computer Information and Control System (KIC [PCICS]), Main Control Room System (KSC [MCRS]) and Remote Shutdown Station System (KPR [RSSS]), are directly related to plant safety or directly contribute to DiD.

Non-centralised I&C systems refer to the systems that perform specific I&C functions and are relatively independent from Centralised I&C systems, which include Nuclear Instrumentation System (RPN [NIS]), In-core Instrumentation System (RIC [IIS]), Rod Position Indication and Rod Control System (RGL [RPICS]), Plant Radiation Monitoring System (KRT [PRMS]), Nuclear Accident Emergency Management System (KCC [NAEMS]), etc.

8.2.6 Overview of I&C Safety Case

The demonstration and justification of I&C systems applies the Claims, Arguments, Evidence (CAE) approach. There are three tiers of documents in the safety case, namely tier 1, tier 2 and tier 3. The I&C safety functions and safety features are claimed and argued in the PCSR which is the tier 1 document. The I&C safety function claims are derived from plant safety design basis (fault analysis, PSA and safety system design). The safety feature claims which include independence, diversity and reliability requirements are derived from UK RGP. In Sub-chapter 8.4, five I&C high level claims and a number of sub-claims are developed and presented. This chapter supports the claim 3.3 which is derived from the claim 3 in Chapter 1.

In order to support the claims and arguments of the PCSR, there are a set of Basis of Safety Case (BSC) documents and Topic Reports (TRs) provided to describe the detailed information and evidence. BSC documents are the tier 2 documents which are categorised as “BSC of overall I&C architecture” and “BSC documents of systems”. “BSC of overall I&C architecture” aims to address categorisation and classification, DiD and reliability to support the PCSR. “BSC documents of systems” aims to address I&C system function, system architecture, platform and qualification requirements to support the PCSR. TRs are mainly used to present the platforms related information. The “TRs of platforms” gives the detailed information and evidence about platforms and supports the platform description of the PCSR and BSC documents.

In UK HPR1000 I&C systems design, the major BSC documents include:

a) *BSC of Overall I&C Architecture*;

b) *BSC of Protection System*;

c) *BSC of Safety Automation System*;

d) *BSC of Severe Accident I&C System*;

e) *BSC of Plant Standard Automation System*.

The major TRs of platforms include:

a) *Topic Report of FirmSys Platform*;

b) *Topic Report of HOLLiAS-N Platform*;

c) *Topic Report of SpeedyHold Platform*.

Independent Confidence Building Measures (ICBMs) and their justifications for the digital I&C systems development process are the key processes. There are a set of documents to demonstrate the process. Sub-chapter 8.14 gives the general description and requirements of ICBMs.

Tier 3 documents include the detailed engineering documents. These documents provide the evidence supporting the claims and arguments demonstrated in the PCSR and BSC documents. These documents include:

a) System Design Manual (SDM I&C part);

b) Control schematic diagram.

8.2.7 Structure of Chapter 8

The structure of Chapter 8 is as follows:

a) Sub-chapter 8.1 presents a list of abbreviations and acronyms;

b) Sub-chapter 8.2 presents a general introduction of Chapter 8;

c) Sub-chapter 8.3 presents the applicable codes and standards;

d) Sub-chapter 8.4 presents the I&C claim architecture;

e) Sub-chapter 8.5 presents the overall I&C architecture description;

f) Sub-chapter 8.6 presents the F-SC1 Centralised I&C system;

g) Sub-chapter 8.7 presents the F-SC2 Centralised I&C systems;

h) Sub-chapter 8.8 presents the F-SC3 Centralised I&C systems;

i) Sub-chapter 8.9 presents the NC Centralised I&C systems;

j) Sub-chapter 8.10 presents the Non-centralised I&C systems;

k) Sub-chapter 8.11 presents the general information about instrumentation and actuators;

l) Sub-chapter 8.12 presents the I&C support systems;

m) Sub-chapter 8.13 presents the control room systems;

n) Sub-chapter 8.14 presents the system development and justification;

o) Sub-chapter 8.15 presents commissioning requirements of I&C systems;

p) Sub-chapter 8.16 presents the EMIT and ageing of I&C systems;

q) Sub-chapter 8.17 presents the general description of ALARP;

r) Sub-chapter 8.18 presents the concluding remarks;

s) Sub-chapter 8.19 presents the references.

8.3 Applicable Codes and Standards

Chapter 4 and *General Principles for Application of Laws, Regulations, Codes and Standards*, Reference [1] present the selection principles and selection process of applicable codes and standards applied to the UK HPR1000. The codes and standards for the I&C design in the UK HPR1000 are determined according to these selection principles and selection process. This sub-chapter provides the list and application of the codes and standards for the I&C design.

8.3.1 HPR1000 (FCG3) Standards Architecture

The I&C design of the UK HPR1000 is based on the current design of the HPR1000 (FCG3) with some necessary modifications to incorporate UK requirements.

The codes and standards in the HPR1000 (FCG3) consist of nuclear safety regulation (Chinese Nuclear Safety Regulation (HAF) 102), nuclear safety guides (NS-G-1.1, Reference [2], NS-G-1.3, Reference [3] and DS367 (the draft version of SSG-30, Reference [4])) and technical standards.

The Chinese standards are used as technical standards in I&C design, development, implementation, operation and maintenance, e.g. NB/T 20026, GB/T 15474, etc.

The international standards are also applied to the UK HPR1000 I&C design, e.g. International Electrotechnical Commission (IEC) standards (IEC 61513, Reference [5], IEC 60880, Reference [6], etc.) and the Institute of Electrical and Electronics Engineers (IEEE) 497, Reference [7].

8.3.2 IAEA and IEC Standards Series

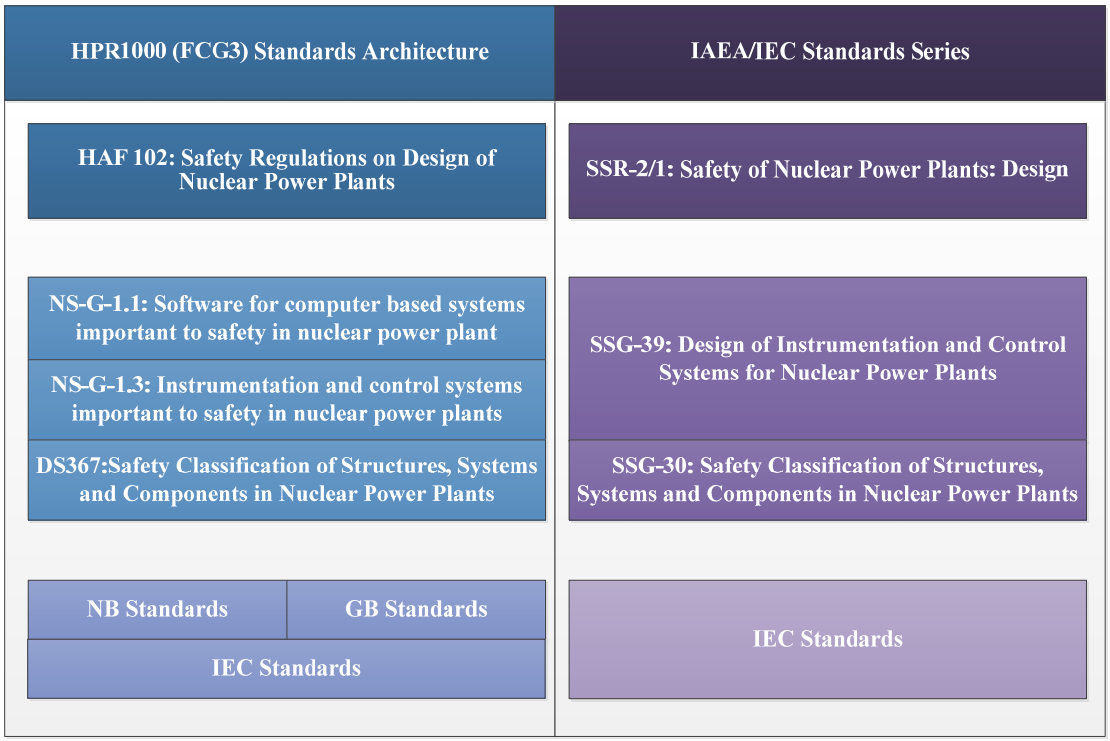
The International Atomic Energy Agency (IAEA) safety standards reflect an

international consensus on what constitutes a high level of safety for preventing people and the environment from the harmful effects of ionising radiation. They are issued in the IAEA safety standards series, which has three categories. The publication categories in the series are safety fundamentals, safety requirements and safety guides. SSR-2/1, Reference [8] provides safety requirements for NPP design. SSG-39, Reference [9] provides safety guides for the design of I&C systems and SSG-30, Reference [4] provides safety guides for safety classification of Structures, Systems and Components (SSCs) in NPPs.

The IEC SC 45A is responsible for the standardisation of activities related to electronic and electrical functions and associated systems and equipment used in instrumentation, control and electrical systems of nuclear facilities. The IEC SC 45A standards series consistently implements and details the principles and basic safety aspects provided in the IAEA code on the safety of NPPs and in the IAEA safety series. IEC SC 45A includes a lot of IEC standards, e.g. IEC 61513, Reference [5], IEC 60880, Reference [6], etc.

8.3.3 Correspondence between Chinese Standards and IAEA/IEC Standards

The relationship between the HPR1000 (FCG3) standards architecture and IAEA/IEC standards series is shown in Figure F-8.3-1. A correspondent summary between Chinese standards and IEC standards is presented in Table T-8.3-1.



F-8.3-1 Relationship between HPR1000 (FCG3) Standards Architecture and IAEA/IEC Standards Series

T-8.3-1 Correspondent Summary between Chinese Standards and IEC Standards

No.	Chinese Standards	Date Issued	Related IEC Standards	Title	Date Issued
1	NB/T 20026	2014	IEC 61513	Nuclear Power Plants - Instrumentation and Control Important to Safety - General Requirement for Systems	2011
2	GB/T 15474	2010	IEC 61226	Nuclear Power Plants - Instrumentation and Control Important to Safety - Classification of Instrumentation and Control Functions	2009
3	NB/T 20054	2011	IEC 60880	Nuclear Power Plants - Instrumentation and Control Systems Important to Safety - Software Aspects for Computer-based Systems Performing Category A Functions	2006
4	NB/T 20055	2011	IEC 62138	Nuclear Power Plants - Instrumentation and Control Important to Safety - Software Aspects for Computer-based Systems Performing Category B and C Functions	2004
5	NB/T 20298	2014	IEC 60987	Nuclear Power Plants - Instrumentation and Control Important to Safety - Hardware Design Requirements for Computer-based Systems	2013
6	NB/T 20068	2012	IEC 62340	Nuclear Power Plants - Instrumentation and Control Systems Important to Safety - Requirements for Coping with Common Cause Failure (CCF)	2007

No.	Chinese Standards	Date Issued	Related IEC Standards	Title	Date Issued
7	GB/T 12721	2017	IEC 60780	Nuclear Facilities - Electrical Equipment Important to Safety - Qualification	2016
8	GB/T 13625	1992	IEC 60980	Recommended Practices for Seismic Qualification of Electrical Equipment of the Safety System for Nuclear Generating Stations	1989
9	GB/T 13286	2008	IEC 60709	Nuclear Power Plants - Instrumentation and Control System Important to Safety - Separation	2004
10	GB/T 5204	2008	IEC 60671	Nuclear Power Plants - Instrumentation and Control System Important to Safety - Surveillance Testing	2007
11	NB/T 20342	2015	IEC 61500	Nuclear Power Plants - Instrumentation and Control Important to Safety - Data Communication in Systems Performing Category A Functions	2009
12	GB/T 13630	2015	BS IEC 60964	Nuclear Power Plants - Control Rooms - Design	2009
13	GB/T 13631	2015	BS IEC 60965	Nuclear Power Plants - Control Rooms - Supplementary Control Room for Reactor Shutdown Without Access to the Main Control Room	2009

8.3.4 Applicable Standards in UK HPR1000

The UK HPR1000 design is based on the current design of the HPR1000 (FCG3) and has learned good practice from the NPPs in China. It also reflects *Safety Assessment Principle (UK) (SAP)*, Reference [10] and *Technical Assessment Guides (UK) (TAGs)*, Reference [11] and [12], and adopts the IAEA standards series, e.g. SSR-2/1, Reference [8], SSG-39, Reference [9] and SSG-30, Reference [4].

The IEC SC 45A standards series is applicable for UK HPR1000 I&C design. IEC 61513, Reference [5] is a top-level document of the IEC SC 45A standard series, which is used in the design process of UK HPR1000 I&C systems for architecture and individual system design. In addition, some other IEC standards are also adopted in the design.

a) IEC 61226, Reference [13] is referred to in I&C safety categorisation in the UK HPR1000;

b) The software design and development of I&C systems performing FC1 functions follows the requirements in IEC 60880, Reference [6];

c) The software design and development of I&C systems performing FC2 and FC3 functions follows the requirements in IEC 62138, Reference [14];

d) The hardware design and development of I&C systems based on the FirmSys platform follows the requirements in IEC 60987, Reference [15];

e) The I&C systems to cope with CCF follow the requirements in IEC 62340, Reference [16];

f) The general qualification process and methodology follow the requirements in IEC 60780, Reference [17];

g) The seismic qualification of I&C systems follows the requirements in IEC 60980, Reference [18];

h) The separation design of I&C systems follows the requirements in IEC 60709, Reference [19];

i) The surveillance testing of I&C systems follows the requirements in IEC 60671, Reference [20];

j) Data communication in I&C systems follows the requirements in IEC 61500, Reference [21];

k) Electromagnetic Compatibility (EMC) test is conducted mainly according to IEC 61000 series, Reference [22];

l) The ageing management of I&C systems follows the requirements in IEC 62342, Reference [23];

m) The computer based procedures design of the Main Control Room (MCR) follows the requirements in IEC 62646, Reference [24];

n) MCR design follows the requirements in BS IEC 60964, Reference [25] and BS IEC 60965, Reference [26];

o) The qualification for smart devices follows the requirements in IEC 61508, Reference [27] and IEC 62671, Reference [28].

Besides the above IEC standards, IEEE 497, Reference [7] is also adopted in the design of accident monitoring functions.

Applicable codes and standards in the design of I&C systems for the UK HPR1000 are listed in Table T-8.3-2.

T-8.3-2 Applicable Codes and Standards

Standards Number	Title	Date Issued
SSR-2/1	Safety of Nuclear Power Plants: Design	2016
SSG-39	Design of Instrumentation and Control Systems for Nuclear Power Plants	2016
SSG-30	Safety Classification of Structures, Systems and Components in Nuclear Power Plants	2014
IEC 61513	Nuclear Power Plants - Instrumentation and Control Important to Safety - General Requirement for Systems	2011
IEC 61226	Nuclear Power Plants - Instrumentation and Control Important to Safety - Classification of Instrumentation and Control Functions	2009
IEC 60880	Nuclear Power Plants - Instrumentation and Control Systems Important to Safety - Software Aspects for Computer - Based Systems Performing Category A Functions	2006

Standards Number	Title	Date Issued
IEC 62138	Nuclear Power Plants - Instrumentation and Control Important to Safety - Software Aspects for Computer-based Systems Performing Category B and C Functions	2004
IEC 60987	Nuclear Power Plants - Instrumentation and Control Important to Safety- Hardware Design Requirements for Computer-based Systems	2013
IEC 62340	Nuclear Power Plants - Instrumentation and Control Systems Important to Safety - Requirements for Coping with Common Cause Failure (CCF)	2007
IEC 60780	Nuclear Facilities - Electrical Equipment Important to Safety - Qualification	2016
IEC 60980	Recommended Practices for Seismic Qualification of Electrical Equipment of The Safety System for Nuclear Generating Stations	1989
IEC 60709	Nuclear Power Plants - Instrumentation and Control System Important to Safety - Separation	2004
IEC 60671	Nuclear Power Plants - Instrumentation and Control System Important to Safety - Surveillance Testing	2007
IEC 61500	Nuclear Power Plants - Instrumentation and Control Important to Safety - Data Communication in Systems Performing Category A Functions	2009
IEC 61000 series	Electromagnetic Compatibility	/
BS IEC 60964	Nuclear Power Plants - Control Rooms - Design	2009
BS IEC 60965	Nuclear Power Plants - Control Rooms - Supplementary Control Room for Reactor Shutdown Without Access to the Main Control Room	2016

Standards Number	Title	Date Issued
IEC 62342	Nuclear Power Plants - Instrumentation and Control Systems Important to Safety - Management of Ageing	2007
BS IEC 62646	Nuclear Power Plants - Main Control Room - Computer Based Procedures	2016
IEC 61508	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems	2010
IEC 62671	Nuclear Power Plants - Instrumentation and Control Important to Safety - Selection and Use of Industrial Digital Devices of Limited Functionality	2013
IEEE 497	IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations	2010

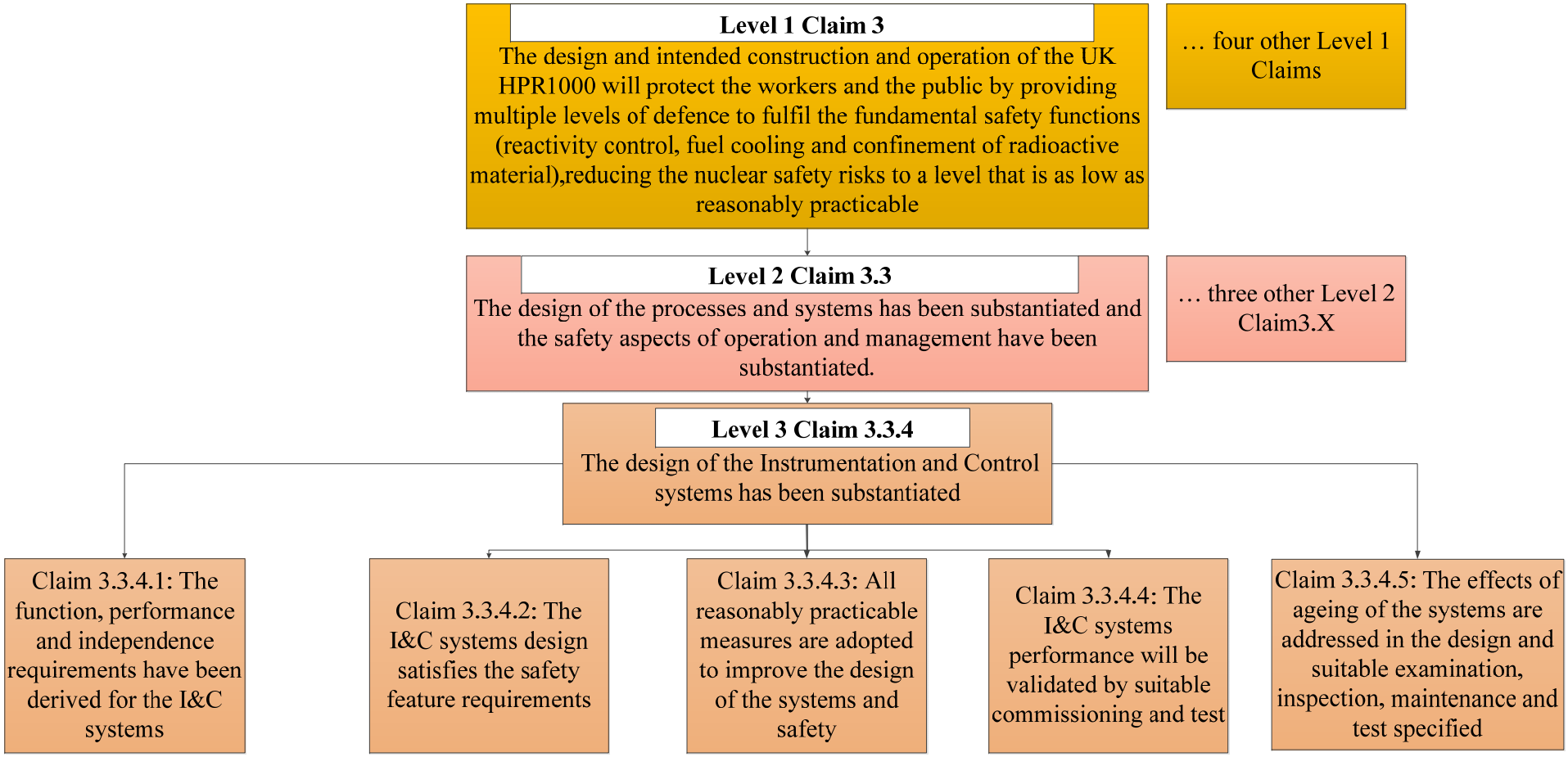
These codes and standards are applicable for the I&C design in the UK HPR1000. The further analysis work for the codes and standards is still in progress.

8.4 I&C Claim Architecture

This sub-chapter incorporates the I&C high level claims derived from Chapter 1. This sub-chapter also specifies the I&C claims for safety functions and safety features to link the I&C SSCs to the overall safety claims.

8.4.1 I&C High Level Claims Development Process

The I&C high level claims are derived from different levels of claims defined in Sub-chapter 1.6. The development process is shown in Figure F-8.4-1.



F-8.4-1 I&C Claims Development Process

The five I&C high level claims are developed corresponding to the five claims at the bottom of Figure F-8.4-1, which are as follows:

Claim I&C-C1 : The function, performance and independence requirements have been derived for the I&C systems;

Claim I&C-C2: The I&C systems design satisfies the safety feature requirements;

Claim I&C-C3: All reasonably practicable measures are adopted to improve the design of the systems and safety;

Claim I&C-C4: The I&C systems performance will be validated by commissioning and test;

Claim I&C-C5: The effects of ageing of the systems are addressed in the design and suitable examination, inspection, maintenance and testing specified.

The I&C systems claim names I&C-C1, I&C-C2, I&C-C3, I&C-C4 and I&C-C5 correspond to the claim names 3.3.4.1, 3.3.4.2, 3.3.4.3, 3.3.4.4 and 3.3.4.5 in Figure F-8.4-1 respectively.

8.4.2 I&C Claims Architecture

The claims and sub-claims regarding I&C are described in Table T-8.4-1, which can be summarised as follows:

a) I&C-C1 is mainly for I&C design basis derived from the plant design basis, including functional requirements, performance requirements, independence requirements and plant constraint requirements;

b) I&C-C2 is mainly for safety feature requirements, including reliability design, e.g. testability, Single Failure Criterion (SFC), redundancy, diversity, failsafe, mature technology and qualification;

c) I&C-C3 is mainly for ALARP requirements, including complying with standards and good practice and taking ALARP principles into account during design;

d) I&C-C4 is mainly for commissioning and test requirements;

e) I&C-C5 is mainly for examination, maintenance, inspection, test and ageing management.

For each claim or sub-claim, there are arguments and evidence to support it, either in Chapter 8 or in the supporting documents of Chapter 8. The names of corresponding sub-chapters to support each of the claims are described in Table T-8.4-1 and Appendix 8A for better traceability.

T-8.4-1 I&C Claims and Corresponding Sub-chapters

I&C High Level Claims	**I&C Sub-claims**		**Corresponding Sub-chapters**
I&C-C1: The function, performance and independence requirements have been derived for the I&C systems.	I&C-C1.1: The safety functional requirements are derived for the I&C systems.	I&C-C1.1.1: There are I&C systems reliability claims for their safety functions to be delivered.	8.5.6, 8.6.6, 8.7.6, 8.8.2.6, 8.8.3.6
		I&C-C1.1.2-1.1.5: Refer to Appendix 8A for 12 system function claims.	8.6.4, 8.7.4, 8.8.1.4, 8.8.2.4, 8.8.3.4
	I&C-C1.2: The I&C systems design incorporates DiD to protect against consequences of anticipated operational occurrences and accidents.		8.5.5, 8.6.6, 8.7.6, 8.8.1.6, 8.8.2.6, 8.8.3.6, 8.10
	I&C-C1.3: The I&C systems are categorised and classified appropriately according to their safety functions.		8.5.3.3, 8.6.6, 8.7.6, 8.8.1.6, 8.8.2.6, 8.8.3.6

I&C High Level Claims	I&C Sub-claims	Corresponding Sub-chapters
	I&C-C1.4: The I&C systems are designed to meet their performance requirements for their safety and operational functions.	8.6.6, 8.7.6, 8.8.1.6, 8.8.2.6, 8.8.3.6
	I&C-C1.5: The I&C systems are designed to withstand internal and external hazards.	8.5.7.8, 8.6.6, 8.7.6, 8.8.1.6, 8.8.2.6, 8.8.3.6, 8.13
	I&C-C1.6: The constraints from the plant design are derived.	8.5.1
I&C-C2: The I&C systems design satisfies the safety features requirements.	I&C-C2.1: The reliability design of I&C systems is commensurate with their safety significance.	8.5.7, 8.6.6, 8.7.6, 8.8.2.6, 8.8.3.6
	I&C-C2.2: The I&C equipment are qualified for their intended functions during their operational life.	8.14.1.2
I&C-C3: All reasonably practicable measures are adopted to improve	I&C-C3.1: The design, development and implementation process of the I&C systems comply with standards and good practice.	8.3, 8.14, 8.17

I&C High Level Claims	I&C Sub-claims	Corresponding Sub-chapters
the design and safety.	I&C-C3.2: The I&C systems design takes the ALARP principle into account.	8.17
I&C-C4: The I&C systems performance will be validated by suitable commissioning and test.	Not applicable.	8.14, 8.15
I&C-C5: The effects of ageing of the I&C systems are addressed in the design and suitable examination, maintenance, inspection and test are taken into account.	Not applicable.	8.16

8.5 Overall I&C Architecture

8.5.1 Introduction

The overall I&C architecture of the HPR1000 (FCG3) is the primary reference of the UK HPR1000 overall I&C architecture design, and RGP from other GDA projects and Operating Experience (OPEX) from other NPPs are also considered. The major design features including I&C platforms adopted for the UK HPR1000 are the same as the HPR1000 (FCG3). However, a new simple hardware based platform will be adopted to implement the diverse actuation functions of the KDS [DAS] in the UK HPR1000.

The principles of categorisation and classification, DiD requirements and plant conditions (DBC-1/2/3/4, Design Extension Condition A (DEC-A) and DEC-B) of each DiD level are taken into account in the overall I&C architecture design. The plant constraints are also considered in the overall I&C architecture design, which include interfaces with sensors and actuators, layout of the plant, power supply and grounding, operation requirements, etc.

The criteria of overall I&C architecture are mainly derived from IAEA SSG-39, Reference [9] including SFC, redundancy, independence, diversity, fail-safe, testability and maintainability, HF, cyber security, etc. The design information on these criteria is described in Sub-chapter 8.5.7.

The further information about overall I&C architecture of the UK HPR1000 I&C systems is described in the BSC of Overall I&C Architecture, Reference [29].

8.5.2 Claims of Overall I&C Architecture

The overall I&C architecture supports the following safety feature claims: I&C-C1.1.1, I&C-C1.2, I&C-C1.3, I&C-C1.5, I&C-C1.6 and I&C-C2.1.

Refer to Table T-8.4-1 for details.

8.5.3 Description of Overall I&C Architecture

8.5.3.1 Overall I&C Architecture

The overall architecture of I&C systems is divided into four levels:

a) Level 0: Process interface level

   This level is comprised of instrumentation and actuators. For details, refer to Sub-chapter 8.11.

b) Level 1: Control and protection level

   This level consists of I&C systems and processing equipment which are used to carry out signal acquisition, logic processing, control arithmetic calculation, data

communication, etc. The following I&C systems are mainly included in level 1:

1) Protection System (PS);
2) Safety Automation System (SAS);
3) Plant Standard Automation System (PSAS);
4) Diverse Actuation System (KDS [DAS]);
5) Severe Accident I&C System (KDA [SA I&C]);
6) Rod Position Indication and Rod Control System (RGL [RPICS]);
7) In-core Instrumentation System (RIC [IIS]);
8) Nuclear Instrumentation System (RPN [NIS]);
9) Plant Radiation Monitoring System (KRT [PRMS]);
10) Turbine Generator Control System (TGCS);
11) I&C system of Fuel Handling and Storage System (PMC [FHSS]);
12) I&C of Balance of Plant (BOP) Systems.

For details about level 1 I&C systems, refer to Sub-chapter 8.6 to Sub-chapter 8.10.

c) Level 2: Operation and information management level

This level consists of the HMIs in the MCR, Remote Shutdown Station (RSS) and Technical Support Centre (TSC), which can perform functions of information display and recording, equipment control, operation log and fault diagnosis. The following I&C systems are included in level 2:

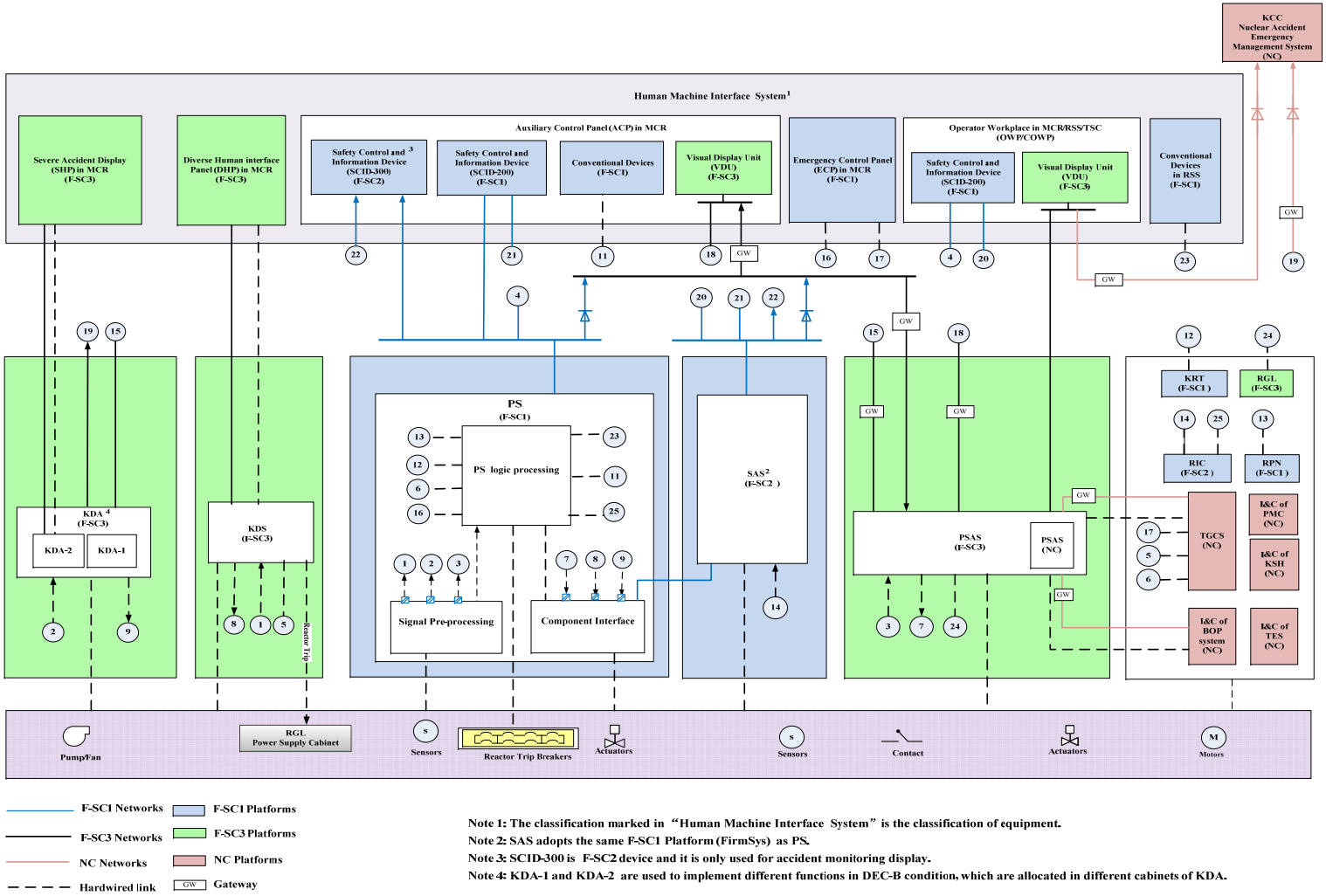
1) Plant Computer Information and Control System (KIC [PCICS]);
2) Main Control Room System (KSC [MCRS]);
3) Remote Shutdown Station System (KPR [RSSS]).

For details about level 2 I&C systems, refer to Sub-chapter 8.13.

d) Level 3: Plant information supervision level

This level is designed to get the necessary signals of the plant through the network from specific I&C systems for emergency management on site. The KCC [NAEMS] is the level 3 system. For further information about the KCC [NAEMS], refer to Sub-chapter 8.10.

The overall I&C architecture of the UK HPR1000 is shown in Figure F-8.5-1.



F-8.5-1 Overall I&C Architecture Chart

8.5.3.2 I&C Function Allocation

a) Principles of I&C function allocation

The I&C function allocation is the process of assigning all the I&C functions to the I&C systems. The factors taken into account in the I&C function allocation are as follows:

1) Function categorisation identified by fault analysis and assessment;

2) Level of DiD to achieve the required plant safety;

3) Requirements of reliability, including the diversity and redundancy;

4) Requirements against internal and external hazards.

Moreover, minimising the complexity of F-SC1 system is another principle of the function allocation, meanwhile it cannot increase complexity of the overall I&C architecture. In the I&C design, I&C functions with a different categorisation may be assigned to the same I&C system. In this case, the system is classified in accordance with the highest category of the allocated I&C functions, and it is necessary to ensure that the higher category functions are not jeopardised by the lower category functions.

b) Function allocation of I&C systems

The main functions allocated to I&C systems are described in Table T-8.5-1.

T-8.5-1 Function Allocation of Centralised I&C Systems

Centralised I&C System	**Main I&C Functions**
PS	The PS performs FC1 control and monitoring functions to bring the plant to the controlled state in DBC-2/3/4; Accident monitoring functions.
SAS	The SAS performs FC2 control and monitoring functions to bring the power plant from the controlled state to the safe state in DBC-2/3/4; DEC-A feature functions; Accident monitoring functions.

Centralised I&C System	Main I&C Functions
PSAS	The PSAS performs FC3 and NC functions. The PSAS controls and monitors the plant in normal operation conditions (DBC-1) and abnormal operation before a fault (DBC-2).
KDS [DAS]	The KDS [DAS] performs FC3 functions to bring the NPP to the final state in the event of DBC-2/3/4 (reactor in power mode) concurrently with CCF of the PS and SAS.
KDA [SA I&C]	KDA-1 performs the required functions to manage DEC-B and monitoring functions which are not required to perform a function in the event of a total loss of AC power supply. KDA-2 performs managing and monitoring functions under DEC-B with a 12-hour Uninterruptible Power Supply (UPS), which is required to perform functions in the event of a total loss of AC power supply.

The plant operation and manual control functions are performed by level 1 and related level 2 HMI equipment, and the function allocation of HMIs would be considered through the function allocation.

c) Allocation of DEC-A features functions

The required functions under DEC-A features are described in Sub-chapter 13.5. Depending on the nature of DEC-A features, the function allocation for DEC-A features is as follows:

1) The DEC-A features functions used for mitigating the consequences of DBC-2/3/4 (reactor in power mode) concurrent with the CCF of the PS and SAS are implemented in the KDS [DAS];

2) The functions in DEC-A features to be used for mitigating the consequences of the failure of mechanical systems are implemented in the SAS.

d) Allocation of accident monitoring functions

Accident monitoring functions in the UK HPR1000 are derived from plant requirements. The design of I&C systems to implement accident monitoring functions is based on IEEE 497, Reference [7]. Accident monitoring variables are a series of information that need to be monitored in the event of DBC-2/3/4. These variables provide the basis for the reactor operation and status estimation to

achieve and maintain a safe state. According to IEEE 497, Reference [7], accident monitoring variables are categorised as five types, namely Type A to Type E variables. The allocation of accident monitoring functions is based on the categorisation of the variables, which are allocated to the PS, SAS, PSAS, etc.

8.5.3.3 Categorisation and Classification

a) Function categorisation and system classification

The categorisation of I&C functions is consistent with the overall categorisation principle of the plant defined in Sub-chapter 4.4.

As addressed in Sub-chapter 4.4, the categorisation of I&C functions is classified to FC1, FC2 and FC3.

The safety classification is linked to the function categorisation scheme as follows:

1) F-SC1 is classified for SSCs that form a principal means of fulfilling FC1 functions;

2) F-SC2 is classified for SSCs that form a principal means of fulfilling FC2 functions;

3) F-SC3 is classified for SSCs that form a principal means of fulfilling FC3 functions.

The classification of I&C systems and equipment is consistent with their function categories. If I&C equipment fulfils multiple functions, the classification will depend on the function with the highest category. The classification of I&C systems in the UK HPR1000 is shown in Table T-8.5-2.

T-8.5-2 I&C System Classification[1]

I&C System	Highest Function Category	System Classification	Platform
PS	FC1	F-SC1	FirmSys
SAS	FC2	F-SC2	FirmSys
PSAS	FC3	F-SC3	HOLLiAS-N

[1] The correlation between UK HPR1000 function category and IEC function category is shown in Table T-8.5-3. The correlation between UK HPR1000 safety classification and IEC safety classification is shown in Table T-8.5-4.

I&C System	Highest Function Category	System Classification	Platform
KDS [DAS]	FC3	F-SC3[2]	FitRel
KDA [SA I&C]	FC3	F-SC3	SpeedyHold

T-8.5-3 Correlation between the UK HPR1000 Function Category and IEC 61513/61226 Function Category

UK HPR1000 Function Category	IEC 61513/61226 Function Category
FC1	Category A
FC2	Category B
FC3	Category C

T-8.5-4 Correlation between the UK HPR1000 Safety Classification and IEC 61513/61226 Safety Classification

UK HPR1000 Safety Classification	IEC 61513/61226 Safety Classification
F-SC1	Class 1
F-SC2	Class 2
F-SC3	Class 3

b) Seismic categories

According to the seismic categorisation principle of the plant, there are two seismic categories: SSE1 and SSE2. F-SC1 and F-SC2 systems are designed according to the seismic requirements of SSE1. The seismic requirements of F-SC3 systems are confirmed case by case. For example, the KDA [SA I&C] is categorised as SSE1 and its safety classification is F-SC3. For further information about SSE1 and SSE2, refer to Chapter 4.

[2] A gap of function categorisation and system classification and for KDS [DAS] between the current design and UK context is identified.

8.5.3.4 Interfaces between I&C Systems

a) Interfaces between level 1 systems

1) Interfaces between the PS and the SAS

- The Input/Output (I/O) bus is used to transmit control signals from the SAS to the Component Interface Module (CIM), and transmit feedback signals from the CIM to the SAS;
- Hardwired links are used to transmit signals between the PS and the SAS.

2) Interfaces between the PS and the PSAS

- Hardwired links are used to transmit signals from the Signal Pre-processing Modules (SPMs) of the PS to the PSAS;
- Hardwired links are used to transmit control signals from the PSAS to the CIMs to control a few actuators between the PS and the PSAS with isolation and priority management measures implemented in the CIMs;
- Hardwired links are used to transmit signals between the PS and the PSAS with electrical isolation measures adopted in the PS.

The unidirectional network is used to transmit the display and alarm information from the PS to the PSAS.

3) Interfaces between the PS and the KDS [DAS]

- Hardwired links are used to transmit sensor measurement signals from the SPMs of the PS to the KDS [DAS];
- Hardwired links are used to transmit actuation signals from the KDS [DAS] to the CIM to control the actuators between the PS and the KDS [DAS] with electrical isolation, and are used as the input signal of priority management logic implemented in the CIM.

4) Interfaces between the PS and the KDA [SA I&C]

- Hardwired links are used to transmit sensor measurement signals from the SPMs of the PS to the KDA [SA I&C];
- Hardwired links are used to transmit control signals from the KDA [SA I&C] to the CIM to control the actuators between the PS and the KDA [SA I&C] with electrical isolation and are used as the input signal of priority management logic implemented in the CIM.

5) Interfaces between the PS and the Non-centralised I&C systems

- Hardwired links are used to transmit the signals between the PS and the

Non-centralised I&C systems, e.g. the RPN (F-SC1), the KRT (F-SC1) and the TGCS. Electrical isolation measures are adopted between the systems with different safety classes.

6) Interfaces between the SAS and the PSAS

- Hardwired links are used to transmit signals between the SAS and the PSAS to implement the required functions;
- The unidirectional network is used to transmit the required information from the SAS to the PSAS.

7) Interfaces between the SAS and the Non-centralised I&C systems

- Hardwired links are used to transmit the signals between the SAS and the Non-centralised systems, e.g. the RIC [IIS]. Electrical isolation measures are adopted in the systems with higher classification.

8) Interfaces between the KDA [SA I&C] and the PSAS

- The network is used to transmit signals between the KDA [SA I&C] and the PSAS for display and control purposes.

9) Interfaces between the PSAS and the Non-centralised I&C systems

- There are some Non-centralised I&C systems which are connected to the PSAS by the network or hardwired links, e.g. the TGCS and the Programmable Logic Controllers (PLCs) of BOP.

b) Interfaces between level 1 equipment and level 2 equipment

1) The network is used to transmit the signals between the PS and the Safety Control and Information Device (SCID) 200 (on the Operator Workplace (OWP) and the ACP) and this communication is bi-directional;

2) The network is used to transmit the accident monitoring signals from the PS to the SCID-300 (on the OWP and the ACP) and this communication is unidirectional;

3) The network is used to transmit signals between the SAS and the SCID-200 (on the OWP and the ACP) and this communication is bi-directional;

4) The network is used to transmit the accident monitoring variables data signals from the SAS to the SCID-300 (on the OWP and the ACP) and this communication is unidirectional;

5) The unidirectional network is used to transmit the information from the PS and the SAS to the ACP Visual Display Unit (VDU);

6) Hardwired links are used to transmit the signals between the PS/SAS and the

conventional devices on the ACP for required functions;

7) Hardwired links are used to transmit the signals between the Emergency Control Panel (ECP) and the PS and the TGCS for emergency control;

8) Hardwired links are used to transmit the signals between conventional devices in the RSS and the PS;

9) The Diverse Human interface Panel (DHP) is the HMI for the KDS [DAS]. The connections between the DHP and the KDS [DAS] consists of a bi-directional network and hardwired links;

10) The Severe accident Human interface Panel (SHP) connects to the KDA [SA I&C] cabinet by hardwired links and bi-directional network for required functions;

11) The bi-directional network is used to transmit the signals between the VDUs in the MCR/RSS/TSC and the PSAS;

12) The bi-directional network is used to transmit the required information between the PSAS and the ACP VDU.

c) Interfaces to the KCC [NAEMS]

1) The unidirectional network is used to transmit the required information from the KDA [SA I&C] to the KCC [NAEMS];

2) The unidirectional network is used to transmit the required information from the KIC [PCICS] network to the KCC [NAEMS].

8.5.4 Layout and Interconnections

a) Layout of I&C equipment

The layout of I&C equipment meets the requirements of physical separation to protect against CCF due to internal hazards, e.g. internal fire and internal flooding. The transportation, installation, maintenance convenience and expandability are taken into account in I&C equipment layout design. The impacts of radiation are also considered in the I&C layout design, to minimise the amount of equipment located in high radiation areas to reduce the operations and maintenance in areas with high radiation. I&C equipment for level 1 and 2 is to be located in a mild (non-harsh) environment.

1) The layout of level 2 equipment

The level 2 I&C equipment is mainly located in the MCR, RSS and TSC. For details about the level 2 layout, refer to Sub-chapter 8.13.

2) The layout of level 1 equipment

The level 1 I&C equipment is arranged in the safeguard buildings, Nuclear Auxiliary Building (BNX), Radioactive Waste Treatment Building (BWX), Turbine Generator Building (BMX) and Conventional Island Electrical Building (BLX). Furthermore, the safeguard buildings are divided into three physically isolated zones (Safeguard Building A, Safeguard Building B and Safeguard Building C) which are separated with hazard barriers to provide protection against hazards, e.g. fire. The level 1 I&C equipment performing safety functions are arranged in the Safeguard Building A, Safeguard Building B and Safeguard Building C according to their division and function requirements.

For example, the ESFACs for division A, B and C and Reactor Protection Cabinets (RPCs) for channel I, II and III are arranged in the Safeguard Building A, Safeguard Building B and Safeguard Building C respectively, while the RPCs for channel IV are arranged in an independent room of Safeguard Building C to meet the requirements of physical separation from other channels.

3) The layout of level 0 equipment

The layout of level 0 instruments follows the layout design of liquid pipes of the plant process systems. Measures, e.g. space separation and physical protection, are implemented to cope with internal or external hazards.

b) Interconnections

Independent cable trays are designed for the I&C cabinets in accordance with their divisions. The cable trays are designed to avoid passing through different divisions, and special fire protection measures are adopted if there are exceptions. The distance separation measure between cable trays with a different safety classification in the same division is also considered. In addition, fire barriers are provided at the cable tray boundaries in each room to prevent the fire from spreading.

8.5.5 Defence in Depth

The overall I&C architecture design of the UK HPR1000 meets the DiD requirements of the plant which are described in Chapter 4. Detailed information is described in Table T-8.5-5.

T-8.5-5 Relationship between DiD of Plant and I&C Systems[3]

DiD Level	Objective	I&C Defence Line	I&C Function	I&C System
1	Prevention of abnormal operation and failures by design.	Preventive defence line	This level maintains the main power plant parameters within the normal operational range in DBC-1.	PSAS
2	Prevention and control of abnormal operation and detection of failures.		This level monitors and controls the plant in normal operation conditions. It maintains the main power plant parameters within the normal operational range in DBC-2 corresponding to abnormal operation before a fault.	
3	Control of faults within the design basis to protect against escalation to an accident.	Main defence line (3a)	This level mitigates the consequences of DBC-2/3/4 accidents to bring the plant to the safe state.	PS&SAS
		Diverse defence line (3b)	This level mitigates the consequences of the DBC-2/3/4（reactor in power mode）concurrent with the CCF of the PS and the SAS.	KDS [DAS]

[3] The I&C functions in each defence line are performed by level 1 systems and related level 2 HMI equipment, and the corresponding relationship and the further information between level 1 systems and level 2 HMI equipment are descripted in Sub-chapter 8.5.3 and the sub-chapters for the corresponding I&C systems. Therefore the level 2 HMI equipment is not described in this table.

DiD Level	Objective	I&C Defence Line	I&C Function	I&C System
		Risk reduction defence line (3b)	This level mitigates the consequences of DEC-A (failures in mechanical systems).	PS&SAS
4	Control of severe plant conditions in which the design basis may be exceeded, including protecting against further fault escalation and mitigation of the consequences of severe accidents.	Severe accident defence line	This level performs the managing and monitoring functions under DEC-B without a total loss of AC power supply.	KDA-1
			This level performs the managing and monitoring functions under DEC-B with a 12-hour UPS, during the event of a total loss of AC power supply.	KDA-2
5	Mitigation of radiological consequences of significant releases of radioactive material.	Emergency response defence line	This level supports the objectives of level 5 (on and off site emergency response).	KCC [NAEMS]

In addition, equipment diversity is also applied to the selection of the I&C platforms for I&C systems in different DiD lines. The platforms and technologies for I&C systems are shown in Table T-8.5-6.

T-8.5-6 Platforms and Technologies for I&C Systems

I&C System	Platform	Technology	Manufacturer
PSAS	HOLLiAS-N	Central Processing Unit (CPU)	HollySys
PS	FirmSys	CPU	CTEC
SAS	FirmSys	CPU	CTEC
KDS [DAS]	FitRel	FPGA	CTEC
KDA [SA I&C]	SpeedyHold	CPU	CTEC
KCC [NAEMS]	To Be Determined (TBD)	CPU	TBD

The following DiD design schemes of the I&C systems in the UK HPR1000 are described in order to support I&C-C1.2:

a) I&C systems are provided to detect and initiate actions for different levels of DiD of the plant;

b) The different levels of DiD for I&C systems are independent as far as practicable.

For further information about DiD for I&C systems, refer to the *BSC of Overall I&C Architecture*, Reference [29].

8.5.6 Targets of Numeric Reliability for I&C Systems

The I&C systems are expected to have reliability numerical targets that are commensurate with their safety importance. The reliability numeric targets of I&C systems are claimed as follows:

a) The reliability claim of the PS does not exceed 10^{-4} probability of failure on demand;

b) The reliability claim of the SAS (each division) does not exceed 10^{-2} probability of failure on demand;

c) The reliability claim of the KDS [DAS] does not exceed 10^{-1} probability of failure on demand[4];

d) The reliability claim of the KDA [SA I&C] does not exceed 10^{-1} probability of failure on demand.

For further information about reliability numerical targets, refer to R*eliability Targets of the I&C Systems for UK HPR1000*, Reference [30].

8.5.7 The Safety Features of I&C Systems

The following safety features of the I&C systems in the UK HPR1000 are described in this sub-chapter in order to support I&C-C2.1. These safety features are consistent with the specific requirements in Sub-chapter 4.4.

8.5.7.1 Single Failure Criterion

A credible single failure within the safety system does not prevent the initiation or accomplishment of a protective function at the system function level.

In the UK HPR1000 I&C design, the F-SC1 system includes sufficient redundancy and independency to meet the system performance requirements even if the system is degraded by a single failure. This redundancy begins with the sensors monitoring the variables and continues through to the signal processing and actuation processor.

The F-SC1 system is designed so that any single failure within the system does not preclude protective action at the “system level”.

The F-SC2 system generally meets the SFC so that it is possible to execute a safety function despite the potential failure of any single component designed to secure a safety function at the “function level”.

The definitions of the SFC at the “function level” and “system level” are described in *Methodology of Safety Categorisation and Classification*, Reference [31].

8.5.7.2 Redundancy

I&C systems are designed to be redundant to the degree necessary to meet the requirements for I&C reliability and the SFC.

In UK HPR1000 I&C design, redundancy of equipment in F-SC1 systems is provided to secure protective functions despite the loss of one of the redundant channels or divisions and simultaneously out of operation due to repair or maintenance to meet the SFC.

[4] A gap in reliability claim for the KDS [DAS] between the current design and UK context has been identified. The reliability claim of the KDS [DAS] is modified in the *Reliability Targets of the I&C Systems for UK HPR1000*, Reference [30].

8.5.7.3 Independence

Independence within the overall I&C architecture is a fundamental requirement to prevent the propagation of failures between each system, or between each division or channel, and to protect them from adverse influence of failures from outside the division or channel or from other systems.

In the UK HPR1000 I&C design, the following items are considered to meet the independence requirement:

a) Between redundant channels or divisions of safety I&C systems

Physical separation is used to achieve separation of redundant channels or divisions of F-SC1 and F-SC2 systems and cabinets by the layout design in different zones. For the redundant cables within F-SC1 and F-SC2 systems, physically separate cable routes, trays and penetrations are provided. If there is no space to use physical separation for entrance into a zone of redundant cables, the barriers and analyses are provided for the independence of the circuit.

The F-SC1 systems are not dependent upon any information or resource originating or residing outside their own safety channels to accomplish their safety functions. However, it is recognised that channel voting logic receives inputs from multiple safety channels.

There are data transmissions between redundant channels or divisions in F-SC1 and F-SC2 systems by optical communication links and hardwired links. Communication isolation and electrical isolation are employed to preserve the independence of the channels or divisions.

b) Between safety I&C systems and effects of DBC

In order to avoid CCF of potential effects caused by DBC, F-SC1 and F-SC2 equipment are designed to mitigate the consequences of a specific DBC by using physical separation to the degree necessary to retain the capability of these systems. For the F-SC1 and F-SC2 cabinets, they are arranged in the safeguard buildings which cannot be affected by DBC in the Nuclear Island (NI) buildings. Additionally, equipment qualification is another method to be used to meet the independence requirement. For example, equipment qualification of F-SC1 and F-SC2 sensors is implemented to verify their intended functions under their expected environmental conditions.

c) Between safety I&C systems and other systems

There is data transmission between safety systems and other systems in the UK HPR1000 I&C design. For communication links, unidirectional transmission from higher class system to lower class system is allowed, e.g. from the PS and the SAS to the VDU for OWP/Compact Operator Workplace (COWP).

Meanwhile, communication transmission from lower class systems to higher class systems is normally forbidden, and exceptional cases are analysed in order to ensure that the higher class systems are not jeopardised by lower class systems.

For hardwired links, signals between safety systems and control systems are transmitted by electrical isolation. The isolation devices are part of the safety I&C systems and are tested to confirm that credible failures at the output of the isolation devices do not prevent the associated safety system meeting its performance requirements. The credible failures are physical damage, short circuits, open circuits, etc.

8.5.7.4 Diversity

Diversity is the means by which two or more redundant systems or components are present to perform an identified function, where the different systems or components have different attributes so as to reduce the possibility of CCF.

The diversity principle is applied to the overall design of I&C systems of the UK HPR1000 through signal diversity and equipment diversity to cope with CCF.

a) Signal diversity: a safety action is initiated based upon the value of different plant parameters. The reactor trip function in the PS can be initiated by at least two different parameters corresponding to the same Postulated Initiating Event (PIE) in the I&C design;

b) Equipment diversity: achieved by hardware that employs different technology, e.g. analogue equipment versus digital equipment. For example, when the PS and the SAS (the main defence line 3a) are unavailable due to the CCF of software, the KDS [DAS] (the diverse defence line 3b) can perform the required functions. The PS and the SAS are implemented by digital technology, while the KDS [DAS] will be implemented by simple hardware.

8.5.7.5 Fail-safe

Systems and components important to safety are designed for fail-safe behaviour, as appropriate, so that their failure or the failure of a support feature does not prevent the performance of the intended safety functions.

In UK HPR1000 I&C design, a digital self-diagnosis mechanism is used to degrade the voting logic of the reactor trip function into a safer state when multiple failures exist so that the fail-safe feature can be guaranteed. If a voting logic module receives an invalid input or detects a problem in the communication by self-diagnosis, it will perform an automatic degrade to inhibit the invalid input. In general, for 2 out of 4 logic, the invalid inputs are handled as follows:

a) If one input is invalid, the logic is degraded from 2 out of 4 to 2 out of 3;

b) If two inputs are invalid, the logic is degraded from 2 out of 4 to 1 out of 2;

c) If three inputs are invalid, whether the logic triggers the safety action or not depends on the PS functional requirements.

To perform turbine trip, the PS emits a de-energised actuation command from each channel to the TGCS.

8.5.7.6 Testability and Maintainability

a) Testability

Self-diagnosis and alarms or anomalous indication functions are applied to I&C systems to confirm the integrity in I&C components, and the contents that cannot be covered by self-diagnosis in I&C systems can be detected by periodic tests.

In the UK HPR1000 I&C design, the built-in diagnosis provides a mechanism for periodically verifying the operability of modules in the digital control system. Continuous on-line error checking also detects and locates failures.

The capability for periodic tests and calibration of safety system equipment are provided while retaining the capability of the safety systems to accomplish their safety functions.

In the UK HPR1000 I&C design, test from the sensor inputs of F-SC1 system to the actuated equipment is accomplished through a series of overlapping sequential tests with the majority of the tests capable of being performed with the plant at full power. This test does not adversely affect the safety function in the F-SC1 system. Where the periodic tests during the power operation would upset plant operation or damage equipment, these periodic tests are performed during the shutdown condition.

F-SC1 and F-SC2 systems are designed to permit periodic tests in order to confirm their ability to perform their required functions. F-SC3 systems are also designed to permit periodic tests except for the case where continuous operation is required.

b) Maintainability

Fault diagnosis of components in the I&C systems is applied. The fault alarm and display can be provided timely for operators. The I&C components support online maintenance without affecting the implementation of safety functions. Maintenance tools are adopted in the I&C systems for the functions of monitoring, configuration software monitoring, fault diagnosis, parameter modification and configuration software modification.

The channel bypass permits the replacement of malfunctioning sensors or channel components without jeopardising plant availability, while still meeting the SFC.

8.5.7.7 Priority Rule

In some situations, contradictory commands are emitted coincidentally by different I&C systems to control the same actuator in UK HPR1000 I&C design. Therefore, priority rules are required in order to obtain the most appropriate action.

The following general rules are applied to actuators:

a) Commands from higher category functions have priority over commands from lower category functions, and the commands from high to low are arranged as follows:

   1) Commands for FC1 function;

   2) Commands for FC2 function;

   3) Commands for FC3 function;

   4) Commands for NC function.

   The priority management between different I&C systems is performed by the CIM. The priority sequence of commands between I&C systems from high to low is: the PS, the KDS [DAS], the SAS, the KDA [SA I&C] and the PSAS.

b) For the FC1 functions, the principle of priority from high to low is arranged as follows:

   1) Load shedding signal;

   2) Automatic protection;

   3) Manual protection.

c) For the FC2, FC3 and NC functions, the principle of priority from high to low is arranged as follows:

   1) Component and system protection;

   2) Automatic or manual action (according to the functional requirements).

8.5.7.8 Internal and External Hazards

The following design for internal and external hazards of the I&C systems in the UK HPR1000 is described in this sub-chapter in order to support I&C-C1.5.

a) The internal and external hazards for I&C systems are identified from the plant design basis.

   The definition of internal hazards of the UK HPR1000 is described in Chapter 19.

   The internal hazards considered in the I&C design include internal fire, internal flooding, Electromagnetic Interference (EMI) and others (e.g. dropped loads, high

energy pipe failures and internal missiles and internal explosion).

The definition of external hazards of the UK HPR1000 is described in Chapter 18.

The external hazards considered in the I&C design include earthquake, EMI, external flooding and aircraft crash.

b) The I&C systems and equipment are protected against the effects of internal and external hazards.

1) For internal fire, the adopted layout design of I&C systems deals with it. The I&C equipment of different divisions (or channels) is allocated to different fire compartments (or fire zones). The appropriate fire prevention, isolation and ventilation measures are taken in these different compartments. Internal fire is considered in MCR design, and the KPR [RSSS] is used to deal with internal fires in the MCR. Fire detection and fire fighting are designed to provide a timely alarm in the event of fire and/or its quick extinguishing. This will minimise the adverse effects on items important to safety and to personnel.

2) For internal flooding, separation and barriers (e.g. walls, floors, doors and building drainage system) are taken into account to cope with the risk of internal flooding.

3) For other internal hazards (e.g. dropped loads, high energy pipe failures, internal missiles and internal explosion), the risks caused by these internal hazards to I&C systems are minimised by the reasonable environmental qualification, layout design or the physical protection measures on the site.

4) For earthquakes, seismic qualification is applied to I&C systems to substantiate that they can perform expected functions under certain situations.

5) For EMI, EMC qualification and grounding design are applied to I&C systems to substantiate that they can still perform their expected functions. The following measures are also considered for minimising the generation and coupling of electromagnetic noise:

- Separation and isolation between the I&C signal cables and the power cables;
- Shielding of equipment and cables;
- Proper grounding of the I&C equipment, raceways, cabinets, components and cable shields.

6) For external flooding and aircraft crash, the layout design of I&C systems is

taken into account based on the structures design of the plant to minimise the effects of hazards on I&C functions.

7) Other external hazards, e.g. meteorological hazards, are addressed through the structures design or Heating, Ventilation and Air Conditioning (HVAC) design of the plant.

8.5.7.9 I&C Cyber Security

I&C systems will adopt technical and management measures to ensure the confidentiality, integrity and availability of computer based I&C systems. Cyber security is considered during the entire lifecycle of the I&C system, from design through to decommissioning, thus ensuring the highest possible assurance that digital processors, communications systems and networks are adequately protected. During the UK HPR1000 I&C cyber security design, the following requirements will be considered:

a) Definition of roles and responsibilities;

b) Implementation of training and subsequent management processes to ensure that personnel are a suitably qualified and experienced person;

c) The undertaking of risk assessments to ensure sufficient mitigations are applied;

d) Implementation of technical and management controls for the following:

   1) Access control;

   2) Data security;

   3) Communication security;

   4) Platform and application security;

   5) Maintenance security.

e) Establishment of emergency response management plans;

f) Confidence of security in the supply chain with a particular focus on “off the shelf” components.

8.5.7.10 Human Factors

The user interface and workspace for I&C systems and equipment, e.g. the layout of I&C equipment rooms and the design of I&C cabinets and I&C cable trays, have considered the implementation of HF guidelines, which are presented in Chapter 15. These HMIs and workspaces will be reviewed from the HF perspective to ensure that the human actions which are performed are reliable and feasible.

8.6 F-SC1 Centralised I&C System

The F-SC1 Centralised I&C system is named as the PS.

8.6.1 Introduction

The PS performs FC1 functions to bring the plant to the controlled state after DBC-2/3/4. It collects the plant parameters for the detection of DBCs and once the plant parameters reach or exceed the specified setpoints, it performs the protection functions automatically or manually.

The PS contributes to the following three basic safety functions:

a) Reactivity control;

b) Heat removal;

c) Confinement of radioactive material.

In addition to the aforementioned safety functions, the PS is used to perform the supporting functions which are named as the extra safety functions.

8.6.2 Claims for Safety Functions

The PS supports the following safety function claims: I&C-C1.1.2-R2, I&C-C1.1.2-R3, I&C-C1.1.3-H1, I&C-C1.1.3-H2, I&C-C1.1.3-H3, I&C-C1.1.3-H4, I&C-C1.1.4-C2, I&C-C1.1.4-C3, I&C-C1.1.4-C4 and I&C-C1.1.5-E1.

Refer to Appendix 8A for details.

8.6.3 Claims for Safety Features

The PS supports the following safety feature claims: I&C-C1.1.1, I&C-C1.2, I&C-C1.3, I&C-C1.4, I&C-C1.5 and I&C-C2.1.

Refer to Table T-8.4-1 for details.

8.6.4 System Function Description

The PS performs the functions of emergency reactor trip, engineered safety feature actuation and safety supporting systems actuation to ensure that the power plant reaches the controlled state.

The main automatic FC1 functions performed by the PS are as follows:

a) Reactor trip;

b) Turbine trip;

c) Safety injection;

d) Reactor Coolant System (RCP [RCS]) pump trip;

e) Safety Injection System (RIS [SIS])/Residual Heat Removal (RHR) train isolation;

f) RIS [SIS]/RHR pump trip;

g) Medium pressure rapid cooldown;

h) Emergency Feedwater System (ASG [EFWS]) actuation and isolation;

i) Atmospheric Steam Dump System (VDA [ASDS]) opening and isolation;

j) Main Steam Isolation Valve (MSIV) closure;

k) Full load line and low load line of Main Feedwater Flow Control System (ARE [MFFCS]) isolation;

l) Containment isolation;

m) Shutdown of the Chemical and Volume Control System (RCV [CVCS]) charging line and RCP [RCS] pumps seal injection;

n) RCV [CVCS] let down line isolation.

The manual FC1 functions performed by PS are listed as follows:

a) Manual reactor trip;

b) Manual ASG [EFWS] isolation;

c) Manual Medium Head Safety Injection (MHSI) actuation.

The PS also transmits the accident monitoring signals required during FC1 manual operations to the ACP, including steam line pressure, steam generator activity, spent fuel pool water level, reactor cavity and internal compartments water level, etc.

In addition, permissive functions are performed by the PS where the permissive signals are used to permit or inhibit the protection functions according to the plant state.

8.6.5 System Architecture

The PS contains four protection channels and three divisions as shown in Figure F-8.6-1. It includes the following I&C equipment:

a) Reactor Protection Cabinet (RPC)

The RPC is responsible for threshold comparison, voting and reactor trip initiation. There are four redundant protection channels: IP, IIP, IIIP and IVP.

Each channel is divided into two groups: group I and group II. The reactor trip commands from the two groups are combined with “OR” logic before being sent to the Reactor Trip Breakers (RTBs).

Each channel collects the threshold comparison results from the other channels by peer to peer data transmittal, and performs the voting and actuation logic.

The RPC also transmits signals for engineered safety feature actuation to the ESFAC by peer to peer data transmittal.

The RPC is implemented by the digitalised FirmSys platform.

b) Engineered Safety Feature Actuation Cabinet (ESFAC)

The ESFAC is responsible for actuation management of engineered safety features and related supporting systems. There are three independent divisions: A, B and C.

Each ESFAC collects partial trip signals from the four redundant channels of the RPC by peer to peer data transmittal, and performs the voting and actuation logic.

The ESFAC transmits output signals to the CIM by the hardwired link.

The ESFAC is implemented by the digitalised FirmSys platform.

c) Safety Control Cabinet (SCC)

The SCC is responsible for FC1 closed loop control functions. It is also used to process and transmit the accident monitoring signals to the ACP. There are three independent divisions: A, B and C.

Each SCC collects partial trip signals from the four redundant channels by peer to peer data transmittal, and performs the voting and closed loop control logic.

The SCC transmits output signals to the CIM by hardwired link.

The SCC is implemented on the digitalised FirmSys platform.

d) Signal Pre-processing Cabinet (SPC)

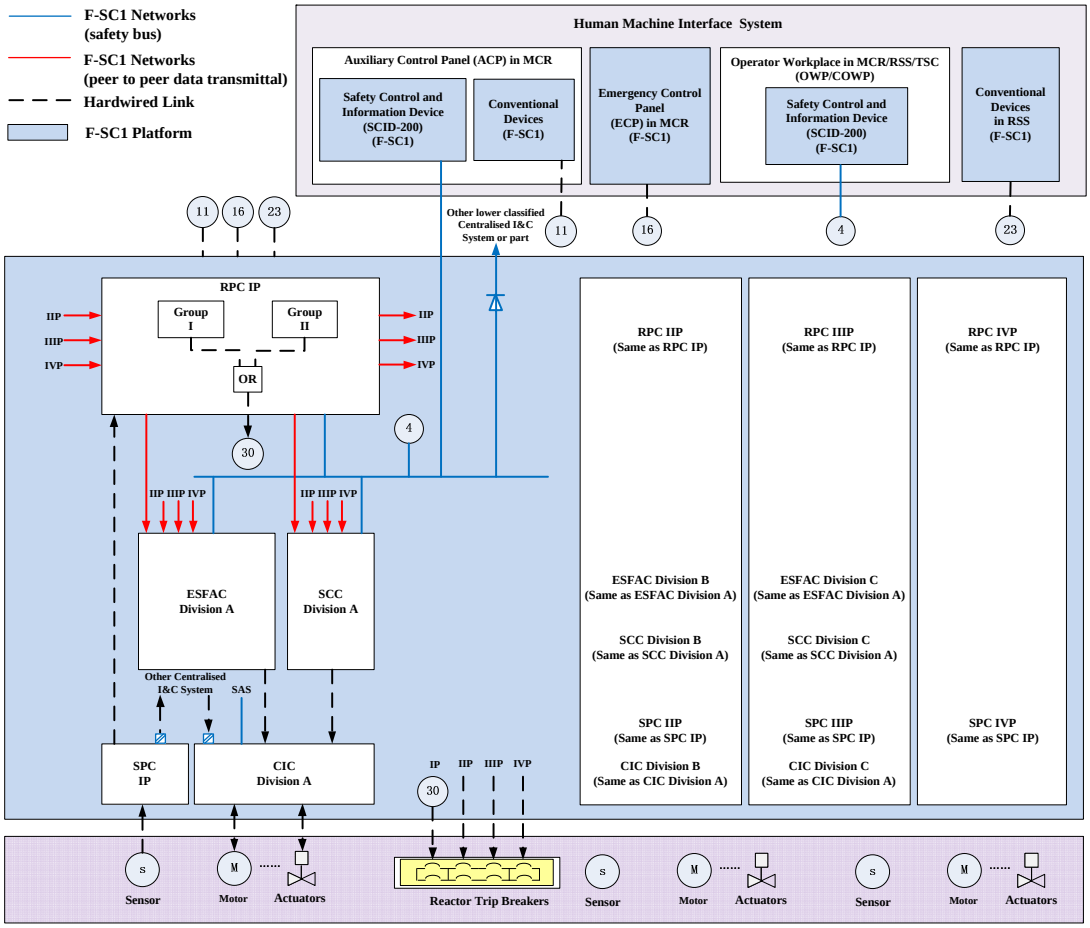
The SPC is responsible for the signal acquisition and pre-processing from sensors and distributing them to the different Centralised I&C systems with isolation measures. There are four independent channels: IP, IIP, IIIP and IVP.

The SPC is implemented by the hardware-based analogue device.

e) Component Interface Cabinet (CIC)

The CIC consists of CIMs and relevant electrical equipment. The CIM performs priority management of the control or actuation commands coming from different Centralised I&C systems or components including the ESFAC, KDS [DAS], SAS, PSAS and KDA [SA I&C]. There are three independent divisions: A, B and C.

The CIC is implemented by Complex Programmable Logic Device (CPLD) technology.



F-8.6-1 Architecture of the PS

8.6.6 System Design Description

a) Classification of system

The PS is classified as F-SC1.

The equipment of the PS complies with the requirements of SSE1 in order to maintain the availability of safety functions during or after a seismic event.

b) Reliability

The reliability claim of the PS does not exceed 10^{-4} probability of failure on demand.

c) Contribution to DiD

The PS provides the main defence line to mitigate the consequences of DBC-2/3/4 in the DiD structure which is described in Sub-chapter 8.5.5.

d) Single failure criterion

The SFC is satisfied by the redundant system configurations with independence.

For the four redundant channels, any failure of a single component does not prevent the PS from performing protection functions.

For the three independent divisions, the PS loses the control of devices if their corresponding division fails. The other two PS divisions and their corresponding mechanical systems can still secure the safety functions required in DBC-2/3/4.

e) Independence

The following measures are taken to meet the independence requirements:

1) The different channels or divisions of the PS are located in different zones to ensure physical isolation to meet the independence requirements. The general layout information of PS cabinets is described in Sub-chapter 8.5.4;

2) Communication isolation measures between redundant channels or from channels to divisions are used to meet the communication independence requirements. The buffering circuit is used in the F-SC1 platform to separate the higher safety category functions from lower safety category functions by the ways of the independent processor (communication process module is different from logic process module), deterministic communication features and the broadcast communication mode. Unidirectional communication is used for the data transmission from the PS to the other Centralised I&C systems;

3) The PS is isolated from other safety class systems by using F-SC1 isolation devices or fibre optical cables such that any failure in other safety class system does not cause a loss of required safety functions;

4) Each channel (or division) receives dedicated power sources.

f) Diversity

The PS measures and processes, where possible, two diverse process variables for the reactor trip functions under DBC-2. The collection and processing functions of the diverse variables are allocated in the two groups respectively.

In addition, the functions of the PS are backed up by the KDS [DAS] which is presented in Sub-chapter 8.8.3.

g) Fail-safe design

The following measures are considered to meet the fail-safe design requirements:

1) In case of loss of the I&C power supply, the RTBs are opened to cut off the power of the RGL, then all the control rods drop into the reactor core by gravity;

2) For the voting logic degradation of the PS, refer to Sub-chapter 8.5.7.

h) Periodic test

Periodic test is employed in the PS to ensure the reliability and operability of the system. During the test, the protection functions for reaching the controlled state under DBC-2/3/4 are available.

i) Internal and external hazards

The I&C equipment of the PS is protected against damaging effects resulting from the following internal hazards: internal fire, internal flooding, EMI and others (e.g. dropped loads, high energy pipe failures and internal missiles and internal explosion).

The external hazards considered in the PS design include: earthquake, EMI, external flooding and aircraft crash.

For the measures against the internal and external hazards, refer to Sub-chapter 8.5.7.

j) Performance requirements

The performance of the PS, including accuracy and response time, meets the functional requirements based on the safety analysis.

The response time between the PS receiving the measurement signals and sending out the actuation commands are as follows:

1) For most of the reactor trip functions, the response time does not exceed { }, while for over temperature or over power reactor trip functions the response time does not exceed { };

2) For those engineered safety feature actuation functions, the response time does not exceed { }.

k) Platform

All the PS functions are implemented on the FirmSys platform. For further information on the platform, refer to Sub-chapter 8.14.

l) Human machine interface

The SCIDs are the main HMIs of the PS, which are computer-based touch screens located at the OWP, ACP and COWP. The data transmission between the PS and the SCIDs is through the safety bus.

There are also some conventional devices on the ECP and ACP in the MCR used as the HMIs of the PS. The interconnections between the PS and the ECP and ACP conventional devices are through hardwired links.

In addition, the monitoring information of the PS is sent to the F-SC3 VDU of the

OWP, ACP and COWP. For further information of HMIs, refer to Sub-chapter 8.13.

8.7 F-SC2 Centralised I&C System

The F-SC2 Centralised I&C system is named as the SAS.

8.7.1 Introduction

The SAS performs automatic and manual functions as well as providing the monitoring information to bring the plant from the controlled state to the safe state after DBC-2/3/4. It also performs the DEC-A features functions to mitigate the consequences of the failure of mechanical systems.

The SAS contributes to the following three basic safety functions:

a) Reactivity control;

b) Heat removal;

c) Confinement of radioactive material.

In addition, the SAS is also used to perform supporting functions (e.g. cooling water system, ventilating and air conditioning system, etc.).

8.7.2 Claims for Safety Functions

The SAS supports the following safety function claims: I&C-C1.1.2-R2, I&C-C1.1.2-R3, I&C-C1.1.3-H1, I&C-C1.1.3-H2, I&C-C1.1.3-H3, I&C-C1.1.3-H4, I&C-C1.1.4-C2, I&C-C1.1.4-C3, I&C-C1.1.4-C4 and I&C-C1.1.5-E1.

Refer to Appendix 8A for details.

8.7.3 Claims for Safety Features

The SAS supports the following safety feature claims: I&C-C1.1.1, I&C-C1.2, I&C-C1.3, I&C-C1.4, I&C-C1.5 and I&C-C2.1.

Refer to Table T-8.4-1 for details.

8.7.4 System Function Description

The SAS mainly performs the following manual functions:

a) Manual starting of the safety injection pumps;

b) Manual stopping of the safety injection pumps;

c) Manual switch of MHSI on its large mini-flow line;

d) Manual connection of RIS [SIS] in RHR mode;

e) Manual isolation of RIS [SIS] in RHR mode;

f) Manual isolation of RIS [SIS] accumulators;

g) Manual stopping of the main coolant pumps;

h) Manual actuation of Emergency Boration System (RBS [EBS]);

i) Manual isolation of RBS [EBS];

j) Manual stopping of the pressuriser heaters;

k) Manual opening/closing pressuriser normal spray valves;

l) Manual isolation of containment isolated valves;

m) Manual VDA [ASDS] opening/closing;

n) Manual actuation of automatic cooldown via the VDA [ASDS];

o) Manual increase of the VDA [ASDS] setpoints;

p) Manual isolation of the MSIV;

q) Manual opening/closing the transfer blowdown lines between steam generators;

r) Manual isolation of steam generator blowdown lines;

s) Manual isolation of the full load line and low load line of the ARE [MFFCS].

The SAS performs the following automatic functions and monitoring functions:

a) Automatic isolation of the RCP [RCS] pumps thermal barrier;

b) Automatic opening of the ASG [EFWS] flow control valve;

c) Automatic isolation of the low head safety injection pump intake valve and miniflow line;

d) Automatic isolation of the containment on high activity in the RCP [RCS];

e) Monitoring of the accident variables.

The SAS performs the following DEC-A features functions:

a) Secondary Passive Heat Removal System (ASP [SPHRS]);

b) Extra Cooling System (ECS [ECS]);

c) Containment Heat Removal System (EHR [CHRS]);

d) Station Black Out (SBO) diesel generator;

e) Safety Chilled Water System (DEL [SCWS]);

f) Manual feed and bleed operation;

g) Manual low pressure full-speed cooldown operation.

8.7.5 System Architecture

The architecture of the SAS is designed according to functional requirements and is shown in Figure F-8.7-1. The SAS includes the following I&C equipment:

a) Safety Automation Cabinet (SAC)

The SAC is responsible for control and monitoring of FC2 functions, including DEC-A features functions. There are three independent divisions: A, B and C.

The SAC mainly receives signals:

1) from the SPC by hardwired link;

2) from the CIC by safety network;

3) from the SCID of the ACP and OWP by safety bus.

The SAC mainly sends signals:

1) to the CIC by safety network;

2) to the SCID of the ACP and OWP by safety bus.

The SAC is implemented on the digitalised FirmSys platform.

b) Core Cooling Monitoring Cabinet (CCMC)

The CCMC is used to monitor core outlet temperature, Reactor Pressure Vessel (RPV) level and calculate the saturation value of the core outlet temperature. The core outlet temperature signal is acquired from the RIC [IIS]. The RPV level signal is acquired from the SPC. These signals and the saturation value of the core outlet temperature are also used for accident monitoring, and are sent to the conventional devices in the ACP via the hardwired link. There are two independent divisions: A and B.

The CCMC is implemented on the digitalised FirmSys platform.

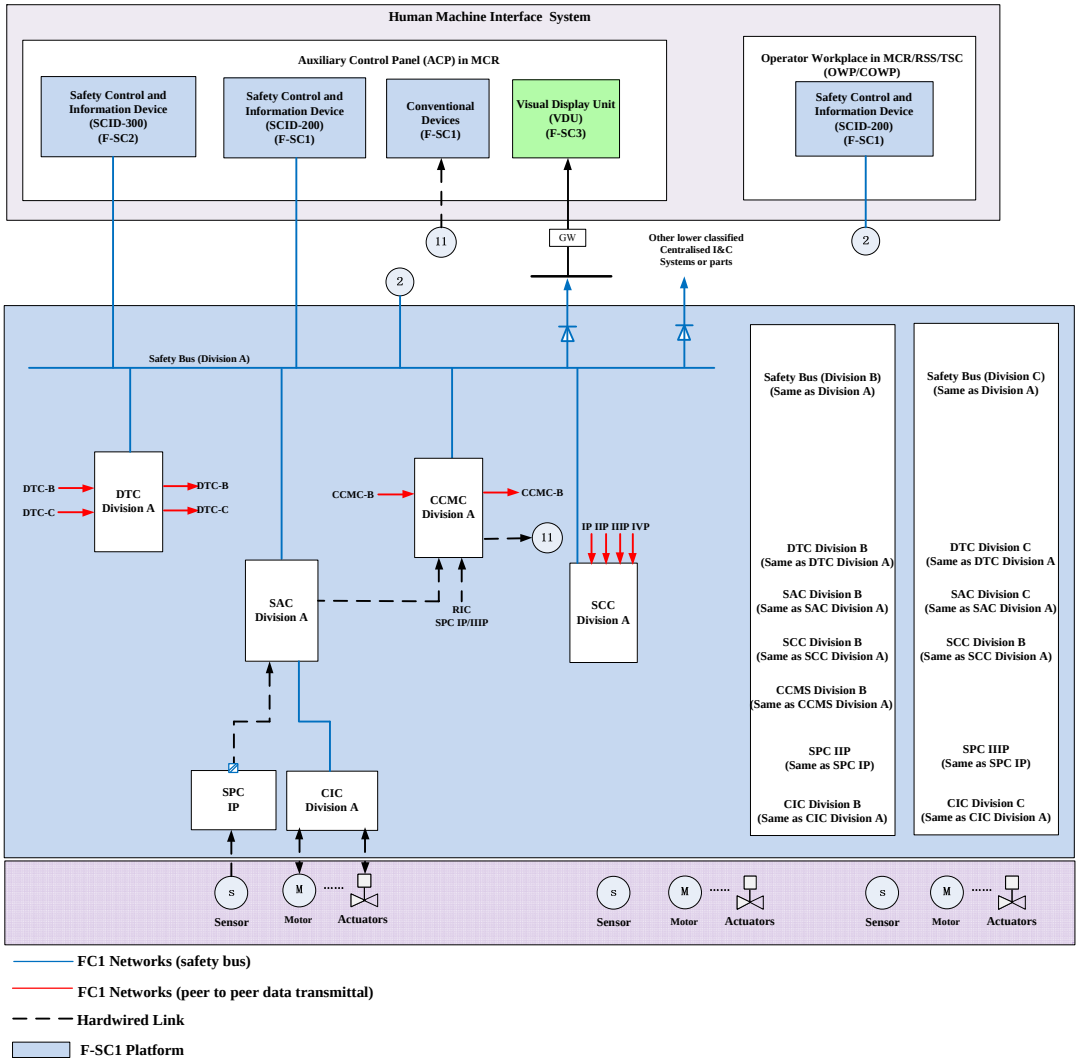
c) Data Transmission Cabinet (DTC)

The DTC is used to perform data transmission between different divisions. There are three independent divisions: A, B and C.

The DTC receives signals from the safety bus of the same division and sends signals to the DTC of the other two divisions by peer to peer data transmittal.

The DTC is implemented on the digitalised FirmSys platform.

In addition, the SCC transmits accident monitoring signals to the ACP. The SCC receives signals from the redundant channels by peer to peer data transmittal, performs the voting logic and sends the accident monitoring signals to the ACP by safety bus.



F-8.7-1 Architecture of the SAS

8.7.6 System Design Description

a) Classification of system

The SAS is classified as F-SC2.

The I&C equipment of the SAS is categorised as SSE1.

b) Reliability

For each division, the reliability claim of the SAS does not exceed 10^{-2} probability of failure on demand.

c) Contribution to DiD

The SAS contributes to the main defence line of the DiD structure, which is described in Sub-chapter 8.5.5.

d) Redundancy

For the SAS, three independent divisions are provided corresponding to the redundant design of mechanical systems.

e) Independence

The following measures are taken to meet the independence requirements:

1) The different divisions of the SAS are located in different zones to ensure physical isolation to meet the independence requirements. The general layout information of SAS cabinets is described in Sub-chapter 8.5.4;

2) Communication isolation measures between the different divisions are used to meet the communication independence requirements. Unidirectional communication is used for the data transmission from the SAS to the lower safety class Centralised I&C systems;

3) The SAS is isolated from other safety class systems by using F-SC1 isolation devices or fibre optical cables such that any failure in other safety class system does not cause a loss of required safety functions;

4) Each division receives dedicated power sources.

f) Diversity

The SAS is backed up by the KDS [DAS] which is presented in Sub-chapter 8.8.3.

g) Internal and external hazards

The I&C equipment of the SAS is protected against the damaging effects resulting from the following internal hazards: internal fire, internal flooding and others (e.g. dropped loads, high energy pipe failures, internal missiles and internal explosion).

The external hazards considered in the SAS design include: earthquake, EMI, external flooding and aircraft crash.

For the measures taken against the internal and external hazards, refer to Sub-chapter 8.5.7.

h) Performance requirements

The maximum time from the variation of a logic input to display is 1s. The maximum time from the variation of an analogue input to display is 1.5s. The maximum time from the receipt of a manual command to the output interface is 1s.

For automatic command:

1) From acquisition of a logic input and calculation of a logic command to an output interface, the maximum time is { };

2) From acquisition of an analogue input and calculation of a logic or analogue command to the output interface, the maximum time is { };

3) For the rapid analogue control loop, the maximum time is { }.

i) Platform

The SAS is implemented on the FirmSys platform. For further information on the platform, refer to Sub-chapter 8.14.

j) Human machine interface

The SCID, ACP and COWP are the main HMIs of the SAS. The conventional devices on the ECP and ACP are also used as the HMIs of the SAS. The equipment-level manual control functions are implemented on SCIDs and the conventional devices, but the monitoring functions are implemented on the F-SC3 VDU of the OWP/COWP and ACP. As a back-up HMI, the ACP also provides monitoring functions through SCIDs and conventional devices. In particular, the F-SC2 SCID-300 is used for displaying and recording accident variables. For further information of HMIs, refer to Sub-chapter 8.13.

8.8 F-SC3 Centralised I&C Systems

8.8.1 Plant Standard Automation System (PSAS)

8.8.1.1 Introduction

The PSAS performs FC3/NC functions to monitor and control the plant in normal operation conditions (DBC-1 and DBC-2 corresponding to abnormal operation before a fault). The PSAS is an operational system that contributes to the following three basic safety functions in normal operation conditions:

a) Reactivity control;

b) Heat removal;

c) Confinement of radioactive material.

In addition to the safety functions above, the PSAS is used to implement the supporting functions which are named as the extra safety functions.

In particular, the following important functions of the plant are performed by the PSAS:

a) Reactor power control;

b) Reactor coolant temperature control;

c) Pressuriser pressure control;

d) Pressuriser level control;

e) Steam generator level control;

f) Steam dump control.

8.8.1.2 Claims for Safety Functions

The PSAS supports the following safety function claims: I&C-C1.1.2-R1, I&C-C1.1.2-R2, I&C-C1.1.2-R3, I&C-C1.1.3-H1, I&C-C1.1.3-H2, I&C-C1.1.3-H3, I&C-C1.1.3-H4, I&C-C1.1.4-C2, I&C-C1.1.4-C4, I&C-C1.1.5-E1 and I&C-C1.1.5-E2.

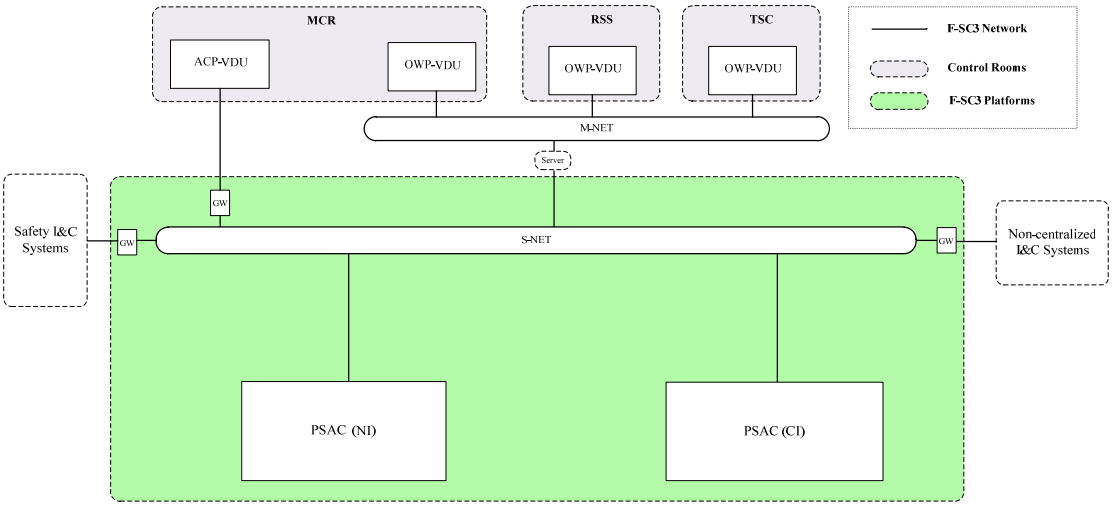
Refer to Appendix 8A for details.

8.8.1.3 Claims for Safety Features

The PSAS supports the following safety feature claims: I&C-C1.2, I&C-C1.3, I&C-C1.4 and I&C-C1.5. Refer to Table T-8.4-1 for detailed information on these claims.

8.8.1.4 System Architecture

The PSAS consists of F-SC3 classified cabinets which are arranged in NI buildings and Conventional Island (CI) buildings separately. The architecture of the PSAS is shown in Figure F-8.8-1.



F-8.8-1 Architecture of the PSAS

The PSAS cabinets are named as the Plant Standard Automation Cabinet (PSAC), including the following two parts:

a) PSAC (NI): The cabinets are arranged in NI buildings to perform the monitoring and control functions of the plant in normal operation conditions;

b) PSAC (CI): The cabinets are arranged in CI buildings to perform the monitoring and control functions of the plant in normal operation conditions.

All the PSAS cabinets are connected together through the System Network (S-NET), which has interfaces with safety I&C systems (e.g. PS, SAS) and Non-centralised I&C systems through the Gateway (GW).

8.8.1.5 System Function Description

The PSAS performs manual and automatic actuation of mechanical systems or components. It can also provide information (feedback signals, measurements, alarms, etc.) to the operators. The main functions performed by the PSAS are given as follows:

a) Reactor power control

The reactor power control system balances the power between the primary loop and the secondary loop by adjusting the position of the regulating rods (bank G and bank N) in the core, so that the power of the reactor quickly matches the power of the secondary side.

b) Reactor coolant average temperature control

The reactor coolant average temperature control system allows the reactor coolant average temperature to be as close as possible to its setpoints, by adjusting the position of the regulating rods (bank R) in the core.

c) Primary coolant inventory control and pressuriser water level control

The primary coolant inventory is maintained by the chemical and volumetric control system. During normal operation of the plant, the pressuriser water level control is accomplished by controlling the let-down flowrate valves.

d) Pressuriser pressure control

The pressuriser pressure control system ensures that the pressuriser pressure is maintained at the setpoints during normal operation to prevent reactor trip or pressuriser safety valve movements during normal operating transients.

The pressure of the pressuriser is controlled by the electric heaters installed at the bottom of the pressuriser and the spray valve mounted at the top.

e) Steam dump control

The steam dump system reduces the magnitude of the nuclear steam supply system temperature and pressure transients resulting from large and rapid turbine load reductions by dumping main steam to the condenser, thereby providing an “artificial” load for the reactor. Steam dump control is accomplished by controlling the steam dump valves that discharge steam to the condensers.

f) Steam generator level control

The steam generator level control is designed to maintain the steam generator level at the setpoints to avoid reactor trip caused by liquid level fluctuations of the steam generator that are too large under normal operating conditions.

8.8.1.6 System Design Description

These requirements are met for all the automatic I&C safety functions performed by the PSAS.

a) Classification of system

This system is classified as F-SC3 and performs FC3 and NC functions.

The seismic categorisation of PSAS cabinets is required according to the categorisation of the functions case by case.

b) Contribution to DiD

The PSAS acts as the prevention line of the DiD structure, to monitor and control the plant in normal operation conditions and maintain the main power plant parameters within the normal operational range to avoid reactor trip or engineered safety feature actuation. The corresponding relation to the plant DiD levels is described in Sub-chapter 8.5.5.

c) Internal and external hazards

The I&C equipment of the PSAS is protected against the damaging effects resulting from internal hazards, e.g. internal fire, internal flooding, EMI and others (e.g. dropped loads, high energy pipe failures and internal missiles and internal explosion).

The external hazards considered in PSAS design include: earthquake (case by case), EMI and external flooding.

For the measures taken against the internal and external hazards, refer to Sub-chapter 8.5.7.

d) Performance requirements

The response time from “the command input to PSAS” to “the command output from PSAS to level 0” is less than 1s. The response time for automatic analogue control loops and on-off control loops is less than { }.

e) Platform

The PSAS is implemented on the HOLLiAS-N platform. For further information on this platform, refer to Sub-chapter 8.14.

f) Human machine interface

The monitoring and manual control functions of the PSAS are performed by VDUs on OWPs normally. These functions can also be performed by VDUs on the ACP when the VDUs on the OWP are unavailable. The monitoring and manual control functions of the PSAS can also be performed with VDUs on OWPs in the RSS when the MCR is not available. For further information of HMIs, refer to Sub-chapter 8.13.

8.8.2 Severe Accident I&C System (KDA [SA I&C])

8.8.2.1 Introduction

The KDA [SA I&C] is comprised of KDA-1 and KDA-2.

The KDA-1 performs DEC-B managing and monitoring functions which are not required in the event of a total loss of AC power supply.

The KDA-2 performs the DEC-B managing and monitoring functions with 12-hour UPS, which are required in the event of a total loss of AC power (loss of offsite power, Emergency Diesel Generators (EDGs) and SBO diesel generators).

The KDA [SA I&C] contributes to the two main safety functions:

a) Heat removal;

b) Confinement of radioactive material.

In addition, the KDA [SA I&C] is used to deliver supporting functions which are named the extra safety functions.

8.8.2.2 Claims for Safety Functions

The KDA [SA I&C] supports the following safety function claims: I&C-C1.1.3-H3, I&C-C1.1.4-C3, I&C-C1.1.4-C4 and I&C-C1.1.5-E1.

Refer to Appendix 8A for details.

8.8.2.3 Claims for Safety Features

The KDA [SA I&C] supports the following safety feature claims: I&C-C1.1.1, I&C-C1.2, I&C-C1.3, I&C-C1.4, I&C-C1.5 and I&C-C2.1.

Refer to Table T-8.4-1 for details.

8.8.2.4 System Function Description

The KDA [SA I&C] implements the following functions:

a) RCP [RCS] depressurisation;

b) Core melt retention:

   1) Core outlet temperature monitoring;

2) RPV lower head outside wall temperature monitoring;

3) Reactor pit flooding and monitoring.

c) Manual opening of the severe accident relief valves;

d) Hydrogen mitigation;

e) Containment integrity:

1) Containment pressure monitoring;

2) Manual operation of the EHR [CHRS] and ECS[ECS];

3) In-containment refuelling water storage tank water level and temperature monitoring.

f) Spent fuel pool water level and temperature monitoring;

g) Radioactivity monitoring:

1) Annulus ventilation dose rate monitoring;

2) Containment dose rate monitoring;

3) Stack dose rate monitoring;

4) Safeguard building dose rate monitoring.

h) Annulus ventilation:

1) Annulus pressure monitoring;

2) Operation of annulus ventilation.

8.8.2.5 System Architecture

The architecture of the KDA [SA I&C] is shown in Figure F-8.8-2. The KDA [SA I&C] is comprised of cabinets and the SHP.

a) Severe Accident Cabinet

The cabinets provide functions including signal acquisition, logic processing and command output which are required in the management of severe accident.

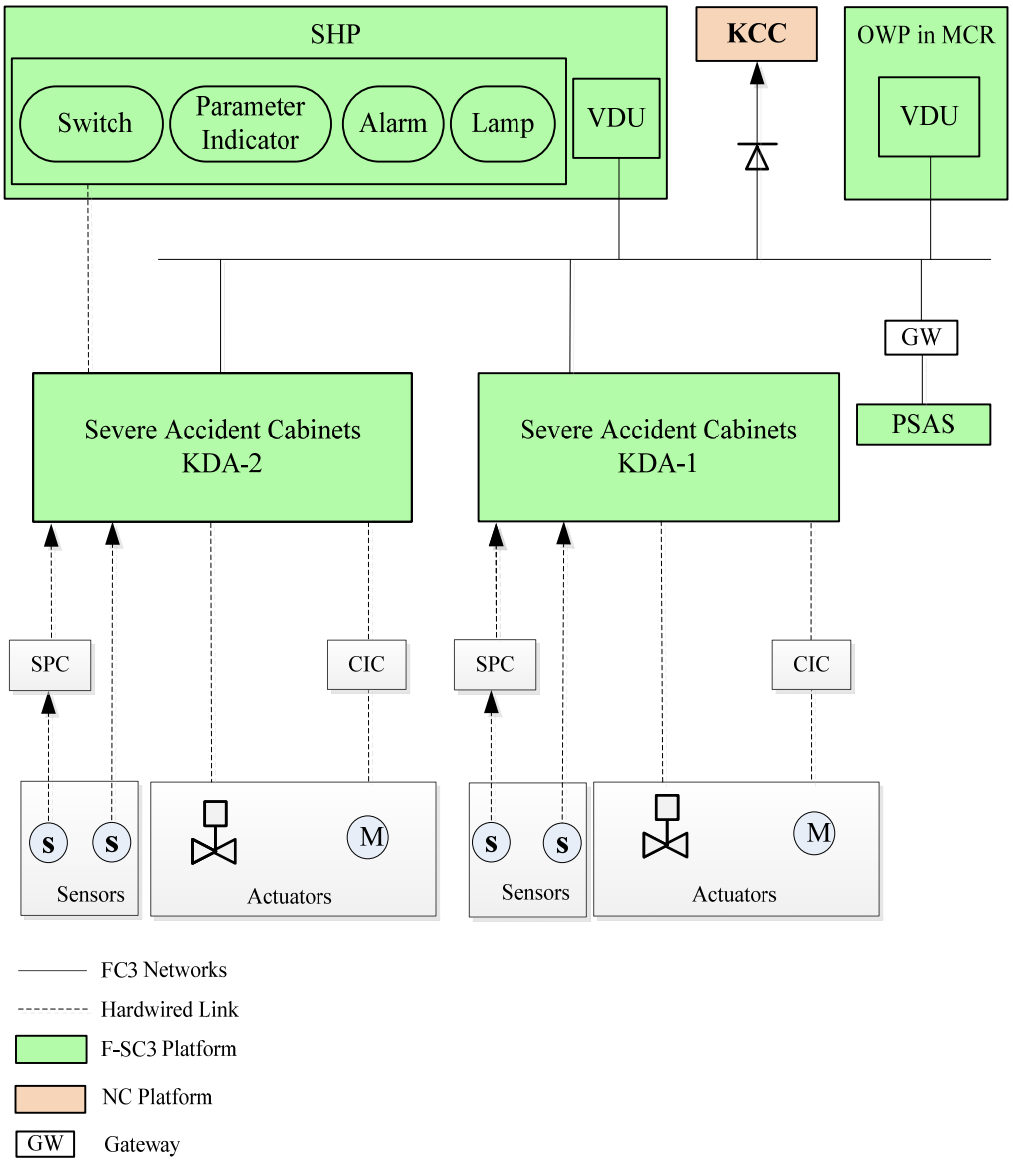
The severe accident cabinets are implemented on the SpeedyHold platform.

b) Severe accident Human interface Panel (SHP)

The SHP is used to provide manual control functions and parameter monitoring functions to perform the management functions for the identified severe accident coincident with total loss of AC power.

The SHP is implemented on the SpeedyHold platform.

Furthermore, the VDU of the OWP is used to provide manual control functions and parameter monitoring functions to mitigate the consequences of the identified severe accident.



F-8.8-2 Architecture of the KDA [SA I&C]

8.8.2.6 System Design Description

a) Classification of system

The KDA [SA I&C] is classified as F-SC3.

The equipment of the KDA [SA I&C] is categorised as SSE1.

b) Reliability

The reliability claim of the KDA [SA I&C] does not exceed 10^{-1} probability of failure on demand.

c) Contribution to DiD

The KDA [SA I&C] provides the severe accident defence line of the DiD structure, which is described in Sub-chapter 8.5.5.

d) Periodic test

In order to ensure the integrity and correctness of the functions, the KDA [SA I&C] is tested periodically.

e) Internal and external hazards

The I&C equipment of the KDA [SA I&C] is protected against the damaging effects resulting from external hazards: earthquake, EMI and external flooding.

For the measures taken against external hazards, refer to Sub-chapter 8.5.7.

f) Performance requirements

The response time (from signal input to the KDA [SA I&C] output) is less than 1s.

g) Platform

The KDA [SA I&C] is implemented on the SpeedyHold platform. Further description of the SpeedyHold platform is given in Sub-chapter 8.14.

h) Human machine interface

The OWP and SHP are the HMIs for the KDA [SA I&C]. The OWP is used to manage the functions which are not required in the event of a total loss of AC power supply. The SHP is used to manage the functions within 12 hours after a severe accident concurrent with a total loss of AC power. For further information of HMIs, refer to Sub-chapter 8.13.

8.8.3 Diverse Actuation System (KDS [DAS])

This sub-chapter presents the current KDS [DAS] design. The gaps between the current KDS [DAS] design and UK requirements have been identified and are being analysed.

8.8.3.1 Introduction

The KDS [DAS] is able to mitigate the consequences of DBC-2/3/4 (reactor in power mode) with the concurrent CCF of the PS and SAS, and it brings the NPP to the final state. In addition, specific measures are taken in the KDS [DAS] to mitigate the consequences in case of an Anticipated Transient Without Scram (ATWS) due to insertion failure of the rod cluster control assembly.

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

a) Reactivity control;

b) Heat removal;

c) Confinement of radioactive material.

In addition, the KDS [DAS] is used to perform supporting functions.

8.8.3.2 Claims for Safety Functions

The KDS [DAS] supports the following safety function claims: I&C-C1.1.2-R2, I&C-C1.1.2-R3, I&C-C1.1.3-H1, I&C-C1.1.3-H2, I&C-C1.1.3-H3, I&C-C1.1.3-H4, I&C-C1.1.4-C2, I&C-C1.1.4-C3, I&C-C1.1.4-C4 and I&C-C1.1.5-E1.

Refer to Appendix 8A for details.

8.8.3.3 Claims for Safety Features

The KDS [DAS] supports the following safety feature claims: I&C-C1.1.1, I&C-C1.2, I&C-C1.3, I&C-C1.4, I&C-C1.5 and I&C-C2.1.

Refer to Table T-8.4-1 for details.

8.8.3.4 System Function Description

In order to bring the NPP to a final state in the event of CCF in the PS and SAS with a concurrent DBC-2/3/4 (reactor in power mode), the KDS [DAS] implements the following functions:

a) Provide diverse automatic actuation functions (e.g. reactor trip, turbine trip, safety injection, containment isolation, ASG [EFWS] actuation, MSIV closure, secondary side partial cooldown, etc.);

b) Provide diverse manual actuation functions for reactor trip and engineered safety feature actuation (e.g. ASG [EFWS] isolation, RBS actuation and isolation, VDA valve regulation, main feedwater line isolation, etc.);

c) Provide diverse indications for plant parameters (e.g. saturation margin, pressuriser pressure, pressuriser level, loop level in primary side, steam generator level, steam generator pressure, hot leg temperature, safety injection flowrate, emergency feedwater flowrate, steam line activity measurement, etc.).

8.8.3.5 System Architecture

The architecture of the KDS [DAS] is shown in Figure F-8.8-3. The KDS [DAS] consists of the Diverse Actuation Cabinet (DAC) and DHP. The letter ‘X’ is used to denote the number of the manual logic processing cabinets.

a) Diverse Actuation Cabinet (DAC)

The DACs that implement diverse automatic reactor shutdown and engineered safety feature actuation functions include acquisition, logic processing and output circuits.

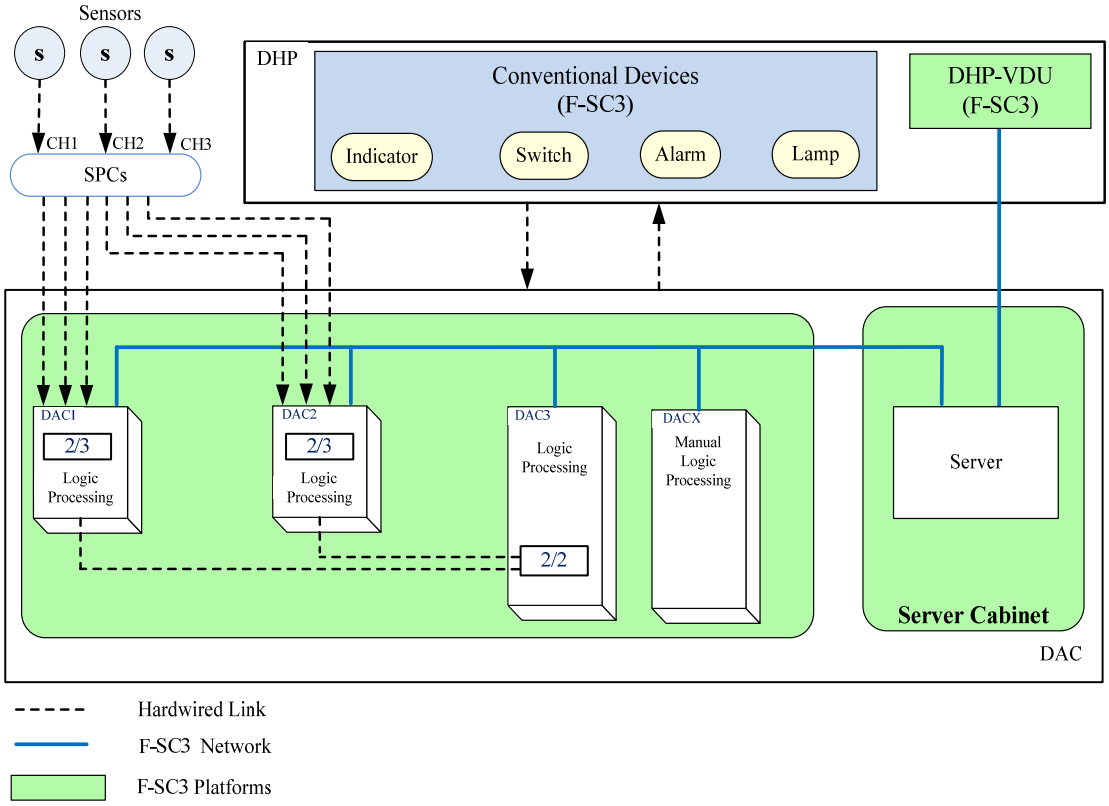
The DACs are implemented on the FitRel platform.

b) Diverse Human interface Panel (DHP)

The DHP is used to realise system-level manual actuation functions and necessary equipment-level manual actuation functions, as well as safety parameter monitoring functions, including controllers, indicators, lamps and alarms.

The automatic actuation functions and the manual system-level actuation signals are sent to DAC1 and DAC2. The manual equipment-level actuation signals are sent to DAC3 and DACX.

For the purpose of reducing the spurious actuation rate, 2 out of 2 logic is implemented in the KDS [DAS].



F-8.8-3 Architecture of the KDS [DAS]

8.8.3.6 System Design Description

a) Classification of system

The KDS [DAS] is classified as F-SC3.

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

order to avoid spurious reactor trip or spurious engineered safety feature actuation caused by the earthquake.

b) Reliability

The reliability claim of the KDS [DAS] does not exceed 10^{-1} probability of failure on demand.

c) Contribution to DiD

The KDS [DAS] provides the diverse defence line of the DiD structure, which is described in Sub-chapter 8.5.5.

d) Independence

Electrical separation between the SPC and CIC is provided to ensure that the failure of the KDS [DAS] is not propagated to the main defence line and does not prevent the implementation of the PS functions and SAS functions.

e) Diversity

The KDS [DAS] is developed by FPGA technology which is diverse from the digital technology adopted in the PS and SAS.

The KDS [DAS] provides the diverse reactor trip function which cuts off electrical power to the control rod drive mechanisms by tripping the motor-generator set supplying power to the control rod drive mechanism magnetic gripper coils.

f) Fail-safe design

To prevent spurious actuation in the event of Loss of Offsite Power (LOOP), the KDS [DAS] signals to actuate reactor trip and engineered safety features are designed to be energised to activate.

When a failure of the acquired signals is detected, the voting logic implemented in the KDS [DAS] is degraded to result in no actuation.

g) Periodic test

In order to ensure the integrity and correctness of the whole functions, the KDS [DAS] is periodically tested.

h) Internal and external hazards

The I&C equipment of the KDS [DAS] is protected against the damaging effects resulting from external hazards: e.g. earthquake, EMI and external flooding.

For the measures taken against external hazards, refer to Sub-chapter 8.5.7.

i) Performance requirements

The KDS [DAS] fulfils the performance requirements of I&C functions in terms of response time and accuracy arising from the safety analysis.

For the automatic functions, the response time from "measurement input to the KDS [DAS]" to "the KDS [DAS] output command to actuator" is not more than { }.

j) Platform

The KDS [DAS] cabinets are implemented on the FitRel platform. Further description of the FitRel platform is given in Sub-chapter 8.14.

k) Human machine interface

The DHP is the HMI panel of the KDS [DAS] in the MCR. The DHP provides switches and buttons for manual actuation and manual control, conventional indicators for displaying key parameters and indicator lamps. In the event of CCF in the PS and SAS with a concurrent DBC-2/3/4 (reactor in power mode), operators can bring the reactor to the safe state and maintain this state with the operational equipment and monitoring equipment on the DHP. For further information of HMIs, refer to Sub-chapter 8.13.

8.9 Non-classified Centralised I&C System

The NC Centralised I&C system, namely part of the PSAS, is described in Sub-chapter 8.8.1.

8.10 Non-centralised I&C Systems

The Non-centralised I&C systems are described as follows:

a) In-core Instrumentation System (RIC [IIS])

The RIC [IIS] is classified as F-SC2, which uses integrated in-core instrumentation assemblies inserted from the top of the RPV to measure temperature and reactor coolant level in the RPV for normal and accident monitoring.

Temperature and RPV level signals are sent to Centralised I&C systems through hardwired links, which are used to evaluate the cooling state of the reactor core and support manual operations to cope with accidents to bring the plant to the safe state. Temperature signals are also sent to the KDS [DAS] through hardwired links to confirm the cooling state and support manual operations to cope with accidents coincident with CCF of the PS and SAS.

b) Nuclear Instrumentation System (RPN [NIS])

The RPN [NIS] is classified as F-SC1, and it measures reactor nuclear power continuously from reactor start-up to full power operation. The RPN [NIS]

includes three measuring ranges: source range, intermediate range and power range.

The power signals from the RPN [NIS] are transferred through hardwired links to the PS and KDS [DAS] to provide the reactor trip functions and the operational bypass functions. The power signals are transferred through hardwired links to the PSAS to provide the safety interlock functions and reactor power control functions.

c) Plant Radiation Monitoring System (KRT [PRMS])

The KRT [PRMS] is classified as F-SC1, and it is designed to measure and indicate whether radiological conditions in the plant are within the bounds of the designed conditions. The KRT [PRMS] measures the radioactivity of the processing fluid (liquid and gas), working area and the effluent. Some measuring channels are also used during and after accidents in order to monitor the radioactive material release.

The KRT [PRMS] is used to support the Centralised I&C systems to perform the associated safety functions. The signals of the steam generator leakage rate, reactor pool area γ dose rate and spent fuel pool area γ dose rate are sent to the PS through hardwired links to support manual operations. The signals used for the implementation of FC2 functions are sent to the SAS through hardwired links, e.g. signals of the activity concentration of the steam generator blow-down and the dose rate of the MCR intake air. The signals used for the implementation of FC3 and NC control functions are sent to the PSAS through hardwired links, e.g. signals of the activity concentration of exhaust air from the Condensate Vacuum System (CVI [CVS]) and the activity concentration of exhaust air from the Gaseous Waste Treatment System (TEG [GWTS]).

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

The RGL [RPICS] is classified as F-SC3, and it consists of the rod position indication system and rod control system. The rod position indication system is used to indicate the position of the control rods in the core, and to monitor the state of the control rods and their related equipment. In order to control the reactor power and the coolant temperature, the rod control system is used to receive commands from the PSAS and then generate insert or withdraw commands for each group of control rod clusters according to pre-defined movement sequences.

The RGL [RPICS] is used to support the Centralised I&C systems to achieve the reactor trip functions, reactor power control functions and coolant temperature regulation functions. The RGL accepts the reactor trip signal from the KDS [DAS] through a hardwired link. In addition, the control rod moving commands from the PSAS are sent to the RGL [RPICS] via hardwired links.

e) I&C system of the Fuel Handling and Storage System (PMC [FHSS])

The PMC [FHSS] is classified as NC, and it consists of the fuel transport system and manipulator crane. The I&C system of the fuel transfer system includes the control console and the control cabinet, which are used to provide the equipment-level manual control functions for the operator. The I&C system of the manipulator crane is used to accurately control the position of the fuel gripper over any X-Y coordinate position of the core and locations specified and pick up fuel assemblies, control rod cluster or thimble plugs.

f) Nuclear Accident Emergency Management System (KCC [NAEMS])

The KCC [NAEMS] supports the safety feature claim I&C-C1.2.

The KCC [NAEMS] is classified as NC, and it not only provides information and technical support for on-site emergency management but it also sends the information to the nuclear emergency organisations and assists the off-site emergency response. The KCC [NAEMS] is deployed in the on-site emergency control centre and is designed to support the function of DiD level 5. As a result, the important network equipment of the KCC [NAEMS] is designed to be available under seismic conditions and it is powered by an independent diesel generator located in the on-site emergency control centre.

g) Turbine Generator Control System (TGCS)

The TGCS is classified as NC. The TGCS includes three systems: the turbine governing system, turbine protection system and turbine supervisory system.

1) The turbine governing system is an electro-hydraulic control system which controls the steam flow that is passed through the control valves to the turbine. The governing functions include speed control, load control, frequency control, fast run back, load rejection and limitation functions;

2) The turbine protection system ensures the trip of the turbine when the turbine-generator is in abnormal conditions or has mechanical failures;

3) The turbine supervisory system continuously collects and monitors the parameters of the turbine shaft and casing, including eccentricity, key phase, vibration, shaft displacement, differential expansion, etc.

The signals exchanged between the TGCS and the PSAS are through the redundant network, but important signals between the PSAS and the TGCS are connected by hardwired links, e.g. the runback signals from the PSAS to the TGCS and turbine trip signals from the TGCS to the PSAS. Turbine trip signals from the PS and the KDS [DAS] to the TGCS are transferred by hardwired links, and the feedback signals of turbine trip are transferred to the PS by hardwired links.

8.11 Instrumentation and Actuators

8.11.1 Instrumentation

The functions of safety related systems rely on the accurate and timely plant information delivered by instrumentation. The instrumentation used for safe and reliable operation of the UK HPR1000 consists of process instrumentation, nuclear instrumentation and radiation instrumentation.

Process instrumentation is used to measure the process parameters, typically including reactor coolant pressure, reactor coolant temperature, reactor coolant flowrate, reactor coolant level, feedwater level and pressure of steam generators, main steam pressure and other parameters.

Nuclear instrumentation described in Sub-chapter 8.10 item b) is used to measure ex-core neutron flux and then to calculate the nuclear power level. The results from nuclear instrumentation are sent to the PS and the KDS [DAS] for protection functions and the PSAS for control functions.

Radiation instrumentation is used to measure the radioactivity of the processing fluid (liquid and gas), working area and the effluent. For general systems description, refer to Sub-chapter 8.10 item c) and item g).

Instruments are classified in accordance with the functions that they perform. The design of instrumentation fully considers the reliability and performance requirements arising from the safety functions. Reliability requirements include redundancy, independence and environment qualification, e.g. four independent power range instruments are adopted to monitor the power range and are fed to the PS realising the reactor protection function during accidents. Performance requirements include accuracy and response time.

Instruments required for monitoring and measuring during accident conditions are designed to withstand the corresponding conditions in the various areas affected by the accident. By conducting qualification as described in Sub-chapter 4.4, instruments are proved to meet these requirements.

In order to reduce the quantity of equipment and facilitate maintenance, some sensors are shared by the PS and other Centralised I&C systems including the KDS [DAS], KDA [SA I&C] and PSAS. For the shared sensors, the associated signals are processed by the F-SC1 SPMs, and are then distributed to different Centralised I&C systems after isolation.

8.11.2 Actuators

Actuators are controlled by Centralised I&C systems to accomplish their assigned functions. The actuators of the UK HPR1000 initiate operation of equipment where electric power, hydraulic pressure and mechanical stored energy are the prime movers.

There are 8 RTBs in the UK HPR1000 to implement emergency reactor trip, and they are grouped into 4 groups and controlled by four channels of the PS. In order to ensure diversity and independence between the PS and KDS [DAS], the KDS [DAS] trips the reactor through the power cabinets of the RGL [RPICS] which are used to regulate the electrical currents to the control rods.

The design of actuators fully considers the reliability and performance requirements arising from the safety functions. Actuators are configured with the same redundancy level as the centralised systems they support. They are qualified to endure the harsh environments in which they are supposed to perform their functions.

For the actuators controlled by different I&C systems, the CIMs located in the CIC are used to manage the priority of actuation commands with different directions coming from different I&C systems. The CIMs are also employed to provide isolation between different I&C systems to avoid the propagation of failures.

8.12 I&C Support Systems

This sub-chapter describes the support systems for the I&C systems, including electrical power systems and HVAC systems.

8.12.1 Electrical Power System

The power supplies of different I&C equipment are configured based on the safety classification, functions and availability requirements. Each channel or division of I&C equipment is supplied by a corresponding division of the electrical power system. The corresponding relation is as follows:

a) Division A and channel IP of I&C equipment are supplied by division A of the electrical power systems;

b) Division B and channel IIP of I&C equipment are supplied by division B of the electrical power systems;

c) Division C and channel IIIP of I&C equipment are supplied by division C of the electrical power systems;

d) Channel IVP of I&C equipment is supplied by division C of the electrical power systems.

The power supply scheme of level 1 I&C equipment is shown in Table T-8.12-1, and the power supply scheme of level 2 I&C equipment is shown in Table T-8.12-2. The types of power supplies in the tables are as follows:

a) Type 1: F-SC1 AC (2-hour UPS) power supply with SSE1 seismic requirement;

b) Type 2: F-SC1 Direct Current (DC) (2-hour UPS) power supply with SSE1 seismic requirement;

c) Type 3: F-SC3 AC (12-hour UPS) power supply with SSE1 seismic requirement;

d) Type 4: NC AC (2-hour UPS) power supply;

e) Type 5: NC DC (2-hour UPS) power supply.

The power supplies of Type 1, Type 2 and Type 3 for division A, B and C of electrical power systems are supported by EDGs which are in operation under the LOOP condition. Furthermore, the power supplies of Type 1, Type 2 and Type 3 for division A and B of electrical power systems are supplied by SBO diesel generators which are in operation under SBO conditions. Further information of electrical power system is described in Chapter 9.

T-8.12-1 The Power Supply Scheme of Level 1 I&C Equipment

I&C Equipment	**Type of Power Supply**		
RPC/ESFAC/SCC	Type 1	Type 2	---
CIC/SPC (without severe accident functions)	Type 1	Type 2	---
CIC/SPC (with severe accident functions)	Type 1	Type 2	Type 3
SAC	Type 1	Type 2	---
DTC	Type 1	Type 2	---
CCMC	Type 1	Type 2	Type 3
PSAC (NI)	Type 1	Type 2	---
PSAC (CI)	Type 4	Type 5	---
DAC	Type 1	Type 4	---
KDA [SA I&C] Cabinets	Type 1	Type 4	Type 3

T-8.12-2 The Power Supply Scheme of Level 2 I&C Equipment

HMI Equipment[5]		**Type of Power Supply**	
OWP in MCR	VDU	Type 1	Type 4
	SCID-200	Type 1	Type 2
KIC-LDP		Type 1	Type 4
ACP	VDU	Type 1	Type 4
	SCID-200	Type 1	Type 2
	SCID-300	Type 1	Type 2
	Conventional Devices	Type 1	Type 2
ACP-LDP		Type 1	Type 4
ECP		Type 1	Type 2
SHP		Type 1	Type 3
DHP		Type 1	Type 4
COWP in RSS	VDU	Type 1	Type 4
	SCID-200	Type 1	Type 2
COWP in TSC		Type 1	Type 4

8.12.2 HVAC

HVAC systems control the temperature and humidity in the MCR, RSS and I&C electronic equipment rooms to maintain the environmental conditions within the stipulated operating range of the I&C equipment and to provide a suitable environment for staff. Each channel or division of I&C equipment is supplied by the corresponding division of HVAC systems. The corresponding relation is as follows:

a) Division A and channel IP of I&C equipment are supported by an HVAC system

[5] Refer to Sub-chapter 8.13 for the description of HMI equipment.

of division A;

b) Division B and channel IIP of I&C equipment are supported by an HVAC system of division B;

c) Division C and channel IIIP of I&C equipment are supported by an HVAC system of division C;

d) Channel IVP of I&C equipment is supported by an HVAC system of division C. When the HVAC system of division C is unavailable, channel IVP of I&C equipment can be supported by an HVAC system of division B.

The HVAC functions above are categorised as FC1. The HVAC systems of the MCR and RSS are independent from each other. Further details of HVAC systems are described in Sub-chapter 10.6.

8.13 Control Room Systems

8.13.1 Introduction

The control room systems provide HMIs for operators to monitor and control the NPP under all operating conditions and maintain it in a safe condition. The control room systems include the KSC [MCRS], KIC [PCICS] and KPR [RSSS].

8.13.2 Claims for Safety Functions

Control room systems provide HMIs to the PS, SAS, KDA [SA I&C], KDS [DAS] and PSAS to support the following safety function claims: I&C-C1.1.2-R1, I&C-C1.1.2-R2, I&C-C1.1.2-R3, I&C-C1.1.3-H1, I&C-C1.1.3-H2, I&C-C1.1.3-H3, I&C-C1.1.3-H4, I&C-C1.1.4-C2, I&C-C1.1.4-C3 and I&C-C1.1.4-C4. Control room systems also provide HMIs to Non-centralised I&C systems functions. Appendix 8A provides more detailed information.

8.13.3 Claims for Safety Features

Control room systems support the safety feature claim I&C-C1.5. Table T-8.4-1 shows detailed information of this claim.

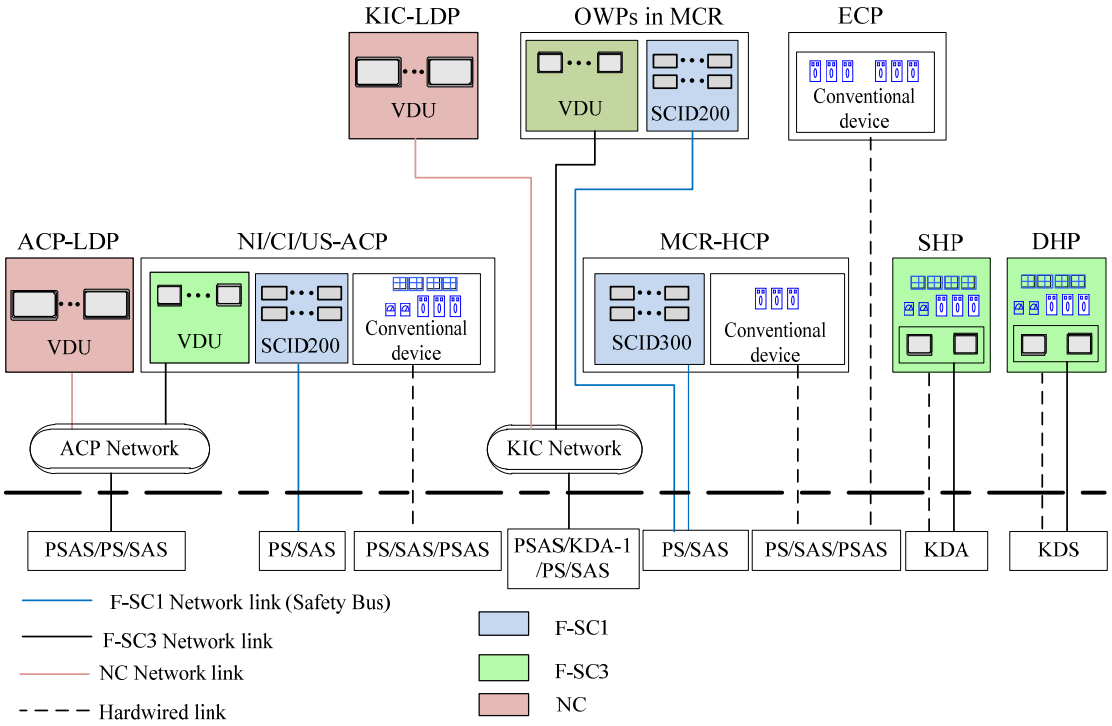
8.13.4 Main Control Room System (KSC [MCRS])

8.13.4.1 Introduction

The KSC [MCRS] provides the operators with HMIs in the MCR to monitor and control the NPP under all conditions.

8.13.4.2 System Architecture

The KSC [MCRS] is the interface of the PS, SAS, PSAS, KDA [SA I&C] and KDS [DAS]. The KSC [MCRS] is located in the safeguard building. The overall configuration of the KSC [MCRS] is shown in Figure F-8.13-1.



F-8.13-1 Overall Configuration of the KSC [MCRS]

The KSC [MCRS] consists of the OWP, LDP, ACP and ACP network, ECP, SHP and DHP. The equipment of the ACP network contains server cabinets, gateway cabinets, printers, engineering stations, etc.

8.13.4.3 System Function Description

The major equipment of the KSC [MCRS] is as follows:

a) Operator Workplace (OWP) and Large Display Panel (LDP)

The OWP and KIC-LDP are connected to the KIC [PCICS] network and arranged in the MCR.

The OWP is the Main Computerised Control Means (MCM) for operators to monitor and control the NPP in normal operating conditions and accident conditions.

There are four identical OWPs: NI-OWP, CI-OWP, Unit Supervisor (US) OWP and Safety Engineer (SE) OWP.

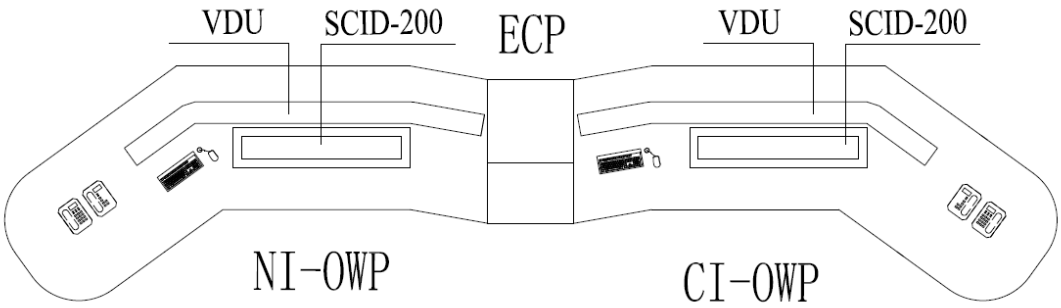
Each OWP consists of VDUs and SCID-200s as shown in Figure F-8.13-2. The general information of VDUs and SCID-200s is as follows:

1) The VDUs are classified as F-SC3 and implemented by the HOLLiAS-N platform. The VDUs receive information from the following systems by the KIC [PCICS] network:

- PSAS;

- PS;
- SAS;
- KDA-1.

2) VDUs send control commands to the following systems by the KIC [PCICS] network:
   - PSAS;
   - KDA-1.
3) The SCID-200s are classified as F-SC1 and are implemented by the FirmSys platform. SCID-200s are used for the manual control of the PS/SAS.
4) The four SCID-200s (SCID-A/B/C/D) correspond to three divisions of the ESFSC, SAC and four channels of the RPC.
   - SCID-A corresponds to division A of the ESFSC, SAC and channel IP of the RPC;
   - SCID-B corresponds to division B of the ESFSC, SAC and channel IIP of the RPC;
   - SCID-C corresponds to division C of the ESFSC, SAC and channel IIIP of the RPC;
   - SCID-D corresponds to channel IVP of the RPC.



F-8.13-2 Basic Layout of the NI-OWP and CI-OWP

The KIC-LDP is located in front of the NI-OWP and CI-OWP, and consists of four large liquid crystal screens. The KIC-LDP is designed to provide displays of the key plant parameters.

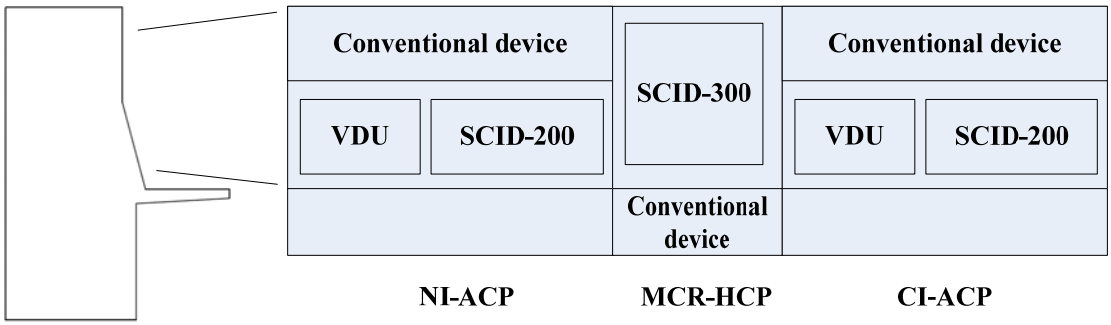
b) Auxiliary Control Panel (ACP)

The ACP is the alternative HMI in case of failure of the OWPs. The ACP is used to:

1) Provide functions to the operators in case the KIC [PCICS] is unavailable in normal operation conditions;

2) Provide functions to the operators in case the KIC [PCICS] is unavailable in DBC-2/3/4.

The ACP is divided into five sections: NI-ACP, CI-ACP, US-ACP, Hardwired Control Panel (HCP) and ACP-LDP. The NI-ACP and CI-ACP consist of VDUs, SCID-200s and conventional devices as shown in Figure F-8.13-3.



F-8.13-3 Panel Layout of the NI-ACP, HCP and CI-ACP

1) The VDUs are classified as F-SC3 and are implemented by the SpeedyHold platform. {

}

VDUs send control commands to the PSAS by the ACP network.

2) The SCID-200s are classified as F-SC1 and are implemented by the FirmSys platform. SCID-200s are used for the manual control of the PS/SAS.

3) The four SCID-200s correspond to three divisions of the ESFSC, SAC and four channels of the RPC.

{

} .

4) Conventional devices include the alarm windows, controllers, indicators and lamps.

The US-ACP is configured with two VDUs for monitoring purposes to support the US responsibility. The US-ACP is placed close to the US-OWP, as shown in Figure F-8.13-5.

The HCP is located between the NI-ACP and CI-ACP, and it consists of SCID-300s and conventional devices. The SCID-300s are used for the display and recording of accident parameters.

The conventional devices include the KIC/ACP mode switches and indicators for transferring operation mode between the KIC [PCICS] and ACP.

The ACP-LDP consists of four large liquid crystal screens hanging on the wall. The function of the ACP-LDP is to provide general status of the NPP to the US and SE of the shift team.

c) Emergency Control Panel (ECP)

The ECP is located between the NI-OWP and CI-OWP in the MCR, as shown in Figure F-8.13-2. The ECP is configured with hardwired qualified equipment which can provide the operators with easily accessible and visible emergency operations.

d) Severe accident Human interface Panel (SHP)

The SHP is the HMI of the KDA [SA I&C]. The SHP is used to perform the management functions for the identified severe accidents when it occurs coincident with a total loss of power. Key plant parameter indication and the manual operation means for accident management with 12-hour UPS are provided on the SHP.

e) Diverse Human interface Panel (DHP)

The DHP is the HMI of the KDS [DAS]. The DHP provides the diverse manual control, alarm and indication functions in case of software CCF in the PS and SAS.

8.13.4.4 System Design Description

a) Classification of system

The classification of the KSC [MCRS] HMIs is described in Table T-8.13-1.

T-8.13-1 Classification of HMI in the MCR

HMI		Safety Classification	Seismic Category
OWP	VDU	F-SC3	SSE1
	SCID-200	F-SC1	SSE1
KIC-LDP		NC	SSE2
NI-ACP CI-ACP	VDU	F-SC3	SSE1
	SCID-200	F-SC1	SSE1
	Conventional Device	F-SC1	SSE1
MCR-HCP	SCID-300	F-SC2	SSE1
	Conventional Device	F-SC1	SSE1
US-ACP	VDU	F-SC3	SSE1
ACP-LDP		NC	SSE2
ECP		F-SC1	SSE1
SHP		F-SC3	SSE1
DHP		F-SC3	SSE1

b) Contribution to DiD

The OWP VDUs and ACP VDUs support the PSAS to achieve its functions corresponding to the DiD line. For further information about the PSAS functions, refer to Sub-chapter 8.5.5.

The SCIDs located on the OWPs (provide control function), SCIDs located on the ACPs (provide monitoring and control function), OWP VDUs and ACP VDUs (provide monitoring function) support the PS/SAS to achieve their functions. For further information about the PS/SAS functions, refer to Sub-chapter 8.5.5.

The DHP supports the KDS [DAS] to achieve its functions corresponding to the DiD line. For further information about the KDS [DAS] functions, refer to Sub-chapter 8.5.5.

The SHP and OWP VDUs support the KDA [SA I&C] to achieve its functions corresponding to the DiD line. For further information about the KDA [SA I&C] functions, refer to Sub-chapter 8.5.5.

c) Internal and external hazards

The MCR is protected against fire, radiation, internal and external missiles, earthquake and hostile acts.

d) Reliability

The level 2 HMIs with level 1 I&C systems together satisfy the reliability targets. Redundancy design and diversity design are considered in the design of HMIs to increase their reliability. For example, OWPs in the MCR consist of four redundant workstations with the identical configuration, the ACP is designed as the back-up HMI of the OWPs, and the DHP is designed as the diverse HMI.

e) Platform

The OWP VDU and KIC-LDP are implemented on the HOLLiAS-N platform. The ACP VDU and ACP-LDP are implemented on the SpeedyHold platform. The SHP, as the HMI of the KDA [SA I&C] is implemented on the SpeedyHold platform and by conventional devices. The DHP is implemented on the SpeedyHold platform and by conventional devices. For further description of these platforms, refer to Sub-chapter 8.14.

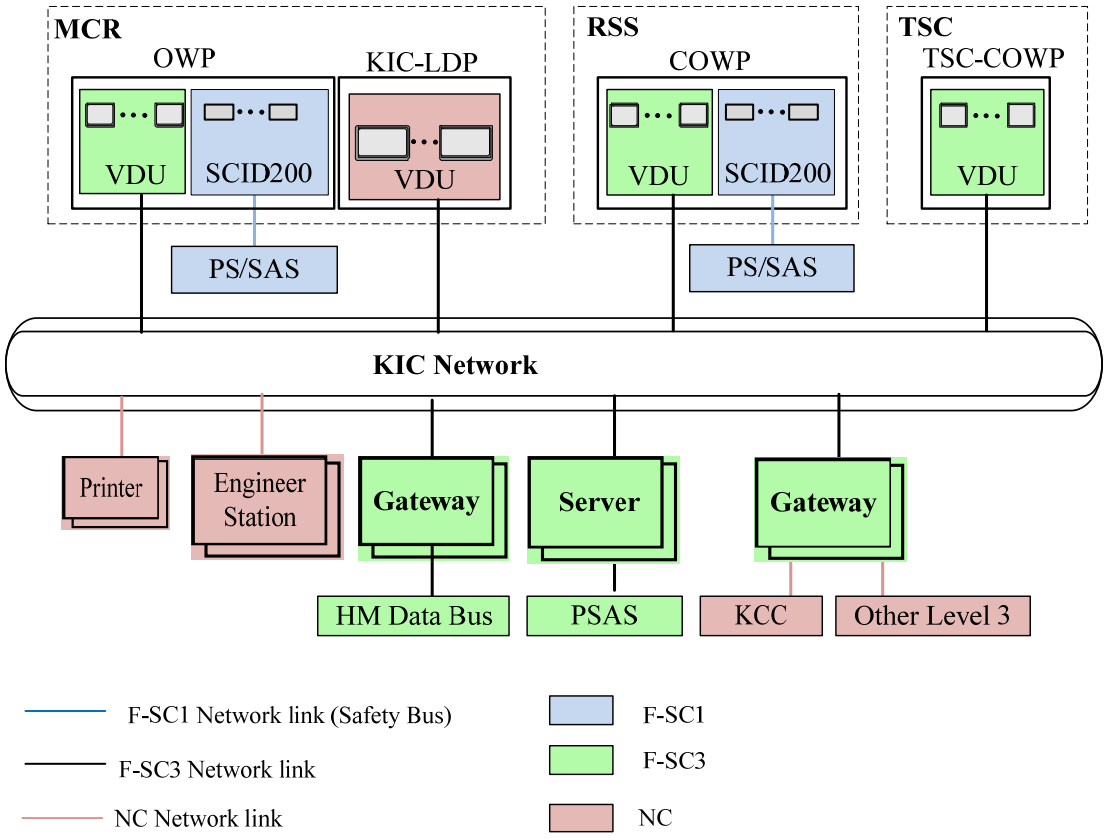
8.13.5 Plant Computer Information and Control System (KIC [PCICS])

8.13.5.1 Introduction

The KIC [PCICS] is based on digital technology and works with SCIDs as the MCM to provide monitoring and control function under all operating conditions of the NPP.

8.13.5.2 System Architecture

The KIC [PCICS] equipment is arranged in the safeguard building. The overall configuration of the KIC [PCICS] is shown in Figure F-8.13-4.



F-8.13-4 Overall Configuration of the KIC [PCICS]

The KIC [PCICS] includes server cabinets, gateway cabinets, power cabinets, printers, engineering stations, etc.

The communication link through the HM data bus is designed to transfer the identification information of the component to be selected on to the VDUs of the KIC [PCICS] to bring up the corresponding command window on the SCID-200s located at the OWPs/COWPs.

8.13.5.3 System Function Description

The KIC [PCICS] provides monitoring and control means through soft display and control, including the following functions:

a) Information display function

1) The status of plant systems and components are provided in display formats based on their tasks;

2) Information is presented on the VDUs of the OWPs/COWPs and KIC-LDP;

3) Information is displayed in an easily understood and interpreted manner.

b) Control function

1) Soft control provides the control means of the plant systems and components

which enable operators to operate the NPP under all conditions on OWPs in the MCR and COWPs in the RSS;

2) Soft control is clearly labelled and is easily identified to minimise operator errors.

c) Alarm management function

1) The alarm gives information to warn operators of existing abnormalities in the plant equipment or processes, which require operator attention or action;

2) Alarms are divided into 4 priority levels according to severity. The alarms are grouped and presented logically to be easily understood to avoid confusion;

3) The digital alarm is designed in accordance with Human Factors Engineering (HFE) good practice and guidance.

d) Computer-based procedure function

1) The computer-based procedure helps operators monitor and control the NPP. Procedures can be invoked from the VDUs on OWPs/COWPs. A set of paper procedure is provided as a backup;

2) There are three kinds of operation procedures, which are normal operating procedures, emergency operating procedures and severe accident management guidelines;

3) The computer-based procedure is designed in accordance with HFE good practice and guidance.

8.13.5.4 System Design Description

a) Classification of system

The KIC [PCICS] is classified as F-SC3 and performs FC3/NC functions. The seismic categorisation of the KIC [PCICS] equipment is designed according to the categorisation of the functions case by case. The KIC [PCICS] equipment (e.g. server cabinets, gateway cabinets and power cabinets) performing FC3 functions are categorised as SSE1, and other KIC [PCICS] equipment (e.g. printers and engineer stations) performing NC functions are categorised as SSE2 or NO case by case.

b) Internal and external hazards

The KIC [PCICS] equipment is protected against the damaging effects resulting from internal and external hazards.

The main internal hazard considered for the KIC [PCICS] is fire. To withstand the hazard physical separation measures are taken. The main external hazard considered for the KIC [PCICS] is earthquakes. To withstand the hazard seismic

qualification is performed.

The redundant components of the KIC [PCICS] (e.g. server cabinets, gateway cabinets and power cabinets) are arranged in two different zones with a fire barrier separating them.

c) Platform

The KIC [PCICS] is implemented on the HOLLiAS-N platform. For detailed description of this platform, refer to Sub-chapter 8.14.

8.13.6 Remote Shutdown Station System (KPR [RSSS])

8.13.6.1 Introduction

The KPR [RSSS] enables operators to perform operations, to place and maintain the plant in a safe condition when the MCR is unavailable.

8.13.6.2 System Architecture

The KPR [RSSS] consists of three COWPs and one HCP (configured with one MCR/RSS mode switch and reactor trip buttons) inside the RSS, and two RSS switch boxes outside of the RSS. These COWPs in the RSS consist of VDUs and SCID-200s, and provide the same monitoring and control function as OWPs in the MCR. For the architecture of the COWPs in the RSS, refer to Sub-chapter 8.13.1.2.

The conventional devices on the RSS-HCP and in RSS switch boxes are connected to level 1 I&C systems by hardwired links.

8.13.6.3 System Function Description

The KPR [RSSS] provides the monitoring and control function to shut down the reactor and reach the safe condition through COWPs.

The KPR [RSSS] switching function is intended to disable MCR control functions and transfer the operation mode to the RSS through three MCR/RSS mode switches.

8.13.6.4 System Design Description

a) Classification of system

COWPs in the RSS consist of VDUs of the KIC [PCICS] and SCIDs of the PS and SAS. The classification of VDUs and SCIDs is the same as that of OWPs in the MCR. The conventional devices of the KPR [RSSS] (including MCR/RSS mode switches and reactor trip buttons) are classified as F-SC1.

T-8.13-2 Classification of HMI in the RSS

HMI		Safety Classification	Seismic Category
RSS-COWP	VDU	F-SC3	SSE1
	SCID-200	F-SC1	SSE1
RSS-HCP	Conventional Devices	F-SC1	SSE1
RSS Switch Box	Conventional Devices	F-SC1	SSE1

b) Internal and external hazards

The RSS is protected against the damaging effects resulting from internal hazards and external earthquakes. The RSS and MCR are located in different zones with a fire barrier to prevent the spread of fire from damaging both control rooms.

c) Reliability

The level 2 HMIs with level 1 I&C systems together satisfy the reliability targets. The redundancy design of three COWPs with the same configuration is considered in the KPR [RSSS] to increase the availability.

d) Platform

COWPs in the RSS are implemented on the HOLLiAS-N platform. The conventional devices of the KPR [RSSS] are realised by hardware technology. For further description of the HOLLiAS-N platform, refer to Sub-chapter 8.14.

8.13.7 HMIs in Control Rooms

8.13.7.1 Introduction

The HMIs provide monitoring and control functions of the NPP in the form of displays, indicators, alarms and controls. The HMIs support the monitoring or delivery of plant functions through observation, analysis, decision making, action and confirmation.

This sub-chapter describes the HMIs in control rooms of the UK HPR1000, including the MCR, RSS and TSC. An overview of the HMIs that are located in control rooms is described as follows:

a) Main Control Room (MCR)

The MCR is the control centre where operators conduct operation and monitoring of the NPP under all conditions.

b) Remote Shutdown Station (RSS)

The RSS is the supplementary control room which enables the operators to shut down the reactor and bring the plant into a safe condition in case the MCR is unavailable.

c) Technical Support Centre (TSC)

The TSC is the place where the technical support team evaluates and diagnoses plant conditions in case of emergency conditions.

8.13.7.2 Requirements for HMIs

The requirements for the HMIs arise from:

a) The design of the HMIs in control rooms is based on the requirements from related codes and standards (IEC 60964, IEC 60965, IEEE 497, etc.) and refers to the RGP;

b) The HMI requirements have been derived from the plant system functions;

c) The HMIs in control rooms are required to meet the requirements arising from good HF engineering practice that accounts human cognitive, physical capabilities and limitations. These requirements are described in *HFE Design Guidelines for Control Room*, Reference [32].

8.13.7.3 Main Control Room (MCR)

This sub-chapter outlines the HMIs in the MCR. For detailed information of MCR design, refer to *Overall Scheme for Control Room System*, Reference [33].

8.13.7.3.1 HMIs in MCR

HMIs in the MCR consist of OWP, LDP, ACP, ECP, SHP and DHP to perform the required operator tasks.

The HMIs in the MCR, RSS and TSC are designed based on human factor engineering requirements and provide friendly interfaces to operators in order to improve work efficiency and reduce human error probability, for example:

a) During the structure design of workstations and control panels, the control room design has considered equipment height, display device location, control device location, clearances for legs and feet, writing space, etc.;
b) During the layout design of the control panel, the control room design has considered the group relationship and logical relationship of the indicators, lamps and controllers so as to increase operator effectiveness and minimise the likelihood of operator misinterpretation and errors;
c) The design of the display is to integrate process information into more meaningful units and reduce the workload associated with extracting meaningful

information;

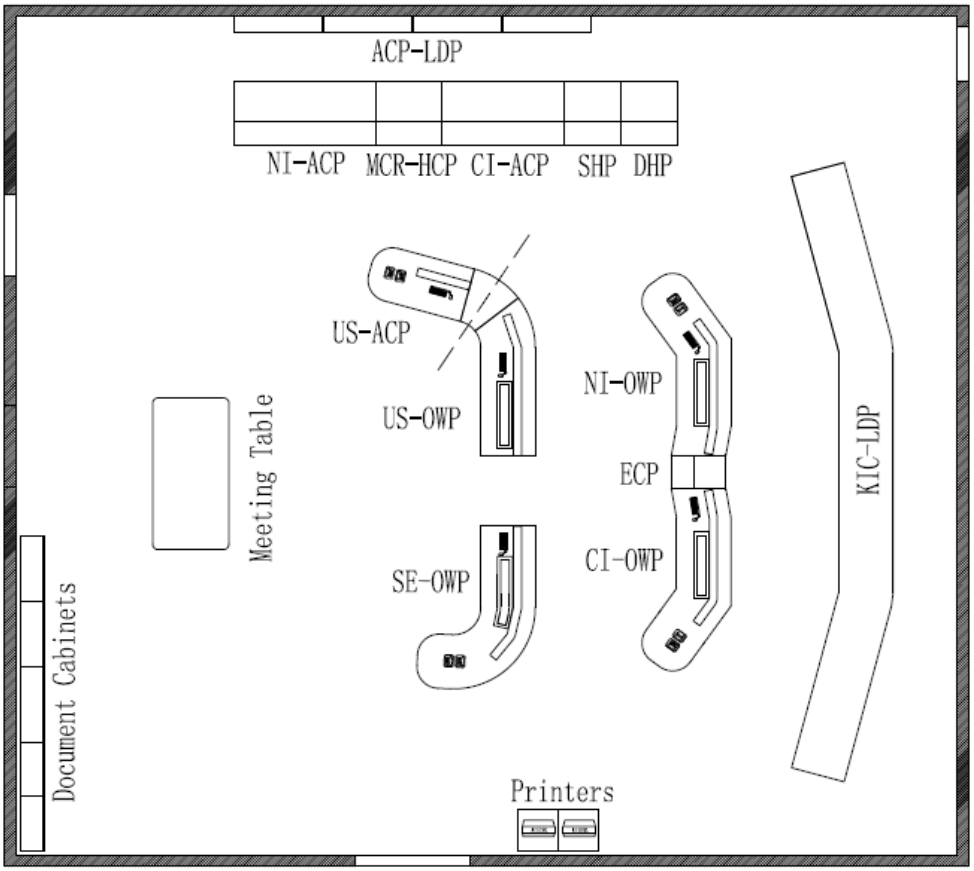
d) The design of alarm system includes an effective design based on HFE good practice and standards in order to ensure that operators focus on key alarms.

8.13.7.3.2 Basic Layout of MCR

The layout of the MCR supports the workflows and interaction of the crew during all plant conditions. The layout design of the MCR is based on functional design, equipment design, operator activities and environmental conditions. It is in line with relevant regulations, standards and human factors engineering requirements to provide operators and maintenance staff with a safe and suitable working space.

There are adequate routes for operators to leave or reach the MCR, or gain access to the RSS under emergency conditions.

The basic layout of the MCR is shown in Figure F-8.13-5.



F-8.13-5 Basic Layout of the MCR

8.13.7.3.3 Environment of MCR

The MCR provides operators with a safe and suitable environment. The environment design requirements of the MCR include air conditioning, illumination, auditory environment, etc.

The Main Control Room Air Conditioning System (DCL [MCDACS]) maintains the ambient conditions required for the safety and habitability of the MCR. The air supply of the MCR is filtered and maintained at a slightly higher pressure through the DCL [MCDACS]). For further information of the DCL [MCDACS], refer to Sub-chapter 10.6.

The lighting of the MCR includes a normal part and an emergency part, and the light level of the different functional zones is designed based on the characteristics of the HMIs. Reducing indirect and direct glare on displays has been considered in the design.

The design of the auditory environment ensures easy communication within the operating team, minimal disturbance by ambient noise and reliable perception of acoustic indicators.

The design of the MCR also provides, within the design basis, protection against fire, radiation, internal and external missiles, earthquake and hostile acts.

8.13.7.4 Remote Shutdown Station (RSS)

This sub-chapter outlines the HMIs in the RSS. For detailed information of RSS design, refer to *Overall Scheme for Control Room System*, Reference [33].

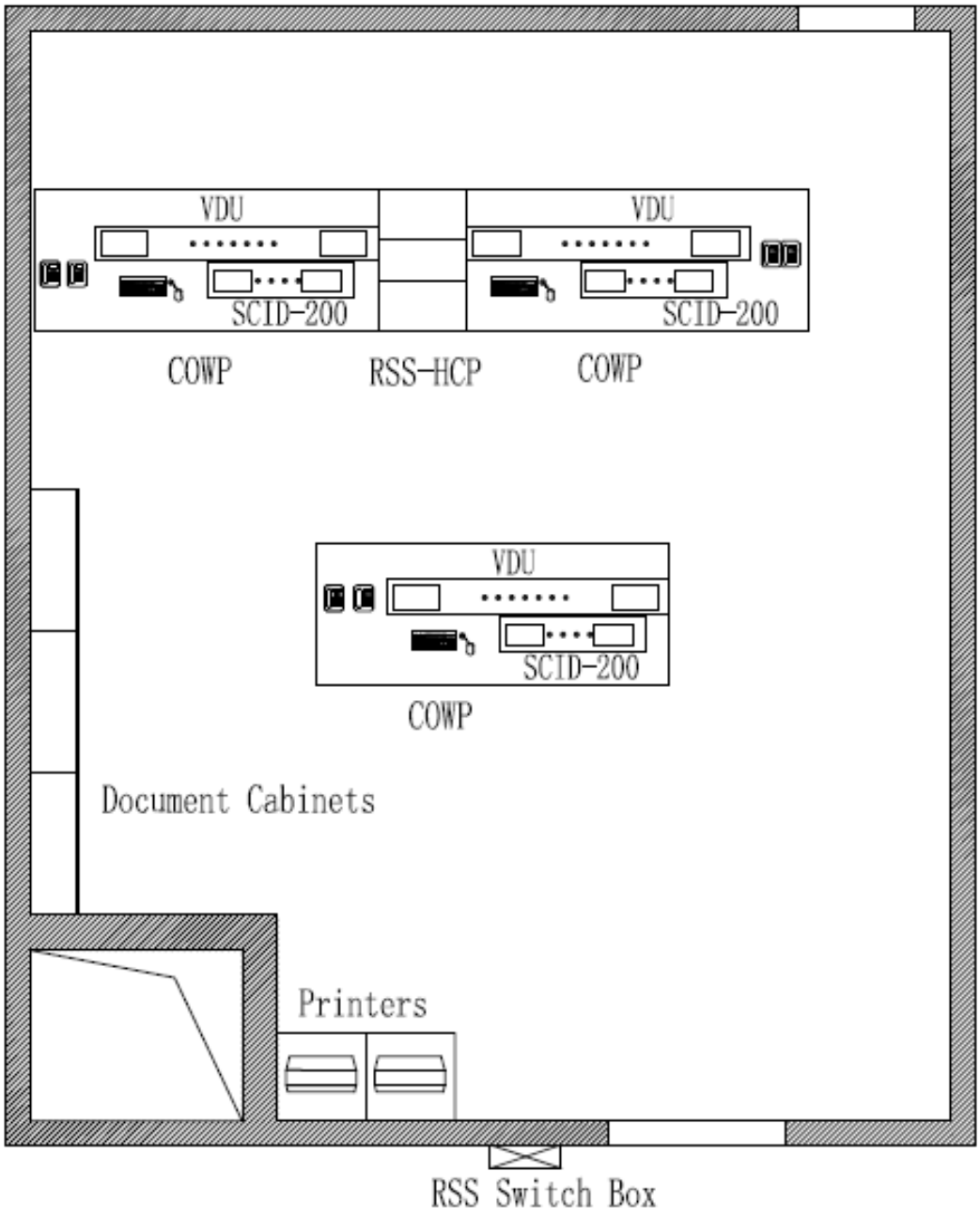
8.13.7.4.1 HMIs in RSS

The RSS is mainly configured of three COWPs and one HCP.

8.13.7.4.2 Basic Layout of RSS

The RSS is located at the floor in the safeguard building, lower than the MCR, however not far from the MCR in order to guarantee the operators can reach the RSS in a timely manner. The safety evacuation path from the MCR to the RSS provides good protection against missiles and earthquakes.

The RSS has sufficient space for three COWPs, the RSS-HCP and other equipment, e.g. communication devices, printers and document cabinets. The basic layout of the RSS is shown in Figure F-8.13-6.



F-8.13-6 Basic Layout of the RSS

8.13.7.4.3 Environment of the RSS

With regards to the emergency preparation and emergency response of operating organisations of the plant, the RSS has appropriate environmental conditions for the operators, including lighting, temperature, humidity, noise, etc. An emergency lighting system is continuously available in the RSS, even upon failure of the normal lighting system. As the backup of the MCR, the RSS is supported by a different independent HVAC system which is the Electrical Division of Safeguard Building Ventilation System (DVL [EDVS]). For further information of the DVL [EDVS], refer to Sub-chapter 10.6.

8.13.7.5 Technical Support Centre (TSC)

This sub-chapter outlines the HMIs in the TSC. For detailed information of TSC design, refer to *Overall Scheme for Control Room System*, Reference [33].

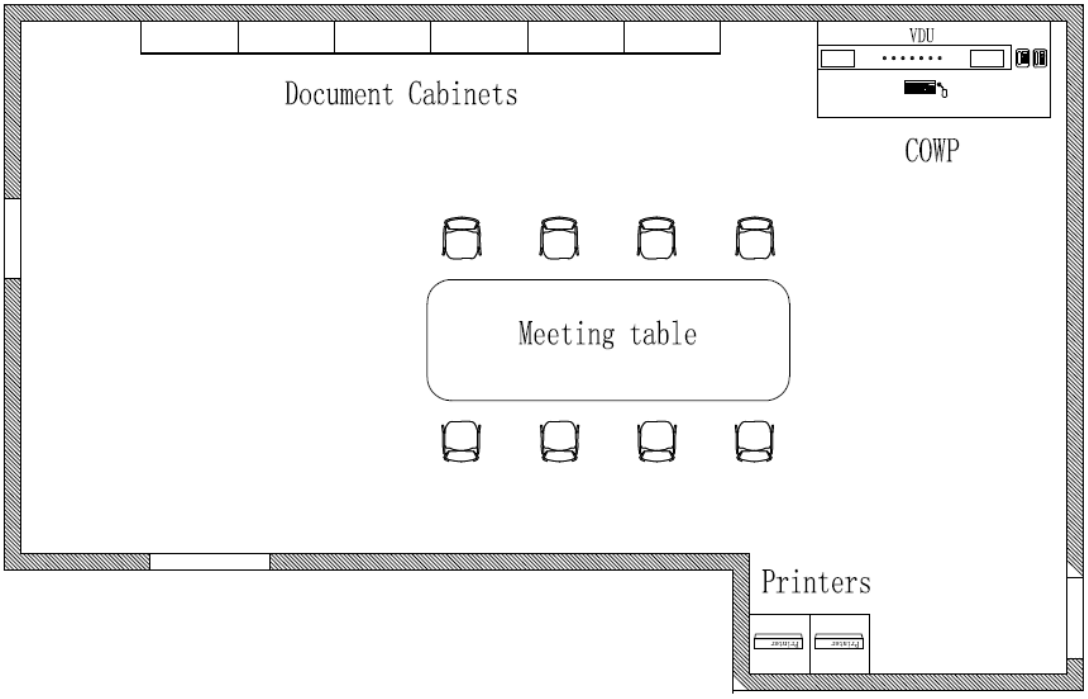
The TSC is used to provide technical support for MCR operators by subject matter experts.

8.13.7.5.1 HMIs in TSC

The TSC provides one COWP (configured with VDUs except for SCID-200s) as the HMI to the technical support team. The VDUs of the COWP in the TSC are connected to the KIC [PCICS] network and provide the same monitoring functions as that of the VDUs of OWPs in the MCR rather than control functions. The TSC also provides other necessary facilities, including communication devices, printers, a meeting table and document cabinets.

8.13.7.5.2 Basic Layout of TSC

The TSC is located at a higher floor than the MCR. There is a stairway between the MCR and TSC inside the inhabitable area for emergency conditions. The basic layout of the TSC is shown in Figure F-8.13-7.



F-8.13-7 Basic Layout of the TSC

8.13.7.5.3 Environment of TSC

The TSC is in the same inhabitable area of the plant as the MCR, and is supported by the same HVAC as the MCR.

8.14 System Development and Justification

This sub-chapter supports the following safety feature claims: I&C-C2.2, I&C-C3.1 and I&C-C4.

8.14.1 System Development

The system development activities are initiated after the overall I&C architecture and the I&C functions allocation are defined. The development of I&C systems important to safety for the UK HPR1000 is in accordance with the requirements of IEC 61513, Reference [5]. For the computer based I&C systems, the software development is in accordance with IEC 60880, Reference [6] for F-SC1 systems and IEC 62138, Reference [14] for F-SC2 and F-SC3 systems, while the hardware development is in accordance with IEC 60987, Reference [15] for F-SC1 and F-SC2 systems.

8.14.1.1 System Lifecycle

The development of I&C systems important to safety follows a lifecycle approach based on IEC 61513, Reference [5].

a) System requirements specification

   The system requirements are developed, including functional requirements, performance requirements, interface requirements, plant constraints, applicable environmental conditions and qualification requirements.

b) System specification

   The system technical solution which fulfils the system requirements is developed, including system architecture, equipment to be used or developed, allocation of the application functions to subsystems, hardware requirements and software requirements.

c) System detailed design and implementation

   The detailed design of the system hardware and software is developed and analysed, and the hardware and software are implemented accordingly.

d) System integration

   The hardware and software components are assembled to make up the system, and the compatibility of the software loaded into the hardware is verified.

e) System validation

   The integrated system is tested to demonstrate its compliance with the system functional, performance and interface specification. The validation is comprised of tests performed on the system in the final assembly configuration including the final version of the software and other programming data.

f) System installation

The system is installed and interconnected with other systems on site, and the functionality is tested.

g) System modification

System modification may be required due to the identification of new system requirement or the discovery of system design defects during system operation. The modification is carried out in accordance with defined procedures, and then the corresponding test is performed to validate its correctness.

8.14.1.2 Equipment Qualification

The equipment qualification is performed to make sure I&C equipment continuously has its designated function in the environmental conditions expected during postulated events, e.g. seismic, EMI and environmental events. The equipment qualification is conducted by type tests and is supplemented by analysis. The programs and procedures of the qualification conform to the relevant codes and standards.

The qualification of essential I&C equipment mainly consists of environmental test, EMC test and seismic test. The qualification process is in accordance with IEC 60780 (qualification), Reference [17], IEC 60980 (seismic), Reference [18] and IEC 61000 series (EMC), Reference [22].

The qualification requirements of equipment are also subject to its operational environmental conditions. For example, if the equipment is located in the containment or operated in severe accident conditions, the environmental conditions of these situations are the requirements of the qualification tests.

8.14.1.3 Software Verification and Validation (V&V)

The software of the computer based I&C systems important to safety is verified and validated throughout the development process according to the system classification. V&V activities are applied to both the system (platform) software and the application software. The software V&V of F-SC1 system is carried out in accordance with IEC 60880, Reference [6]. The software V&V of F-SC2 and F-SC3 systems is carried out in accordance with IEC 62138, Reference [14].

8.14.2 System Justification

For the computer based I&C systems important to safety, the quality of the development process and the final product is demonstrated by a two-legged approach, which is considered as good practice in the UK context.

a) Production Excellence (PE)

A demonstration of excellence in all aspects of production from the initial specification through to the final commissioned system, including:

1) The thorough application of technical design practice consistent with current accepted standards for the software development of the system;

2) The implementation of a modern standards quality management system;

3) The application of a comprehensive testing program formulated to check every system function.

The demonstration of standards compliance will cover quality management and testing activities, and the applicable standards adapted in the system development will be used.

If weaknesses are identified in the production process, compensatory measures will be applied to address them case by case.

b) Independent Confidence Building Measures (ICBMs)

An independent and thorough assessment of the system's fitness for purpose, comprising the following elements:

1) The complete and preferably diverse checking of the finally validated software by a team that is independent of the suppliers, including:

- Independent product checking that provides a searching analysis of the final system;

- Independent checking of the design and production process including the activities undertaken to confirm the realisation of the design intent.

2) The independent assessment of the comprehensive testing program covering the full scope of the test activities.

ICBMs are carried out on the finally delivered system, and they will be completed in the nuclear site licensing phase. However, the demonstration methodology will be developed and a pilot study of the selected methods will be completed during the GDA process.

8.14.3 I&C Platforms

There are four I&C platforms applied in the development of the Centralised I&C systems of the UK HPR1000, i.e. FirmSys, HOLLiAS-N, FitRel and SpeedyHold. The development process of these I&C platforms complies with the relevant standards and good practice.

8.14.3.1 Design and Implementation

8.14.3.1.1 FirmSys

The FirmSys platform is a qualified safety digital I&C platform which is applied to F-SC1 and F-SC2 I&C systems including the PS and the SAS in the UK HPR1000.

The overall design development of these systems refers to the requirements defined in IEC 61513, Reference [5].

a) Software design and implementation

The software development of the FirmSys platform is compliant with IEC 60880, Reference [6].

The I&C functional requirements are available before the software design and implementation begins. The I&C functional requirements constitute the main inputs for the design and are used during the V&V steps to prove the conformance of the application software with these requirements.

The FirmSys platform application software is mainly designed using the real-time and deterministic application coding environment tool of the engineering application software toolkit. The SCID application software is designed using the safe video graphic console panel environment design tool of the engineering application software toolkit. In real-time and deterministic application coding environment software tools, the graphical user interface is used via combining basic graphic operators to design and generate application software with algorithm functions. The safe video graphic console panel environment design tool software offers different types of icon libraries, and users can flexibly configure all kinds of graphic and element objects of the display graphic. The software also provides a built-in page template library which enables specific functions, while allowing users to define the page template library themselves.

b) Hardware design and implementation

The hardware development of the FirmSys platform is compliant with IEC 60987, Reference [15].

The hardware requirements are available before the start of the design phase. The design phase implements the hardware requirements and provides the basis for the verification of the design.

8.14.3.1.2 HOLLiAS-N

The HOLLiAS-N platform is a general digital I&C platform which is applied to F-SC3 I&C systems including the PSAS and the KIC [PCICS] in the UK HPR1000.

a) Software design and implementation

The software development of the application programme in the HOLLiAS-N platform is compliant with the requirements of category C functions in IEC 62138, Reference [14].

The I&C functional requirements are available before the software design and implementation begins. The functional requirements (captured in functional

diagrams and screen formats) constitute the main input for the design and are used during the V&V steps to prove the conformance of the application software with these requirements.

The application software is mainly designed and implemented by the MACS VI tools, including:

1) Project Explorer: The main interface of the configuration system;
2) AutoThink: The programming tool for creating controller applications;
3) The HMI-editor enables engineers to design a direct and clear OWP interface.

The MACS VI tools provide a function-oriented graphical representation of the software and make the design understandable for the I&C engineer (who can design the software without programming knowledge), the process engineer (who verifies the compliance with the functional requirements) and the end user (who operates the I&C systems).

b) Hardware design and implementation

The hardware requirements are available before the start of the design phase. The hardware design and configuration is based on standardised catalogues for processing. The following hardware design activities are supported by tools:

1) Choice of devices based on standard catalogues;
2) Device arrangement in cabinets;
3) Interconnection between devices.

8.14.3.1.3 FitRel

The FitRel platform is a general I&C platform based on FPGA technology which is applied to the KDS [DAS] (F-SC3) in the UK HPR1000. The logic design of the KDS [DAS] refers to the requirements of category C functions in IEC 62138, Reference [14], and the hardware development is compliant with IEC 60987, Reference [15].

The function blocks are developed in Hardware Description Language (HDL) by using the Libero tool, and they can be used to be inter-connected and configured to meet different logic function requirements. The graphical user interface provided by the Libero tool is simple and can be easily understood by the logic designer.

The hardware requirements are available before the start of the design phase. The hardware design and configuration is based on standard hardware catalogues. The following hardware design activities are performed:

a) Choice of devices based on standard hardware catalogues;

b) Device arrangement in cabinets;

c) Interconnection between devices.

8.14.3.1.4 SpeedyHold

The SpeedyHold platform is a general computer based I&C platform which is applied to the KDA [SA I&C], the ACP and the DHP in the UK HPR1000.

a) Software design and implementation

The software development of the SpeedyHold platform is compliant with the requirements of category C functions in IEC 62138, Reference [14].

The software requirements are available before the software design and implementation begins. The functional requirements constitute the main input for the design and are used during the V&V steps to prove the conformance of the application software with these requirements.

The application software is mainly designed and implemented by the SpeConT, SpeGEditor and SpeProg tools:

1) SpeConT: The main interface of the configuration system;

2) SpeProg: The programming tool for creating the application software;

SpeGEditor: The tool that provides standardised and pre-existing software modules for the design and coding of HMI software.

b) Hardware design and implementation

The hardware requirements are available before the start of the design phase. The hardware design and configuration process is the same as the HOLLiAS-N platform.

8.14.3.2 Equipment Qualification

A series of qualification tests including the pre-qualification acceptance test, environmental test, EMC test and seismic test are conducted on the FirmSys platform in accordance with IEC 60780, Reference [17].

a) Pre-qualification acceptance test

In accordance with IEC 60780, Reference [17], the FirmSys pre-qualification acceptance test including the test for board function, performance, dielectric strength and insulation resistance is conducted in normal environmental conditions so as to generate test data for the follow-up test benchmark. Technical specifications of respective products are referred to for its pre-qualification acceptance test and conformity criteria.

b) Environmental test

According to IEC 60780, Reference [17], the limit conditions concerning equipment transportation, storage and operation are considered in the environmental test. The environmental test performed for the FirmSys prototype comprises of a temperature variation test, cyclic damp heat test, long-term operation test, temperature and humidity combined test and mechanical vibration test.

c) EMC test

The EMC test is conducted mainly according to IEC 61000 series, Reference [22], including conducting an emission test, radiated emission test, harmonic immunity of AC power lines test, conducted susceptibility induced by radio frequency field, electrical fast transient, combination wave, ring wave, test of 0-150kHz immunity to conducted common mode disturbance, radiated susceptibility, power frequency magnetic field immunity, pulsed magnet field immunity, damped magnet field immunity and electro static discharge test.

d) Seismic test

The seismic test is carried out after the completion of the environmental test and the EMC test, as required by IEC 60980, Reference [18]. In the seismic test process, the chassis, modules or cabinets are installed to the seismic platform, and five “1/2 Safe Shutdown Earthquake (SSE)” tests and one SSE tests are carried out before the pre-check of the functional performance.

8.14.3.3 Software V&V

V&V activities are performed throughout the whole development process of the software in order to identify and trace anomalies during the software development process, to reveal and control the process risks and validate the final delivered software to meet the requirements from users and regulations.

The software V&V of the FirmSys platform is performed by V&V teams based on IEC 60880, Reference [6].

The methods of software V&V are comprised of evaluation, specific analysis and test.

The software V&V is comprised of the following two parts:

a) Platform software V&V

The platform software V&V activities are performed to verify that the platform software achieves the required quality level. The scope of the V&V is comprised of the embedded software, programmable logic, function block library and converting tools.

b) Application software V&V

Application software V&V activities are performed. The scope of the V&V is

comprised of the embedded software, programmable logic, engineering display and software configuration data.

8.14.4 Smart Devices

The smart device is a device that contains a microprocessor or other form of complex programmable electronic components to provide specialised capabilities, e.g. measuring, actuating and recording. It often contains pre-developed software or programmed logic (e.g. FPGA) which cannot be re-programmed after manufacturing and can only be configured by the end user.

If the use of smart devices cannot be avoided due to the fact that the traditional devices, with the same required functionality and reliability, are not available for commercial acquisition or some other reasons, they will be justified in a manner consistent with the classification of the system that they are deployed in. The justification will be performed through a two-legged approach:

a) Production Excellence

Compliance with the applicable safety standards is demonstrated as the basis. The industry safety standard IEC 61508, Reference [27] is used for the smart devices already having certification according to IEC 61508. Otherwise the nuclear safety standard IEC 62671, Reference [28] is used.

If the smart device is to be assessed against IEC 61508, Reference [27], it will need to be compliant with the requirements of SIL3/SIL2/SIL1 when used in an F-SC1/F-SC2/F-SC3 system respectively.

If the smart device is to be assessed against IEC 62671, Reference [28], it will need to be compliant with the requirements commensurate with the intended application of the corresponding class (class 1/class 2/class 3) when used in an F-SC1/F-SC2/F-SC3 system respectively.

If minor gaps are identified in the standards compliance demonstration, additional compensating measures will be applied to address the gaps.

b) Independent Confidence Building Measures (ICBMs)

The independent and thorough assessment of the fitness for purpose will be performed by a team that is independent of the device supplier. This task will be initiated after the PE activities are finished and the identified gaps are addressed (if any).

The techniques, e.g. desktop review, type testing, static analysis, dynamic testing and statistical testing, will be selected according to the classification of the system in which the smart device is to be employed. When used in F-SC1 or F-SC2 systems, analysis of the source code will be performed. However, for smart device to be used in F-SC2 systems, if the source code is not accessible,

statistical testing will be performed instead. When used in F-SC3 systems, assessment of the source code is not necessary, and black box testing is sufficient.

The measures adopted by ICBMs will be diverse from those used as compensating measures for the PE.

The approach and techniques for smart device justification will be developed and applied to sample devices during the GDA process to demonstrate that they work.

8.15 Commissioning

This sub-chapter supports the safety feature claim I&C-C4.

In order to demonstrate the functional characteristics of operation and safety, acceptance tests of SSCs will be implemented at site. The commissioning activities of I&C systems will be developed and carried out independent of the system supplier, including post-installation inspection, component commissioning, system commissioning, system start-up and performance tests. The arrangements for the development and management of the commissioning are discussed in Chapter 30 in detail.

The commissioning arrangements will be adapted from those developed for the HPR1000 (FCG3). Except the contents described in Chapter 30, further arrangements for the UK HPR1000 commissioning activities will be presented during the nuclear site licensing phase.

8.16 EMIT and Ageing

This sub-chapter supports the safety feature claim I&C-C5.

8.16.1 Examination, Maintenance, Inspection and Testing

The regular and systematic EMIT of I&C systems in the plant life cycle are implemented to ensure that the I&C systems are operated within the operational limits and in accordance with the design assumptions and intent. The EMIT activities of I&C systems involve the qualification, factory acceptance test, commissioning test and maintenance. The qualification, factory acceptance test and commissioning test are implemented to ensure the initial quality and reliability of I&C systems, while maintenance is implemented to ensure the continuing quality and reliability of I&C systems during plant operation.

The maintenance activities of I&C systems and equipment are divided into preventive and corrective maintenance, which are described as follows:

a) Preventive maintenance includes periodic, predictive and planned maintenance activities and is performed prior to failure of I&C equipment or components in order to maintain their service life by controlling degradation or preventing their failure. Preventive maintenance activities of I&C systems involve inspection,

sensor calibration, surveillance test and replacement of equipment or components.

In the UK HPR1000, surveillance test is implemented by self-diagnosis and periodic test, and there are three types of periodic tests:

1) T1 test: the instruments channel test is implemented to check the correct operation of input signals of I&C systems;

2) T2 test: the processing channel test is implemented to check the correct operation of the logic inside the processing units of I&C systems;

3) T3 test: the actuator control channel test is implemented to check the correct operation of output signals sent to the actuators of I&C systems.

The general requirements of self-diagnosis and periodic test are described in Sub-chapter 8.5.7.

b) Corrective maintenance includes activities that, by means of repair, overhaul or replacement, restore the capability of failed I&C equipment or components to perform their defined function. In the UK HPR1000, I&C system faults can be self-diagnosed and announced to maintenance staff. Hot plug is allowed for maintenance activities during plant operation.

Further information on maintenance activities of I&C systems and equipment will be presented during the nuclear site licensing phase.

8.16.2 Ageing Degradation

Ageing management is implemented to ensure that any potential impact on NPP safety due to I&C ageing degradation will be identified and that suitable activities are performed to demonstrate that the safety of the plant will not be impaired. The approach of ageing management refers to IEC 62342, Reference [23]. The ageing management mainly involves the following three steps in the UK HPR1000:

a) Based on the experience of ageing mechanisms and ageing effects, I&C equipment or components which are susceptible to ageing mechanisms and whose failure has a significant consequence on safety systems will be identified.

b) The ageing degradation of I&C equipment or components identified will be evaluated to demonstrate that the required level of plant safety can be assured throughout the system operation. The two approaches for evaluation are as follows:

1) An analysis approach combined with qualification and calculation;

2) A pragmatic approach combined with equipment testing, visual inspection, operating experience, and engineering judgment.

c) The necessary mitigating actions will be implemented to counteract the effects of

ageing, e.g. improved testing and maintenance, establishing ageing control programs, and developing modification and replacement strategies.

In the UK HPR1000 I&C design, the ageing degradation of equipment or components susceptible to ageing mechanisms, which are not easily replaced, will be evaluated by the analysis approach combined with qualification and calculation, e.g. cables and connectors. The ageing degradation of equipment or components susceptible to ageing mechanisms, which are easily replaced, will be evaluated by the pragmatic approach with a qualitative judgment, e.g. I/O modules.

The ageing control of these equipment or components is managed by ageing control programs. During the nuclear site licensing phase, further information of the ageing management will be presented.

8.17 ALARP Assessment

This sub-chapter supports the following safety feature claims: I&C-C3.1 and I&C-C3.2.

Refer to Table T-8.4-1 for details.

8.17.1 General Description

This sub-chapter gives a high level overview of the ALARP principles to be applied in Chapter 8 for I&C systems. Chapter 33 presents a generic approach used for demonstrating that the UK HPR1000 design is ALARP. The main steps of this approach are listed as follows:

a) Presenting a design evolution review of the HPR1000 design to demonstrate that safety improvements have been incorporated and OPEX has been considered;

b) Systematic Reviews of the UK HPR1000 design against RGP, OPEX and insights from the PSA;

c) Identifying and collating the potential improvements;

d) Optioneering which is the process of generation and evaluation of options;

e) Implementing all reasonably practicable options until a suitable solution is reached and the ALARP justification is given;

f) Performing an iterative holistic review of the UK HPR1000 design.

The I&C ALARP analysis process follows the generic approach, including the following steps:

a) Presenting the HPR1000 I&C design evolution;

b) Identifying and analysing the UK RGP and OPEX;

c) Analysing the insights from the PSA;

d) Identifying gaps through step b) and step c);

e) Undertaking the optioneering;

f) Selecting an optimal solution and implementation of it to close the gaps and giving the ALARP justification.

8.17.2 Presenting the HPR1000 I&C Design Evolution

The design evolution of the HPR1000 is described in Chapter 33.

The design evolution of HPR1000 I&C systems and platforms is described in Sub-chapter 8.2.

8.17.3 Identifying and Analysing the UK RGP and OPEX

The RGP conformance analysis is the starting point of the ALARP analysis. An in-depth review of the RGP is undertaken to help identify suitable options to reduce the risks. In UK HPR1000 I&C systems design, the sources of RGP mainly include the following aspects:

a) IAEA safety standards;

b) Recognised design codes and standards;

c) SAPs and TAGs;

d) Regulator expectations.

The UK HPR1000 I&C systems are designed according to the relevant IEC standards and IAEA guidance. The design of I&C overall architecture and systems is considered to meet the requirements of IEC 61513, Reference [5]. The safety classification is derived from the safety functional requirements, which is considered to meet IAEA SSG-30, Reference [4]. The DiD design of I&C systems is considered to meet the requirements of plant DiD and IAEA SSR-2/1, Reference [8]. The safety features including diversity, independence, SFC, redundancy, etc., are referred to in IAEA SSG-39, Reference [9]. Further information about codes and standards is described in Sub-chapter 8.3.

Besides the RGP, the previous GDA experience is a source of OPEX. A major advantage of the UK HPR1000 I&C systems design is that the OPEX learned from similar units has been integrated, including the lessons learned from the Japanese Fukushima nuclear accident and the operating plant experience of CGN. The development of the main technical features for UK HPR1000 I&C systems is described in Sub-chapter 8.2.

The OPEX from previous GDA experience is considered. This information and regulator expectations are important parts integrated in the UK HPR1000 I&C systems design.

8.17.4 Analysing the Insight from the PSA

This is a cross-cutting technical issue. The insights from PSA for the UK HPR1000 are not available in the current phase, and further work and efforts will be made after receiving the results from the UK HPR1000 PSA.

8.17.5 Identifying Gaps

The gaps have been identified and analysed, and will be eliminated gradually in GDA step 3 and step 4.

8.17.6 Undertaking an Options Analysis

This process requires analysing the risk of potential improvements which have been identified, and then provides corresponding improvement schemes for these improvements. The options analysis applies the ALARP methodology.

For I&C scheme options, it consists of the following aspects:

a) Analysing the risk of the potential improvements;

b) Generating risk reduction options;

c) Identifying assessment criteria;

d) Assessing the options against identified criteria.

The risk reduction options identification is a wide range of potential options that not only lead to the selection of the appropriate option but also help in the demonstration that there are no additional reasonably practicable options to those selected. An important part of this process is ensuring an appropriate team is selected to conduct the option study.

Suitable assessment criteria are chosen and defined to ensure that there is differentiation between the various options. Examples of criteria are listed as follows:

a) Nuclear safety and conventional safety;

b) Impact on environment;

c) Technical difficulty;

d) Cost;

e) Schedule.

Once a list of viable options has been generated, the benefits and disadvantages of each option are identified in order to assess each option and provide input to the decision making process.

8.17.7 Selecting an Optimal Solution and Implementation to Close the Gaps and Giving the ALARP Justification

After analysis of the options, all reasonably practicable options are considered and further analysis is implemented until a suitable solution is reached. The final scheme is to close the gaps between the UK HPR1000 and UK context.

The ALARP justification is provided proportionately to different GDA phases and more information is provided for GDA step 3 and step 4.

8.18 Concluding Remarks

Chapter 8 presents the design principles of the I&C systems, and describes the overall I&C architecture and I&C systems of different safety classifications as well as the main HMIs of the UK HPR1000.

Chapter 8 presents that the I&C systems developed for the UK HPR1000 adopt proven technology and are designed to be reliable and safe. Meanwhile the I&C systems meet the safety functional requirements and contribute to the DiD of the whole plant.

This chapter provides confidence that the I&C systems developed for the UK HPR1000 are in compliance with UK requirements including the requirements of IEC standards. The claims described in this chapter are supported by the main body of the PCSR and the supporting documents.

8.19 References

[1] CGN, General Principles for Application of Laws, Regulations, Codes and Standards, GHX00100018DOZJ03GN, Revision F, August 2018.

[2] IAEA, Software for Computer Based Systems Important to Safety in Nuclear Power Plants Safety Guide, NS-G-1.1, 2000.

[3] IAEA, Instrumentation and Control Systems Important to Safety in Nuclear Power Plants Safety Guide, NS-G-1.3, 2002.

[4] IAEA, Safety Classification of Structures, Systems and Components in Nuclear Power Plants, SSG-30, 2014.

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

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

[7] IEEE, Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations, IEEE 497, November 2010.

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

[9] IAEA, Design of Instrumentation and Control Systems for Nuclear Power Plants, SSG-39, 2016.

[10] ONR, Safety Assessment Principles for Nuclear Facilities, Revision 0, 2014.

[11] ONR, Safety Systems, NS-TAST-GD-003, Revision 8, March 2018.

[12] ONR, Computer Based Safety Systems, NS-TAST-GD-046, Revision 4, February 2017.

[13] IEC, Nuclear power plants - Instrumentation and control systems important to safety - Classification of instrumentation and control functions, IEC 61226, Revision 3, 2009.

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

[15] IEC, Nuclear power plants - Instrumentation and control systems important to safety - Hardware design requirements for computer-based systems, IEC 60987, 2013.

[16] IEC, Nuclear power plants - Instrumentation and control systems important to safety - Requirements for coping with common cause failure (CCF), IEC 62340, Revision 1, 2007.

[17] IEC, Nuclear facilities - Electrical equipment important to safety - Qualification, IEC 60780, 2016.

[18] IEC, Recommended practices for seismic qualification of electrical equipment of the safety system for nuclear power stations, IEC 60980, Revision 1, 1989.

[19] IEC, Nuclear power plants - Instrumentation and control systems important to safety – Separation, IEC 60709, Revision 2, November 2004.

[20] IEC, Nuclear power plants - Instrumentation and control systems important to safety - Surveillance testing, IEC 60671, Revision 2, 2007.

[21] IEC, Nuclear power plants - Instrumentation and control systems important to safety - Data communication in systems performing category A functions, IEC 61500, Revision 2, 2009.

[22] IEC, Electromagnetic compatibility, IEC 61000 series.

[23] IEC, Nuclear power plants - Instrumentation and control systems important to safety - Management of ageing, IEC 62342, 2007.

[24] IEC, Nuclear power plants - Main control room - Computer based procedures,

IEC 62646, 2016.

[25] IEC, Nuclear power plants - Control rooms - Design, IEC 60964, Revision 2, 2009.

[26] IEC, Nuclear power plants - Control rooms - Supplementary control points for reactor shutdown without access to the main control room, IEC 60965, 2016.

[27] IEC, Functional safety of electrical/electronic/programmable electronic safety-related systems, IEC 61508, Revision 2, 2010.

[28] IEC, Nuclear power plants - Instrumentation and control important to safety - Selection and use of industrial digital devices of limited functionality, IEC 62671, Revision 1, 2013.

[29] CGN, BSC of Overall I&C Architecture, GHX06002001DIYK01GN, Revision B, 2018.

[30] CGN, Reliability Targets of the I&C Systems for UK HPR1000, GHX06001015DIYK03GN, Revision B, 2018.

[31] CGN, Methodology of Safety Categorisation and Classification, GHX00100062DOZJ03GN, Revision B, 2018.

[32] CGN, HFE Design Guidelines for Control Room, GHX06001021DIKX03GN, Revision D, April 2018.

[33] CGN, Overall Scheme for Control Room System, GHX06001009DIKX03GN, Revision C, 2018.

Appendix 8A I&C Systems Function Claims[6]

Claims Name	Claims Content	Safety Function Claims for the Centralised I&C Systems	Linking Sub-chapters
I&C-C1.1.2-R1	R1 - Maintain core reactivity control	The PSAS provides the FC3 functions to maintain core reactivity control.	8.8.1.2
I&C-C1.1.2-R2	R2 - Shutdown and maintain core sub-criticality	The PS provides the FC1 functions to shut down the reactor and maintain core sub-criticality.	8.6.2
		The SAS provides the FC2 functions to shut down the reactor and maintain core sub-criticality.	8.7.2
		The PSAS provides the FC3 functions to shut down the reactor and maintain core sub-criticality.	8.8.1.2
		The KDS [DAS] provides the FC3 functions to shut down the reactor and maintain core sub-criticality as the diverse line of protection.	8.8.3.2

[6] The claims for safety functions are developed corresponding to the identification of fundamental safety functions described in Sub-chapter 4.4.3. In Appendix 8A, the fundamental functions are represented by the letters as follow:
R: Control of reactivity (including prevention of accidental criticality);
H: Removal of heat from the reactor and from the fuel store;
C: Confinement of radioactive material, shielding against radiation and control of planned radioactive releases, as well as limitation of accidental radioactive releases;
E: Extra safety functions.

Claims Name	Claims Content	Safety Function Claims for the Centralised I&C Systems	Linking Sub-chapters
I&C-C1.1.2-R3	R3 - Prevention of uncontrolled positive reactivity insertion into the core	The PS provides the FC1 functions to prevent uncontrolled positive reactivity insertion into the core.	8.6.2
		The SAS provides the FC2 functions to prevent uncontrolled positive reactivity insertion into the core.	8.7.2
		The PSAS provides the FC3 functions to prevent uncontrolled positive reactivity insertion into the core.	8.8.1.2
		The KDS [DAS] provides the FC3 functions to prevent uncontrolled positive reactivity insertion into the core as the diverse line of protection.	8.8.3.2
I&C-C1.1.3-H1	H1 - Maintain sufficient RCP [RCS] water inventory for core cooling	The PS provides the FC1 functions to maintain sufficient RCP [RCS] water inventory for core cooling.	8.6.2
		The SAS provides the FC2 functions to maintain sufficient RCP [RCS] water inventory for core cooling.	8.7.2
		The PSAS provides the FC3 functions to maintain sufficient RCP [RCS] water inventory for core cooling.	8.8.1.2

Claims Name	Claims Content	Safety Function Claims for the Centralised I&C Systems	Linking Sub-chapters
I&C-C1.1.3-H1	H1 - Maintain sufficient RCP [RCS] water inventory for core cooling	The KDS [DAS] provides the FC3 functions to maintain sufficient RCP [RCS] water inventory for core cooling as the diverse line of protection.	8.8.3.2
I&C-C1.1.3-H2	H2 - Remove heat from the core to the reactor coolant	The PS provides the FC1 functions to remove heat from the core to the reactor coolant.	8.6.2
		The SAS provides the FC2 functions to remove heat from the core to the reactor coolant.	8.7.2
		The PSAS provides the FC3 functions to remove heat from the core to the reactor coolant.	8.8.1.2
		The KDS [DAS] provides the FC3 functions to remove heat from the core to the reactor coolant as the diverse line of protection.	8.8.3.2
I&C-C1.1.3-H3	H3 - Transfer heat from the reactor coolant to the ultimate heat sink	The PS provides the FC1 functions to transfer heat from the reactor coolant to the ultimate heat sink.	8.6.2
		The SAS provides the FC2 functions to transfer heat from the reactor coolant to the ultimate heat sink.	8.7.2

Claims Name	Claims Content	Safety Function Claims for the Centralised I&C Systems	Linking Sub-chapters
I&C-C1.1.3-H3	H3 - Transfer heat from the reactor coolant to the ultimate heat sink	The PSAS provides the FC3 functions to transfer heat from the reactor coolant to the ultimate heat sink.	8.8.1.2
		The KDA [SA I&C] provides the FC3 functions to transfer heat from the reactor coolant to the ultimate heat sink in the severe accident mitigation strategy.	8.8.2.2
		The KDS [DAS] provides the FC3 functions to transfer heat from the reactor coolant to the ultimate heat sink as the diverse line of protection.	8.8.3.2
I&C-C1.1.3-H4	H4 - Maintain heat removal from fuel stored outside the RCP [RCS] but within the site	The PS provides the FC1 functions to maintain heat removal from fuel stored outside the RCP [RCS] but within the site.	8.6.2
		The SAS provides the FC2 functions to maintain heat removal from fuel stored outside the RCP [RCS] but within the site.	8.7.2
		The PSAS provides the FC3 functions to maintain heat removal from fuel stored outside the RCP [RCS] but within the site.	8.8.1.2

Claims Name	Claims Content	Safety Function Claims for the Centralised I&C Systems	Linking Sub-chapters
I&C-C1.1.3-H4	H4 - Maintain heat removal from fuel stored outside the RCP [RCS] but within the site	The KDS [DAS] provides the FC3 functions to maintain heat removal from fuel stored outside the RCP [RCS] but within the site as the diverse line of protection.	8.8.3.2
I&C-C1.1.4-C2	C2 - Maintain integrity of the Reactor Coolant Pressure Boundary (RCPB) to ensure confinement of radioactive material	The PS provides the FC1 functions to maintain integrity of the RCPB.	8.6.2
		The SAS provides the FC2 functions to maintain integrity of the RCPB.	8.7.2
		The PSAS provides the FC3 functions to maintain integrity of the RCPB.	8.8.1.2
		The KDS [DAS] provides the FC3 functions to maintain integrity of the RCPB as the diverse line of protection.	8.8.3.2
I&C-C1.1.4-C3	C3 - Maintain integrity of reactor containment to ensure confinement of radioactive material	The PS provides the FC1 functions to maintain integrity of reactor containment.	8.6.2
		The SAS provides the FC2 functions to maintain integrity of reactor containment.	8.7.2
		The KDA [SA I&C] provides the FC3 functions to maintain integrity of reactor containment in the severe accident mitigation strategy.	8.8.2.2

Claims Name	Claims Content	Safety Function Claims for the Centralised I&C Systems	Linking Sub-chapters
I&C-C1.1.4-C3	C3 - Maintain integrity of reactor containment to ensure confinement of radioactive material	The KDS [DAS] provides the FC3 functions to maintain integrity of reactor containment as the diverse line of protection.	8.8.3.2
I&C-C1.1.4-C4	C4 - Maintain integrity of the fuel stored outside of reactor containment	The PS provides the FC1 functions to maintain integrity of the fuel stored outside of reactor containment.	8.6.2
		The SAS provides the FC2 functions to maintain integrity of the fuel stored outside of reactor containment.	8.7.2
		The PSAS provides the FC3 functions to maintain integrity of the fuel stored outside of reactor containment.	8.8.1.2
		The KDA [SA I&C] provides the FC3 functions to maintain integrity of the fuel stored outside of reactor containment in the severe accident mitigation strategy.	8.8.2.2
		The KDS [DAS] provides the FC3 functions to maintain integrity of the fuel stored outside of reactor containment as the diverse line of protection.	8.8.3.2

Claims Name	Claims Content	Safety Function Claims for the Centralised I&C Systems	Linking Sub-chapters
I&C-C1.1.5-E1	E1 - Support the type R, H or C safety function	The PS provides the FC1 functions to support the type R, H or C safety function.	8.6.2
		The SAS provides the FC2 functions to support the type R, H or C safety function.	8.7.2
		The PSAS provides the FC3 functions to support the type R, H or C safety function.	8.8.1.2
		The KDA [SA I&C] provides the FC3 functions to support the type R, H or C safety function in the severe accident mitigation strategy.	8.8.2.2
		The KDS [DAS] provides the FC3 functions to support the type R, H or C safety function as the diverse line of protection.	8.8.3.2
I&C-C1.1.5-E2	E2 - Prevent, protect and mitigate hazard impact	The PSAS provides the FC3 functions to prevent, protect and mitigate hazard impact.	8.8.1.2