Eskom	Standard	Technology

Title: **Power Plant Controls & Instrumentation; Control Systems; Distributed Control Systems (DCS); Part 3: Engineering System Standard**

Unique Identifier:	**240-132042345**
Alternative Reference Number:	**N/A**
Area of Applicability:	**Engineering**
Documentation Type:	**Standard**
Revision:	**1**
Total Pages:	**16**
Next Review Date:	**January 2024**
Disclosure Classification:	**CONTROLLED DISCLOSURE**

Compiled by	Approved by	Authorised by
……..	……..	……..
Chief Engineer, C&I Plant	**Middle Manager, C&I Plant (Acting)**	**Senior Manager, EC&I**
Date: ……	Date: ……	Date: ……

Supported by SCOT/SC/TC

……..

Chairperson, Power Plant C&I SC

Date: ……

PCM Reference: **240-53458811**

SCOT Study Committee Number/Name: **Power Plant C&I SC**

CONTENTS

Page

FIGURES

TABLES

1. INTRODUCTION

A distributed control system is a control system that is used in the process industry to monitor, operate and control process plant. In general, distributed control systems are highly configurable and are designed for use in a wide range of industries such as manufacturing, oil & gas, mining and power generation. While each industrial sector has the same basic control requirements, the specific design requirements of each can differ widely as a result of its availability, reliability and maintainability targets.

As such, this multipart document defines the design requirements for a DCS used in Eskom power plants; with the overall intent of ensuring that the DCS is highly available, reliable and maintainable over the life of the power plant.

This multipart document has five parts, with this part being **Part 3: Engineering System**. Each part addresses a separate technical aspect of the DCS. The framework of this multipart document is as shown in Table 1 and Figure 1.

Table 1: Overall framework of this multipart document

Part	Title	Requirements addressed in this part
1	General	Overall requirements, framework and definitions
2	Operator & Supervisor System	Supervision and monitoring layer
3	Engineering System **[This Part]**	Engineering and diagnostic layer
4	Automation System	Automation layer
5	Network & Computer Equipment	Communication networks and computers

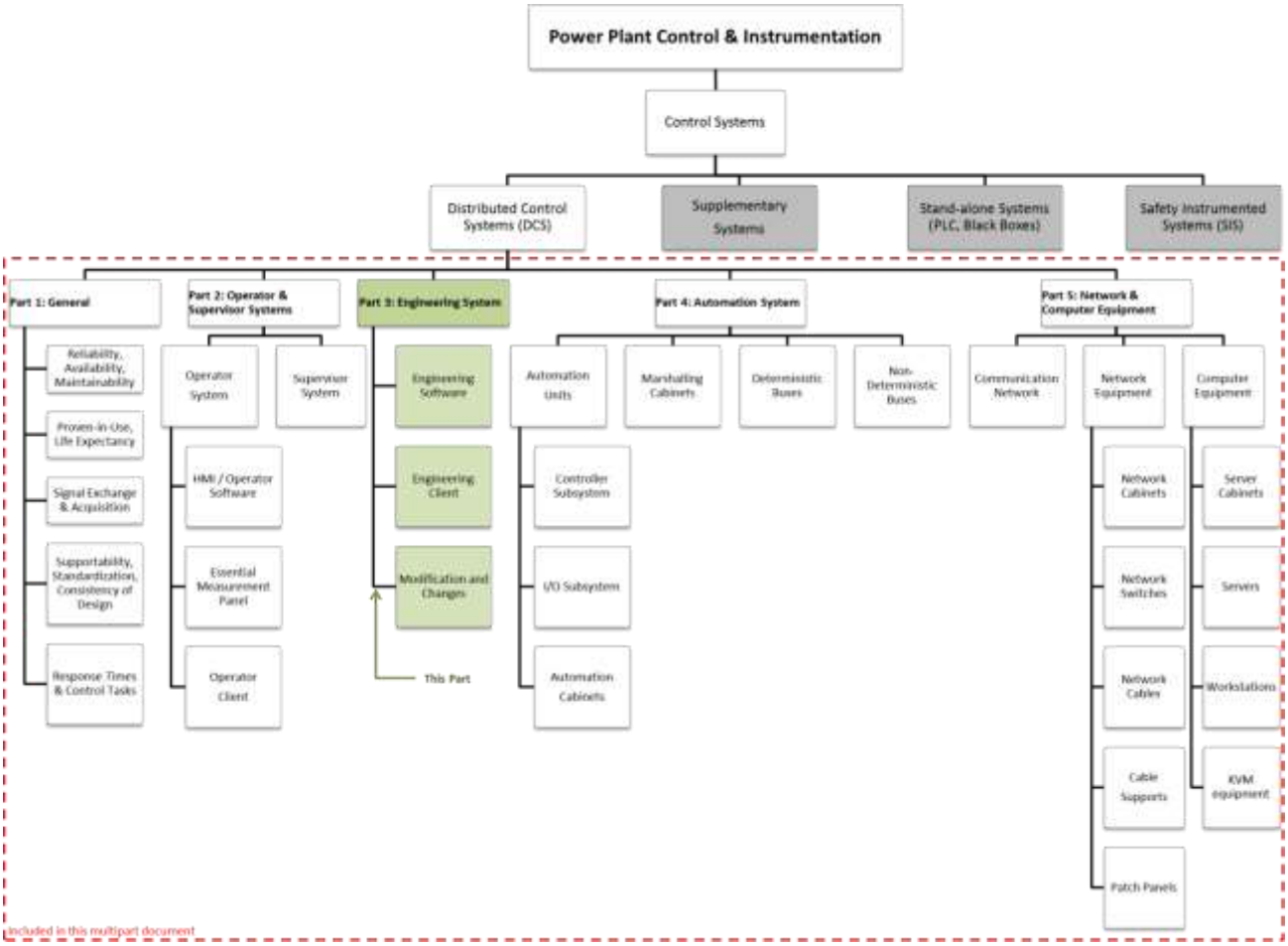

Figure 1: Overall framework of this multipart document

2. SUPPORTING CLAUSES

2.1 SCOPE

This multipart document specifies the design requirements for a power plant's distributed control system (DCS). In particular, it defines the design requirements for the operator & supervisor system, engineering system, automation system and network & computer equipment.

This multipart document has five parts, with this document being **Part 3: Engineering system**; the scope of which is the specification of the engineering systems. It excludes specification of the content of design documentation.

The scope of this multipart document excludes the operational and maintenance (O&M) requirements of a DCS.

2.1.1 Purpose

The objective of this multipart document is to define the design requirements for a DCS used in Eskom power plants; with the overall intent of ensuring that the DCS is highly available, reliable and maintainable over the life of the power plant.

2.1.2 Applicability

This document does not apply to nuclear power plants. This document applies to distributed control systems installed in all other Eskom power plants after this document was first published, this being January 2019. As such it applies to new build; refurbishment; DCS migration; and HMI retrofit projects.

2.2 NORMATIVE/INFORMATIVE REFERENCES

Parties using this document shall apply the most recent edition of the documents listed in the following paragraphs.

2.2.1 Normative

[1] VGB R 170 B5e: VGB PowerTech; Design standards for instrumentation and control equipment: Field device visualisation.

[2] VGB R 170 Ce: VGB PowerTech; Function-related documentation of power plant instrumentation and control in line with operating requirements.

[3] VGB R 170B2e: VGB PowerTech; Design standards for instrumentation and control equipment: Automation Function.

[4] VGB B 106B4e: VGB PowerTech; KKS- Identification System for Power Stations: Identification of instrumentation and control tasks/functions in process systems and identification of functions in instrumentation and control systems.

[5] VGB R171 e: VGB PowerTech; Provision of Technical Documentation (Technical Plant Data, Documents) for Power Plants.

[6] VGB B 103: VGB PowerTech; Designation codes for document kind classification code (DCC key)

[7] IEC 61355: IEC; Standard for the classification and designation of documents for plants, systems and equipment.

2.2.2 Informative

Not applicable.

2.3 DEFINITIONS

The terms and definitions provided in **Part 1: General (240-132042241)** of this multipart document applies throughout this document.

2.4 ABBREVIATIONS

The abbreviations provided in **Part 1: General (240-132042241)** of this multipart document applies throughout this document.

2.5 ROLES AND RESPONSIBILITIES

Group Technology, C&I Design application is responsible for implementing this document. Group Technology, C&I Governance is accountable for ensuring conformance to this document.

2.6 PROCESS FOR MONITORING

The SCOT PP C&I SC shall monitor the effectiveness and implementation of this document. The SCOT C&I PP SC shall also maintain this document in accordance with the SCOT document procedures.

2.7 RELATED/SUPPORTING DOCUMENTS

Not applicable.

3. CONFORMANCE TO THIS DOCUMENT

The provisions of this document are individually specified and identified with unique clause numbers. To conform to this document, it shall be shown that each of the requirements, capabilities and possibilities in clause 4 has been be satisfied.

In some instances, additional information is provided to either explain the reasoning behind a clause or to aid with the understanding of a clause. This information is informative only; does not form part of the requirements of this document and is always identified by a surrounding text box such as that in which this text is contained.

Requirements, recommendations, permissions, capabilities and possibilities are collectively referred to as provisions. As per the drafting rules applied to this document:

Requirements are mandatory and are to be strictly followed to conform to this document. Requirements are identified with the verbal forms “shall” and “shall not”.

Capabilities and possibilities refer to functions and abilities that are available to a user of this document. They are to be followed to conform to this document and are identified with the verbal forms “can” and “cannot”.

Recommendations are suggestions or technically preferred provisions and/or actions. It is not necessary for recommendations to be followed to conform to this document. Recommendations are identified with the verbal forms “should” and “should not”.

Permissions are permitted actions. It is not necessary for permissions to be followed to conform to this document. Permissions are identified with the verbal forms “may” and “need not”.

4. ENGINEERING SYSTEM REQUIREMENTS

4.1 GENERAL

The typical structure and components of a DCS's engineering system is shown in Figure 2 below.

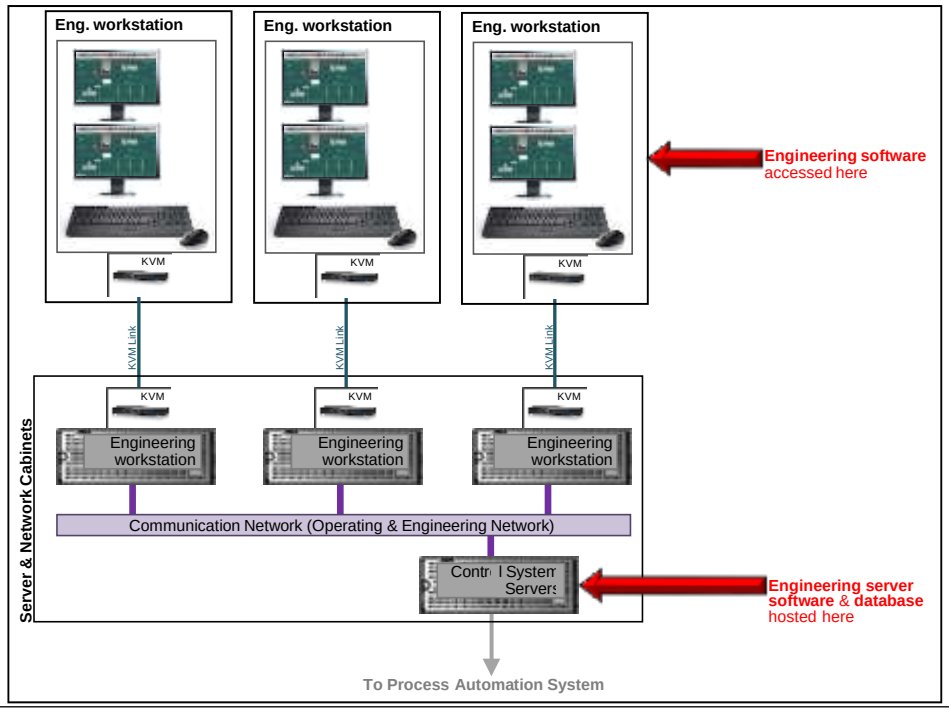

Figure 2: Typical structure of an engineering system

4.1.1 In addition to the requirements specified in this document, the engineering system shall comply with the requirements of the VGB field device visualisation design standard, VGB R 170 B5e.

4.1.2 The engineering system shall provide engineers with all information and facilities required to engineer, configure, maintain and troubleshoot the C&I system.

4.1.3 The engineering system shall consist of the following components:

a. Engineering software (refer to clause 4.3);
b. Engineering server software (refer to clause 4.4);
c. Engineering clients (refer to clause 4.5);
d. Communication networks (refer to part 5).

4.2 KEY PERFORMANCE REQUIREMENTS

4.2.1 Each control island shall contain within itself its own engineering system.

4.2.2 Engineering of each control island shall be restricted to its own engineering system. A user cannot engineer a control island from any other control island.

4.2.3 The engineering database shall be fully redundant.

The requirements for redundant equipment are specified in Part 1 of this multipart document.

4.3 ENGINEERING SOFTWARE

4.3.1 General

The scope of the engineering system is the engineering and diagnostic of the entire C&I system (including field equipment, power distribution systems, etc.) and not just the DCS. As such, the engineering system is likely to include multiple software packages, each suitable for a different aspect of engineering. Figure 3 is an overview of the designs and documentation that the engineering system is expected to produce and/or access.

Note, it is outside the scope of this document to specify the design philosophies, content, layout and format of designs and documentation. This being applicable to all control systems and not just the DCS, it is specified elsewhere.

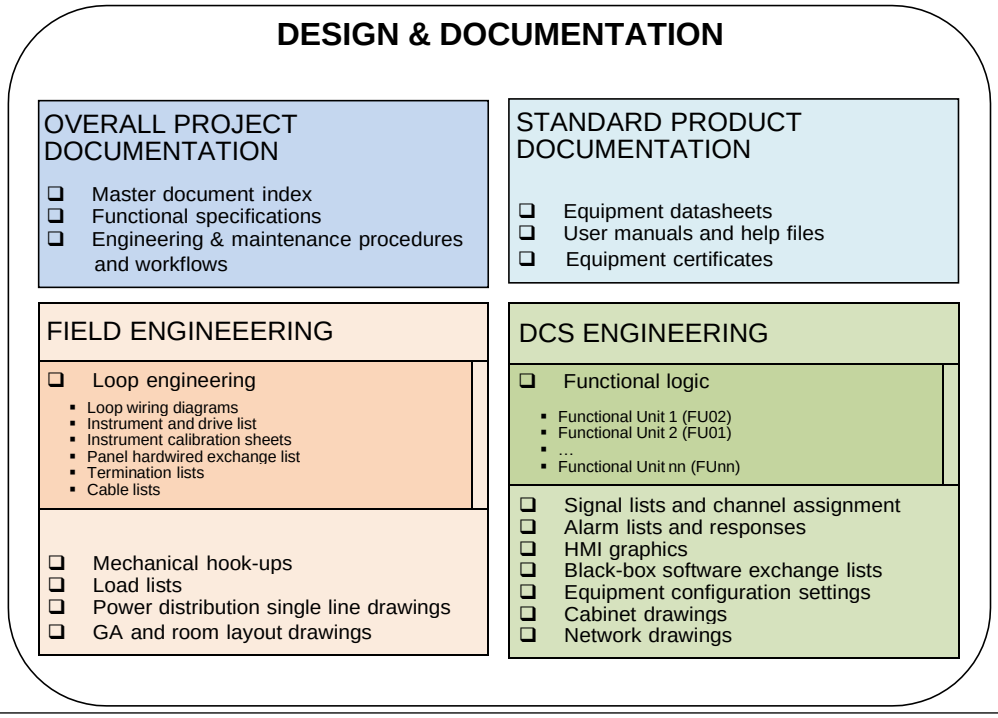

Figure 3: Overview of the design and documentation of the engineering system

4.3.1.1 The engineering software shall consist of all software packages necessary to perform the following tasks:

a. DCS engineering;
b. Network engineering;
c. Field engineering;
d. Alarm management;
e. User management;
f. Design and documentation management;

This does not necessitate that one engineering software package contains all functionalities listed above. The functionalities listed can be provided using multiple software packages, which are collectively referred to as the engineering software.

4.3.1.2 Every software package used during the design of the C&I system shall form part of the engineering software.

4.3.1.3 The engineering software shall use graphical user interfaces (GUI) and object orientated programming philosophies.

4.3.1.4 The engineering software shall ensure the full security and integrity of all control tasks and data at all times.

4.3.1.5 The engineering software can export all lists and schedule type data to Microsoft ® Excel.

4.3.1.6 A user can execute queries and run searches on the engineering databases.

4.3.2 DCS Engineering

4.3.2.1 The engineering software can produce and access the following DCS designs and documentation:

a. Application software:
   i. Functional logic;
   ii. Signal lists and channel assignment;
   iii. Alarm lists and responses;
   iv. HMI graphics;
   v. Black-box software exchange lists;
   vi. Equipment configuration settings.
b. Cabinet drawings;
c. Network drawings;

4.3.2.2 The engineering software shall be used to generate and transfer all application software and configuration changes to the applicable elements of the DCS.

4.3.2.3 Using the engineering software, a user can:

a. View, edit and print the running version of all application software;
b. View, edit and print older versions of the application software;
c. View and print the functional logic with the dynamic status of all signals shown;
d. View, edit and print the real-time configuration settings of the DCS (including I/O allocation IP addresses, cycle time, etc.);
e. View and update the firmware version of all automation system components;
f. Force signals;
g. View and print C&I system alarms and related alarm response procedures;
h. View and print detailed diagnostic information of faulty C&I equipment;
i. Graphically view and print the real-time status of the DCS and all its components, with drill down capabilities to each fault, disturbance cause.

4.3.3 Functional logic

4.3.3.1 In addition to the requirements specified in this document, the functional logic shall comply with the requirements of:

a. VGB function-related documentation guideline, VGB R 170 Ce;
b. VGB design standards for instrumentation and control equipment – Automation function, VGB R 170B2e;
c. VGB identification of instrumentation and control tasks/functions in process systems and identification of functions in instrumentation and control systems, VGB B 106B4e.

4.3.3.2 The running version of the functional logic in the controllers shall be unambiguously identified.

4.3.3.3 All functional logic is displayed and implemented through the functional diagrams including that of:

a. Closed loop control;
b. Sequence control;
c. Group control;
d. Generation of process alarms;
e. Permissives

4.3.3.4 With no more than two clicks a user can automatically navigate directly from any signal in a functional diagram to same signal in the selected destination/source functional diagrams.

4.3.3.5 The engineering software shall automatically create and manage the references for interlinks between functional diagrams. Users shall not need to manually create references.

4.3.3.6 A user can view the signal identifier and tag identifier of any signal on a functional diagram.

4.3.3.7 The engineering software libraries shall contain standard function blocks for:

a. Analogue drive control (4-20mA output signal);
b. Binary drive control (pulsed (inching) output);
c. Measurement voting (2oo3, 1oo2, etc…);
d. Group control, sub-group control and automatic changeover;
e. Sequence control.

4.3.4 Network engineering

4.3.4.1 The engineering software shall contain network management functions for the management of the communication network.

4.3.4.2 Using the network management functions of the engineering software a user can:

a. View, edit and print the network topology with and without the dynamic status of network and computer equipment shown;
b. View, edit and print the real-time configuration settings of network equipment;
c. View and update the firmware version of all network equipment;
d. View and print alarms and detailed diagnostic information of network equipment;
e. View and analyse the network performance using trends, graphs and summary charts;
f. View and print network traffic statistics (latency, jitter, throughput, errors, and dropped packets).

4.3.4.3 The engineering software shall automatically detect changes to the network, including new network devices added to the network.

4.3.5 Field engineering

4.3.5.1 The engineering software can produce and access the following field engineering designs and documentation:

a. Loop engineering:
   i. Loop wiring diagrams;
   ii. Instrument and drive list;
   iii. Instrument calibration sheets;
   iv. Panel hardwired exchange list;
   v. Termination lists;
   vi. Cable lists;

b. Mechanical hook-ups;
c. Load lists;
d. Power distribution single line drawings;
e. GA and room layout drawings.

4.3.6 Loop engineering

Loop engineering refers to the design and configuration of field equipment electrical loops (with the loop being the circuit between the device itself and the automation system). It overlaps with aspects of both field engineering (loop wiring diagrams, instrument lists, etc.) and DCS engineering (channel assignment, signal lists). It excludes aspects of field engineering not related to the electrical loop design, for example the mechanical hook-ups, junction box GA, etc.

4.3.6.1 All loop engineering designs and documentation shall be intelligently linked to each other such that a user can navigate from an equipment object on one design to other related designs and documentation.

Example 1: A user should be able to navigate from the loop drawing of transmitter 10LAC00CP001 to the junction box termination schedule in which 10LAC00CP001 is terminated by clicking on the junction box object in the 10LAC00CP001 loop drawing and using the right click context menu.

4.3.6.2 Product documentation for field devices shall be intelligently linked to the loop engineering design and documentation such that a user can navigate from an equipment object on the loop engineering design and documentation to the applicable standard product documentation.

Example 1: A user should be able to navigate from the loop drawing of transmitter 10LAC00CP001 to the transmitter's datasheet by clicking on the transmitter object in the 10LAC00CP001 loop drawing and using the right click context menu.

4.3.6.3 The loop engineering design and documentation produced by all engineering software packages shall be synchronised with no manual manipulation of the data. The synchronisation process shall be highly automated and shall perform automated data consistency checks.

The above clause is necessitated by the C&I suppliers' practice of using different software packages for field engineering and for DCS engineering. The channel assignment is commonly done in the DCS engineering software, whereas the loop drawing is usually done using a separate field engineering software package. Therefore to ensure consistency of designs produced, some form of integration, synchronisation and consistency checks is required between the designs produced by the different software packages.

4.3.7 Alarm management

4.3.7.1 The engineering software shall contain alarm analysis and management functions to:

a. Automatically generate daily alarm performance reports (as per the alarm key performance indicators);
b. Create and edit alarm responses;
c. Calculate the frequency of individual alarms;
d. Identify and find standing alarms and nuisance alarms (chattering, stale, frequent and fleeting);
e. Report the number of times an alarm has occurred in a given period of time.

4.3.8 User management

4.3.8.1 The engineering software shall contain user management functions to manage all users, user rights and user authentication.

4.3.8.2 A user can use a single username and password to access all software packages of the applicable control island.

4.3.8.3 The user management functions shall enable the system administrator to:

a. Define users, user roles and groups;
b. Manage and configure user rights across all software packages, servers, workstations and directories.
c. Monitor all permissible and active connections;
d. Define allowable password formats;
e. Define time periods for which user passwords remain valid.

4.3.8.4 As a minimum, the following user roles shall be defined:

a. Administrator;
b. Engineer;
c. Commissioning Engineer;
d. Safety Engineer;
e. Maintenance;
f. Supervisor;
g. Operator.

4.3.9 Design and documentation management

4.3.9.1 In addition to the requirements specified in this document, the management, breakdown structure and numbering of design and documentation in the engineering system shall comply with the requirements of:

a. VGB provision of technical documentation for Power Plants, VGB R171 e;
b. VGB designation codes for DCC, VGB B 103;
c. IEC standard for the classification and designation of documents for plants, systems and equipment, IEC 61355.

4.3.9.2 The engineering software can produce and access the following overall project documentation:

a. Master document index;
b. Functional specifications;
c. Engineering & maintenance procedures and workflows.

4.3.9.3 A user can navigate directly from the master document index to the selected design and documentation.

4.3.9.4 The engineering software can access the following standard product documentation:

a. Equipment datasheets;
b. User manuals and help files;
c. Equipment certificates.

4.3.9.5 The engineering software shall contain master templates for each type of documentation produced.

4.3.9.6 The designs and documentation shall be logically structured according to the plant breakdown structure, functional unit definitions and tag identifiers.

4.3.9.7 Designs and documentation shall be produced using defined workflows.

4.3.9.8 The workflows to produce designs and documentation shall be embedded in the engineering system.

4.3.9.9 Workflows should be automated to the extent possible.

4.3.10 Access Control

4.3.10.1 Access to the engineering software shall be password protected.

4.3.10.2 A C&I system's engineering database shall not be accessible from outside the C&I system concerned except as allowed by the relevant cybersecurity standards and policies.

4.3.10.3 All designs and documentation stored in the engineering database shall be accessible through the engineering software.

4.3.10.4 A user can access all designs and documentation in its native/original form.

4.4 ENGINEERING SERVER SOFTWARE

4.4.1 The engineering server software shall be hosted on control system servers as specified in Part 5 of this multipart document.

4.4.2 Storage and revision control

4.4.3 The engineering database shall contain all designs and documentation of the control island's C&I system, including the following:

a. DCS engineering designs and documentation as listed in clause 4.3.2.1;
b. Field engineering designs and documentation as listed in clause 4.3.5.1;
c. Project documentation as listed in clause 4.3.9.1;
d. Standard product documentation as listed in clause 4.3.9.3;

4.4.3.1 The engineering database shall store older revisions of designs and documentation in its native/original form.

4.4.3.2 Each revision of the stored designs and documentation shall be clearly and uniquely identified.

4.5 ENGINEERING CLIENT

Only the functional requirements of the engineering clients are provided here. Each power plant may have a different engineering clients configuration and room location dependent on its requirements. As such, requirements related to the engineering client configuration, quantities and locations have not been specified in this document and should be defined elsewhere.

4.5.1 The engineering client shall consist of the following:

a. Engineering screens;
b. Workstation computer;
c. KVM modules;
d. Keyboard & mouse.

4.5.2 The engineering clients shall allow for the secure extraction of data through removable media.

The requirements for the engineering client equipment (computers, screens etc.) are specified in Part 5: Network and Computer equipment.

4.6 MODIFICATIONS AND CHANGES

4.6.1 Configuration and application software changes shall be automatically pre-tested by the engineering software before the transfer of the changes is allowed to the applicable elements of the DCS.

4.6.2 Any changes made to the engineering databases shall be made in real-time and on-load.

4.6.3 Changes shall be made to the operator system and engineering system without requiring the simultaneous shutdown and/or restart of redundant equipment.

4.6.4 Changes shall be made to the functional logic without requiring the simultaneous shutdown and/or restart of both controllers in a redundant pair.

4.6.5 Changes shall be made to the application software without disrupting the unrelated portions of the HMI.

4.6.6 Tuning constants are parameterised and can be altered without restarting any controller.

5. AUTHORISATION

This document has been seen and accepted by:

Name	Designation
	Senior Manager, EC&I
	Senior Manager, Electrical and C&I PEI (Acting)
	Chairperson, Power Plant C&I SC
	Middle Manager, C&I Design Application
	Chief Technologist, PEIC C&I

6. REVISIONS

Date	Rev.	Compiler	Remarks
November 2016	0.1		Draft of this document circulated for first round of comments.
November 2016	0.2		Intermediate update of document after some comments received back.
November 2017 – October 2018	0.3 – 0.5		Main changes made: • Updated the document with comments received.
November 2018	0.6		Main changes made: • Revised, reformatted, updated with comments. • Added document number.
January 2019	1		Final Document for Authorisation and Publication

7. DEVELOPMENT TEAM

The following people were involved in the development of this document:

a. [redacted]

8. ACKNOWLEDGEMENTS

The following people provided valuable insight and comments during the review of this document:

a. [redacted]
b.
c.
d.