	<b>Standard</b>	<b>Technology</b>
---	-----------------	-------------------

Title: **Power Plant Controls & Instrumentation; Control Systems; Distributed Control Systems (DCS); Part 2: Operator & Supervisor System Standard**

Unique Identifier: **240-132042275**

Alternative Reference Number: **N/A**

Area of Applicability: **Engineering**

Documentation Type: **Standard**

Revision: **1**

Total Pages: **19**

Next Review Date: **January 2024**

Disclosure Classification: **CONTROLLED DISCLOSURE**



Compiled by	Approved by	Authorised by
..... <b>Chief Engineer, C&amp;I Plant</b>	..... <b>Middle Manager, C&amp;I Plant (Acting)</b>	..... <b>Senior Manager, EC&amp;I</b>
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
<b>1. INTRODUCTION</b> .....	<b>3</b>
<b>2. SUPPORTING CLAUSES</b> .....	<b>5</b>
2.1 SCOPE .....	5
2.2 NORMATIVE/INFORMATIVE REFERENCES .....	5
2.3 DEFINITIONS .....	6
2.4 ABBREVIATIONS.....	6
2.5 ROLES AND RESPONSIBILITIES.....	6
2.6 PROCESS FOR MONITORING .....	6
2.7 RELATED/SUPPORTING DOCUMENTS.....	6
<b>3. CONFORMANCE TO THIS DOCUMENT</b> .....	<b>7</b>
<b>4. OPERATOR SYSTEM REQUIREMENTS</b> .....	<b>8</b>
4.1 GENERAL .....	8
4.2 KEY PERFORMANCE REQUIREMENTS .....	8
4.3 OPERATOR SOFTWARE .....	9
4.4 OPERATOR CLIENT.....	14
4.5 ESSENTIAL MEASUREMENT PANEL.....	14
4.6 EMERGENCY PUSH BUTTONS .....	15
4.7 ALARM SIREN .....	15
4.8 OPERATOR SERVER SOFTWARE .....	16
<b>5. SUPERVISOR SYSTEM REQUIREMENTS</b> .....	<b>17</b>
5.1 GENERAL .....	17
5.2 KEY PERFORMANCE REQUIREMENTS .....	17
5.3 SUPERVISOR SOFTWARE .....	17
5.4 SUPERVISOR CLIENTS.....	17
<b>6. AUTHORISATION</b> .....	<b>19</b>
<b>7. REVISIONS</b> .....	<b>19</b>
<b>8. DEVELOPMENT TEAM</b> .....	<b>19</b>
<b>9. ACKNOWLEDGEMENTS</b> .....	<b>19</b>

## FIGURES

Figure 1: Overall framework of this multipart document.....	4
---	---

## TABLES

Table 1: Overall framework of this multipart document.....	3
Table 2: Functionality requirements per faceplate type.....	11

### CONTROLLED DISCLOSURE

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

## 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 2: Operator & Supervisor 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**

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

### **CONTROLLED DISCLOSURE**

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

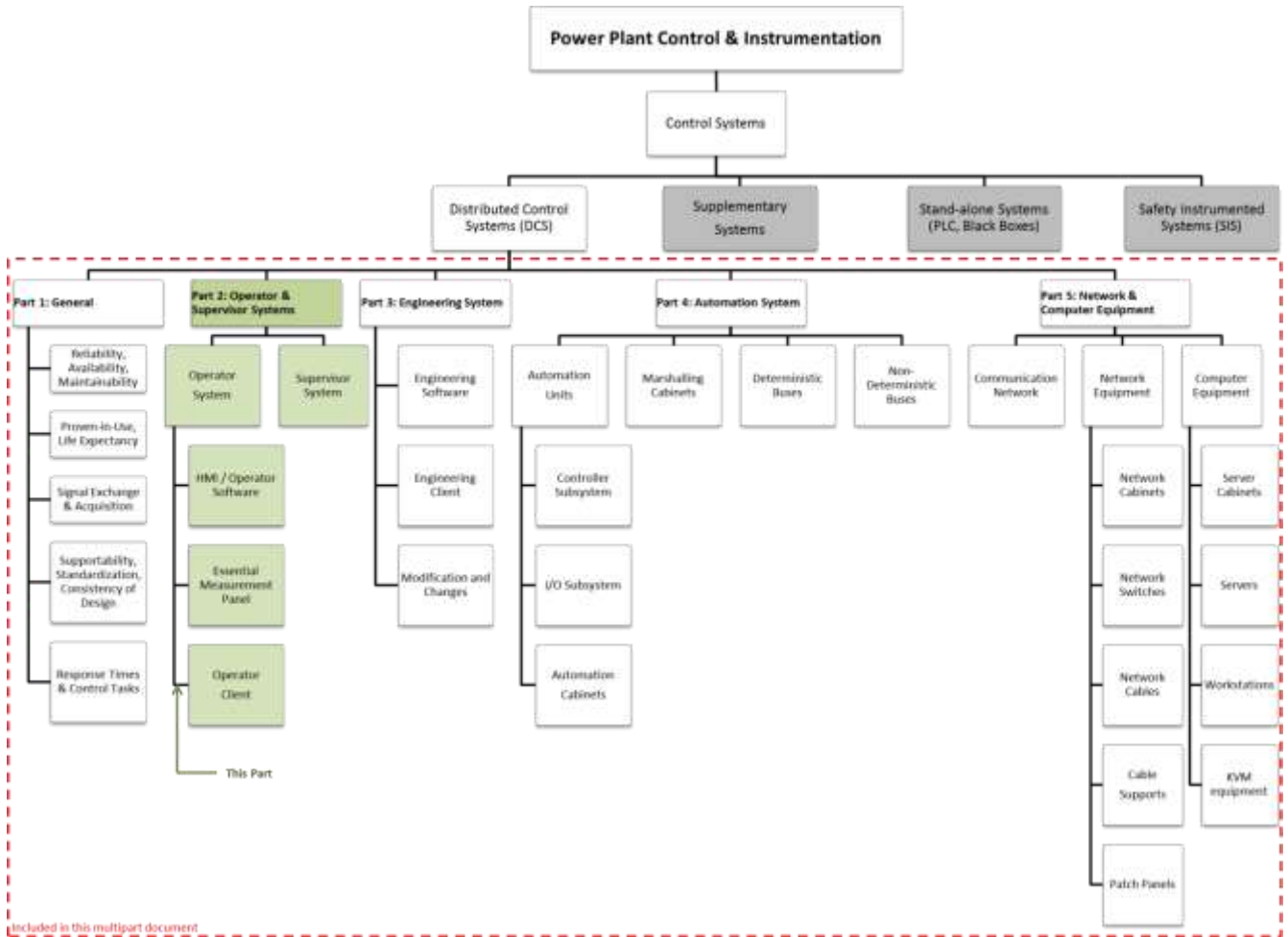


Figure 1: Overall framework of this multipart document

**CONTROLLED DISCLOSURE**

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

## **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 2: Operator & Supervisor system**; the scope of which is the specification of the operator and supervisor systems.

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 R170 B3e: VGB PowerTech; Design standards for instrumentation and control equipment: Operation and Monitoring.
- [2] 240-56355728: Eskom; HMI design requirements standard.
- [3] 240-56355466: Eskom; Alarm management system guideline.
- [4] IEC 62682: IEC; Management of alarm systems for the process industries.
- [5] 240-105453648: Eskom; Fossil fuel firing regulation.
- [6] 240-132042241: Power Plant Controls & Instrumentation; Control Systems; Distributed Control Systems (DCS); Part 1: General.

### **2.2.2 Informative**

Not applicable.

**CONTROLLED DISCLOSURE**

## **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.

### **CONTROLLED DISCLOSURE**

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

### **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 clauses 4 and 5 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”.

#### **CONTROLLED DISCLOSURE**

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

## **4. OPERATOR SYSTEM REQUIREMENTS**

### **4.1 GENERAL**

- 4.1.1** In addition to the requirements specified in this document, the operator system shall comply with the requirements of the VGB operation and monitoring design standard, VGB R 170 B3e.
- 4.1.2** The operator system(s) shall provide plant operators with all information, protection, and control facilities required to operate the plant safely, reliably and consistently.
- 4.1.3** The operator system should provide a plant operator with an integrated and standardised set of displays and facilities which are designed to conform to ergonomic principles and modern power plant practices.
- 4.1.4** The operator system shall consist of the following components:
- Operator software (refer to clause 4.3);
  - Operator clients (refer to clause 4.4);
  - Essential measurement panel (refer to clause 4.5);
  - Emergency push buttons (refer to clause 4.6);
  - Alarm sirens (refer to clause 4.7);
  - Operator server software (refer to clause 4.8);
  - Communication networks (refer to Part 5).

### **4.2 KEY PERFORMANCE REQUIREMENTS**

- 4.2.1** Each control island shall contain within itself its own operator system.
- 4.2.2** A user cannot operate across control islands. A user can only operate a control island from the operator system of that control island.
- 4.2.3** A single failure in the DCS shall not cause the failure of more than one operator client.
- 4.2.4** The operator database shall be fully redundant.

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

- 4.2.5** In the event of failure of any small or large screen, the operator client shall remain fully functional.

To achieve this requirement there should be no 'main screen' (this being the only screen with the main menu and/or navigation functions), or if there is a 'main screen', the 'main screen' should be automatically reconfigured on another screen when the screen displaying the 'main screen' fails.

- 4.2.6** The operator client shall be configured such that it can be maintained while on-load.
- 4.2.7** The response times of the operator system shall be as follows:
- The maximum time taken to completely populate a HMI graphic page or faceplate with dynamic data shall not exceed 1.5 seconds.
  - The average time taken to completely populate any HMI graphic page or faceplate with dynamic data shall be less than 0.5 seconds.
  - The maximum time taken to completely populate a trend with dynamic data shall not exceed 3 seconds.
  - The average time taken to completely populate any trend with dynamic data shall be less than 1.5 seconds.

### **CONTROLLED DISCLOSURE**



## **4.3 OPERATOR SOFTWARE**

### **4.3.1 General**

4.3.1.1 In addition to the requirements specified in this document, the operator software shall comply with the requirements of the Eskom HMI design requirements standard, 240-56355728.

4.3.1.2 A fully functional HMI shall be provided. The HMI shall provide the following functionality:

- a. HMI graphic pages for plant schematics with dynamic indication of the plant statuses and values;
- b. HMI graphic pages for system schematics with dynamic indication of DCS equipment status and values;
- c. Faceplates;
- d. Alarm handling;
- e. Process alarm list;
- f. System alarm list;
- g. Trends;
- h. Plant performance information;
- i. Event lists;
- j. Dynamic indication of forced signals;
- k. Viewing of the historical process data stored in the operator database;
- l. Viewing of the dynamic state of the functional logic in the automation system;
- m. Access to the plant information system (PIS);
- n. Access to operating procedures and alarm response procedures;
- o. Short term historian;
- p. Characteristic curves and deviation curves.

4.3.1.3 Individual users can configure, save and restore the arrangement of the HMI graphic pages on the operator clients.

### **4.3.2 Navigation**

4.3.2.1 Selection of any HMI graphic shall not require more than two mouse clicks.

To facilitate easy navigation, a hierarchical structure should be implemented for the HMI graphics, with overview diagrams, area level diagrams and individual level diagrams. From the overview diagram(s) no more than two mouse clicks should be required to navigate to any HMI graphic page.

4.3.2.2 In alarm or abnormal conditions, not more than one mouse click shall be required to access the relevant HMI graphic.

To achieve this, a user should be able to navigate directly from the alarm on the alarm list to the applicable HMI graphic.

4.3.2.3 The user can navigate directly from a HMI graphic page; alarm list and event list to a dynamic view of the related the functional logic.

4.3.2.4 The user can navigate directly from a HMI graphic page to the related alarm response procedure.

4.3.2.5 The user can navigate directly from an alarm on the alarm list to the related alarm response procedure.

4.3.2.6 The user can navigate directly from an alarm on the alarm list to the related HMI graphic page in which the equipment in alarm condition in shown.

## **CONTROLLED DISCLOSURE**

4.3.2.7 Operating procedures shall be directly accessible through the HMI.

### **4.3.3 Printing**

4.3.3.1 All information available on the HMI system can be printed directly without the use of any third party software.

### **4.3.4 Trends**

4.3.4.1 A user should be able to fully colour the area under a line graph, such that the deviation from a set point is more clearly visible.

4.3.4.2 In addition to the standard trending functionality, pre-configured trends shall be provided on the HMI.

### **4.3.5 Event List**

4.3.5.1 On the event list, a user can view both dynamic and historical events from the short term historian.

4.3.5.2 The event list shall display the following types of events:

- a. All operator actions;
- b. All alarms;
- c. All state changes of field devices;
- d. All state changes of signals acquired from black-boxes;
- e. All thresholds configured on analog inputs signals;
- f. All state changes of output signals;
- g. Fault status of C&I equipment.

4.3.5.3 The following information shall be displayed for each event on the event list:

- a. Tag identifier
- b. Signal identifier;
- c. Tag description;
- d. Functional unit;
- e. Alarm priority (if the event is an alarm);
- f. Time stamp (when the state change occurred);
- g. Event state;
- h. Alarm type (if the event is an alarm);
- i. Alarm set point (if the event is an alarm).

4.3.5.4 The event list can be sorted (ascending and descending) and filtered on all of the fields defined in 4.3.5.1.

4.3.5.5 The event list can be exported to Microsoft ® Excel.

### **4.3.6 Faceplates**

4.3.6.1 Faceplates shall be provided for the following:

- a. Sequence control;
- b. Analogue drives;
- c. Binary drives;
- d. Instruments;

## **CONTROLLED DISCLOSURE**

- e. Closed loop control;
- f. Group control;
- g. Actuators.

4.3.6.2 The functionality provided for each faceplate type shall be that shown in Table 2.

4.3.6.3 The status of all permissives and criteria shall be displayed dynamically.

<b>Table 2: Functionality requirements per faceplate type</b>									
No.	Information Required	Faceplate Type							
		Seq. Control	Analog Drive	Binary Drive	Instr.	Closed loop control	Group Control	Binary Actuator	Analog Actuator
	<b>General</b>								
A	Tag identifier (e.g. KKS, AKZ)	X	X	X	X	X	X	X	X
B	Tag Description	X	X	X	X	X	X	X	X
	<b>Commands</b>								
C	Auto/Manual	X	X	X		X	X	X	X
D	On/Off, Open/Close, Start/Stop	X		X			X	X	
E	Raise/Lower		X			X			X
F	Manual set point		X			X			X
	<b>Indications</b>								
G	Engineering Units		X		X	X			X
H	Auto/Manual Indication	X	X	X		X	X	X	X
I	On/Off, Open/Close, Start/Stop	X	X	X			X	X	X
J	Trip/Fault/Abnormal	X	X	X	X	X	X	X	X
K	Local/Remote/Maintenance		X	X				X	X
L	Permissives/Criteria	X	X	X		X	X	X	X
M	Step number & timers	X							
N	Set point and deviation		X			X			X
O	Position feedback		X			X			X
P	Current		X	X					X
Q	Torque faults							X	
R	Busy moving							X	

### 4.3.7 Alarm Handling

4.3.7.1 In addition to the requirements specified in this document, alarm handling shall comply with the requirements of the Eskom alarm management system guideline, 240-56355466.

4.3.7.2 In addition to the requirements specified in this document, alarm handling shall comply with the requirements of the IEC management of alarm systems for the process industries, IEC 62682.

4.3.7.3 All process alarms shall be generated within the functional logic. No process alarms shall be generated within the software contained in the operator system.

4.3.7.4 Each of the following fields of a system alarm can be configured:

- a. Tag identifier;
- b. Signal identifier;
- c. Tag description;
- d. Functional unit;

### CONTROLLED DISCLOSURE

e. Alarm priority (with both colour and alphanumeric);

4.3.7.5 Alarms shall be dynamically presented to the operator with information matched to the current situation and its criticality.

4.3.7.6 The HMI shall clearly distinguish between different alarm types and alarm priorities.

4.3.7.7 Users can search for nuisance alarms (chattering, stale, frequent and fleeting).

4.3.7.8 Users can access alarm response procedures for all alarm types and categories including those related to system alarms.

#### **4.3.8 Alarm Lists**

4.3.8.1 On the process alarm list, a user can view all active process alarms.

4.3.8.2 On the system alarm list, a user can view all active system alarms.

4.3.8.3 The following information shall be displayed as a summary for each alarm list at the top of that alarm list:

- a. The total number of unacknowledged alarms in the alarm list;
- b. The total number of alarms in the alarm list per functional unit.

4.3.8.4 The following information shall be displayed for each alarm on the alarm list:

- a. Tag identifier;
- b. Signal identifier;
- c. Tag description;
- d. Functional unit;
- e. Alarm priority (with both colour and alphanumeric);
- f. Time stamp (when the alarm became active);
- g. Alarm state (acknowledged alarm, unacknowledged alarm and returned unacknowledged alarm);
- h. Alarm type;
- i. Alarm set point.

4.3.8.5 The alarm list can be sorted (ascending and descending) and filtered on all of the fields defined in 4.3.8.4

4.3.8.6 New alarms shall always be visible and shall appear at either the top or bottom of the alarm list.

#### **4.3.9 Forcing**

4.3.9.1 The HMI graphic pages shall provide visual indication when a signal is forced or disturbed.

A forced signal is one for which the actual signal value (from the measurement device) is replaced or substituted with a user defined value, i.e. it is a simulation. A disturbed signal is one which is in fault (for example out of range, line break, short circuit, etc.).

4.3.9.2 On the forced signal list, a user can view the forced signals that are active at the time.

4.3.9.3 The forced signal list may be contained within the operator system or the engineering system.

If the forced signal list is contained in the operator system, the user can access it via the HMI. If the forced signal list is contained within the engineering system the user can access it via the engineering client.

4.3.9.4 The following information shall be displayed for each forced signal on the forced signal list:

- a. Tag identifier

### **CONTROLLED DISCLOSURE**

- b. Signal identifier;
- c. Tag description;
- d. Functional unit;
- e. Time stamp (when the signal was forced);
- f. Actual value of the signal;
- g. Forced value of the signal;
- h. User that forced the signal.

#### **4.3.10 DCS equipment status**

4.3.10.1 HMI graphic pages shall be provided to dynamically display the state of the DCS. The following DCS equipment shall be dynamically displayed:

- a. All workstations;
- b. All control system servers;
- c. All network switches;
- d. All automation units.

This requires HMI graphic pages (similar to the plant mimics) to be created for the plant operators such that they have a visual and dynamic indication of the status of the DCS.

4.3.10.2 On the HMI graphic pages, the following information shall be displayed for the DCS equipment identified in 4.3.10.1:

- a. Tag identifier
- b. Tag description;
- c. Equipment overall health (Fault / No fault).

#### **4.3.11 Access Control**

4.3.11.1 No passwords or access control of any form is required for view-only access to the plant status.

4.3.11.2 A multilevel password system shall be used to restrict the operating functionality to authorised personnel only.

4.3.11.3 The log in and log out functionality shall be seamless without requiring the shutdown or restarting of the operator system.

#### **4.3.12 Short term historian**

4.3.12.1 The short term historian shall be the short term repository of the applicable control island's DCS.

4.3.12.2 The following shall be logged and stored in the short term historian:

- a. All event types as described in 4.3.5.2;
- b. All process alarms;
- c. All system alarms;
- d. All analog input and output signals.

4.3.12.3 For alarms and events, all state changes shall be logged.

This includes the return to normal (inactive) state, and acknowledgment of alarms by operators.

4.3.12.4 The short term historian shall store records from the last 90 days.

Beyond the 90 day window, alarm and event records are accessed from the long term historian (plant information system).

### **CONTROLLED DISCLOSURE**

#### **4.4 OPERATOR CLIENT**

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

**4.4.1** Each control island's operator clients shall be configured such that:

- a. It allows for a single plant operator to operate the entire control island under normal operating conditions.
- b. It allows two independent operations to be undertaken concurrently by the plant operator and an assisting operator.

**4.4.2** The operator client shall not lockup (freeze or crash) under any circumstance.

**4.4.3** The operator client shall consist of the following:

- a. Small screens;
- b. Large screens;
- c. Workstation computer;
- d. KVM modules;
- e. Keyboard & mouse.

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

#### **4.5 ESSENTIAL MEASUREMENT PANEL**

It is a requirement of the Eskom Fossil Fuel Firing Regulations Standard, 240-105453648 that in the event of the complete failure of the operator client, essential instrumentation is still displayed to the plant operator. This functionality is provided by an essential measurement panel, the required specifications of which are defined in this section.

Only the functional requirements of the essential measurement panel are provided here. Each power plant will have a different set of essential instrumentation. As such, the list of essential instrumentation required to be displayed on the essential measurement panel has not been specified in this document and should be specified elsewhere.

**4.5.1** In addition to the requirements specified in this document, the essential measurement panel shall comply with the requirements of the Eskom Fossil Fuel Firing Regulations, 240-105453648.

**4.5.2** The essential measurement panel shall be located at the operator desk.

The panel should be integrated in the operator desk along with the operator clients and emergency push buttons so that together they represent one operator interface.

**4.5.3** The essential measurement panel shall consist of the following:

- a. Binary indications;
- b. Analogue indications.

The Eskom fossil fuel firing regulation, 240-105453648 defines the minimum measurements that should be on the essential measurement panel.

**4.5.4** The essential measurement panel shall be fully independent of the operator clients and control system servers.

#### **CONTROLLED DISCLOSURE**

The intent behind this is that on DCS failures of the operator client or control system servers the essential measurement panel is still operational and provides the operator with visual indication of the unit status.

**4.5.5** The binary and analogue indications of the essential measurement panel may be hardwired to the automation system.

**4.5.6** The essential measurement panel may be implemented via a black-box or standalone system.

If, at the power station concerned, there is a black-box with its own operator client on the operator desk, e.g. a Turbine protection system then this black-box (being independent of the DCS) may be used to display the essential measurements to the operator in the event of a DCS failure.

**4.5.7** Analogue indications shall be dynamically presented.

**4.5.8** Binary indications shall be dynamically presented with information matched to the current situation and shall clearly distinguish between different alarm priorities.

## **4.6 EMERGENCY PUSH BUTTONS**

Only the functional requirements of the emergency push buttons are provided here. Each control island will require different emergency push buttons. As such, the emergency push buttons required have not been specified in this document and should be defined elsewhere.

**4.6.1** The emergency push buttons shall be located at the operator desk.

**4.6.2** The emergency push button shall be fitted with transparent covers to prevent accidental activation.

**4.6.3** The emergency push buttons shall be mushroom-shaped buttons which latch in after activation and thereafter can only be released by a deliberate action.

**4.6.4** The emergency push buttons shall be certified as suitable for use in safety applications.

**4.6.5** Each emergency push buttons shall be hardwired as a 2oo3 voting circuit to the application automation system.

## **4.7 ALARM SIREN**

**4.7.1** The alarm siren shall be located at the operator desk.

**4.7.2** The alarm siren shall be dual redundant.

The alarm siren redundancy should be configured in a master slave configuration such that when the master fails, the slave takes over.

Both sirens should not sound simultaneously.

Each alarm siren in the redundant set should be driven from a different source (output card).

**4.7.3** The alarm siren shall provide an audible indication to the plant operator of unacknowledged and active level 1 and level 2 process alarms.

**4.7.4** The alarm siren audible tones shall be fully configurable.

Where multiple operator systems are located in the same control room, the alarm siren tones of each system should be such that an operator can easily distinguish the source (from which operator system the alarm originated).

## **CONTROLLED DISCLOSURE**

**4.7.5** The alarm siren shall be configured such that the plant operator cannot globally disable it either physically or via the operator software.

**4.7.6** The alarm siren shall be silenced with an acknowledge action by the operator.

#### **4.8 OPERATOR SERVER SOFTWARE**

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

**4.8.2** The operator database shall contain all configuration information of the control island.

**4.8.3** All operator information, process data, signals, alarms, logs and calculated values shall be retained in the short term historian.

#### **CONTROLLED DISCLOSURE**

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.



## **5. SUPERVISOR SYSTEM REQUIREMENTS**

### **5.1 GENERAL**

**5.1.1** In addition to the requirements specified in this document, the supervisor software shall comply with the requirements of the Eskom HMI design requirements standard, 240-56355728.

**5.1.2** The supervisor system shall provide plant supervisors with all information facilities required to monitor the power plant.

**5.1.3** The supervisor system shall consist of the following components:

- a. Supervisor software;
- b. Supervisor clients.

### **5.2 KEY PERFORMANCE REQUIREMENTS**

**5.2.1** Each supervisor client can simultaneously monitor at least two control islands.

**5.2.2** The supervisor clients shall be configured to prevent operation.

### **5.3 SUPERVISOR SOFTWARE**

**5.3.1** The supervisor HMI shall not be limited to a single control island but can monitor any control islands.

**5.3.2** The supervisor HMI shall be a replica of the operator software defined in clause 4.3 but for the following:

- a. The supervisor HMI shall be limited to monitoring (view-only).

**5.3.3** The response times of the supervisor system shall be as follows:

- a. The maximum time taken to completely populate a HMI graphic or trend with dynamic data shall not exceed 5 seconds.
- b. The average time taken to completely populate any HMI graphic or trend with dynamic data shall be less than 2 second.
- c. The maximum time taken for any HMI graphic to update with any change in a process value shall not exceed 1 second.
- d. The maximum time taken to log into a control island shall not exceed 20 seconds.

### **5.4 SUPERVISOR CLIENTS**

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

**5.4.1** The supervisor client shall consist of the following:

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

### **CONTROLLED DISCLOSURE**

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

**CONTROLLED DISCLOSURE**

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

## 6. AUTHORISATION

This document has been seen and accepted by:

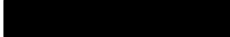
Name	Designation
	Senior Manager, EC&I
	Senior Manager, Electrical and C&I PEI (Acting)
	Chairperson, Power Plant C&I SC
	Middle Manager, C&I Design Application
	Chief Technologist, PEIC C&I

## 7. 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: <ul style="list-style-type: none"><li>• Updated the document with comments received.</li></ul>
November 2018	0.6		Main changes made: <ul style="list-style-type: none"><li>• Revised, reformatted, updated with comments.</li><li>• Added document number.</li></ul>
January 2019	1		Final Document for Authorisation and Publication

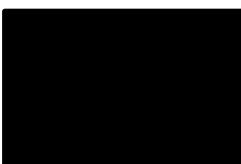
## 8. DEVELOPMENT TEAM

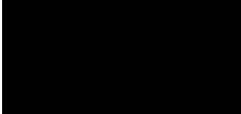
The following people were involved in the development of this document:

a. 

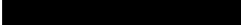
## 9. ACKNOWLEDGEMENTS

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

a. 

b. 

c. 

d. 

**CONTROLLED DISCLOSURE**

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.