Eskom	Standard	Technology

Title: **Essential HMI and Instrumentation Systems for Power Plants Standard**

Unique Identifier:	**240-124465468**
Alternative Reference Number:	**N/A**
Area of Applicability:	**Engineering**
Documentation Type:	**Standard**
Revision:	**1**
Total Pages:	**15**
Next Review Date:	**April 2023**
Disclosure Classification:	**CONTROLLED DISCLOSURE**

Compiled by	Approved by	Authorised by
……..	……..	……..
Chief Engineer C&I Governance	**Acting Middle Manager C&I Governance**	**Senior Manager EC&I**
Date: ……	Date: ……	Date: ……

Supported by SCOT/SC/TC

……..

SCOT/SC/TC Chairperson

Date: ……

PCM Reference : **240-56355828**

SCOT Study Committee Number/Name : **Power Plant C&I Study Committee, PP C&I SC08-03**

CONTENTS

FIGURES

TABLES

EXECUTIVE SUMMARY

The FFFR has a requirement for an essential instrumentation display, which in the event of a control system HMI failure, should provide a display of essential plant parameters for informed Plant Operator decision making. Common Cause and Common Mode failures can cause loss of the HMI, therefore the essential instrumentation display provides a mechanism through which redundancy, and physical separation is achieved. This document presents principles to be considered during the design of the essential display.

1. INTRODUCTION

The intent of this document is to provide design guidance in meeting the FFFR requirement [FFFR, 3.1.12] for essential instrumentation. The aim of this requirement is to provide plant status information to mitigate against loss of HMI systems for Unit Control, and to ensure that the plant operator has sufficient information regarding unit statuses in the event of HMI failure.

Failure of HMI systems during plant operation is a common event, although design aspects relating to HMI network redundancy, diversified power supply concepts and distribution of control functions are implemented within DCS control systems, HMI failure does occur on occasion. It is for this reason that an essential instrumentation display is necessary to mitigate failure.

2. SUPPORTING CLAUSES

2.1 SCOPE

The scope of this document focuses on requirements for designing and implementing essential instrumentation mimics. The document focuses on the design aspects of the essential instrumentation displays; it's logical and functional requirements, and principles of redundancy and diversity to mitigate failure and loss of HMI systems.

2.1.1 Purpose

It is the purpose of this document to address the FFFR requirement [FFFR, 3.1.12] for essential instruments displays of coal fired power plants.

2.1.2 Applicability

This document is applicable to Coal Fired Power Plants within Generation only.

2.2 NORMATIVE/INFORMATIVE REFERENCES

2.2.1 Normative

[1] ISO 9001 Quality Management Systems.

[2] 240-105453648 Fossil Fuel Firing Regulations Standard.

[3] 240-119638133 Control Systems Design for Redundancy and Diversity Standard.

2.2.2 Informative

None.

2.3 DEFINITIONS

Definition	Description
Common Mode Failure	A failure of two or more channels in the same way, causing the same erroneous result.
Common Cause Failure	A failure which is the result of one or more events, causing failures of two or more separate channels in a multiple channel system, leading to a failure.

2.3.1 Disclosure Classification

Controlled Disclosure: Controlled Disclosure to external parties (either enforced by law, or discretionary).

2.4 ABBREVIATIONS

Abbreviation	Description
AC	Alternating Current
AP	Automation Processor
DC	Direct current
DCS	Distributed Control System
DRT	Design Review Team
EC&I	Electrical Control and Instrumentation
FFFR	Fossil Fuel Firing Regulations
HMI	Human Machine Interface
IDR	Internal Design Review
IO	Input Output
LDE	Lead Discipline Engineer
LHS	Left Hand Side
RHS	Right Hand Side
UPS	Uninterruptable Power Supply

2.5 ROLES AND RESPONSIBILITIES

The following are the roles and responsibilities for the implementation of this document:

1. SCOT C&I Study Committee – responsible for establishing the standards that govern the implementation of the Essential Instrumentation Standard.
2. Lead Discipline Engineer (LDE) – responsible for applying this standard during project implementation, ensuring that design deliverables are met according to the requirements of the standard.
3. Design Review Team (DRT) – responsible for detailed design review of the design, and ensures that the detailed design meets the design criteria contained within this standard. The IDR process will ensure effective application of this document.

2.6 PROCESS FOR MONITORING

The SCOT C&I Study Committee will monitor and maintain this document.

2.7 RELATED/SUPPORTING DOCUMENTS

None.

3. DESIGN REQUIREMENTS FOR HMI SYSTEMS

3.1 CONTROL SYSTEM HMI

Modern power plant control systems are complex, consisting of a large number of integrated networked components such as servers, processors and communication devices functioning as an integrated unit. In the event of emergencies and failure of HMI systems, plant operators must cope with high mental stress and have the ability to make informed decisions about the status of the plant and its controlled condition. The primary mechanism through which the plant operator obtains information is through the HMI System, and therefore the HMI system shall be designed with the principles of redundancy, and functional diversity to ensure reliable HMI operations.

HMI systems have progressed substantially as advancements in control systems technology have been made. With the integration of various instruments for monitoring tasks, automatic controllers for machine control and performing of various control functions which have previously been manual, HMI systems have developed to become complex components of automatic control systems.

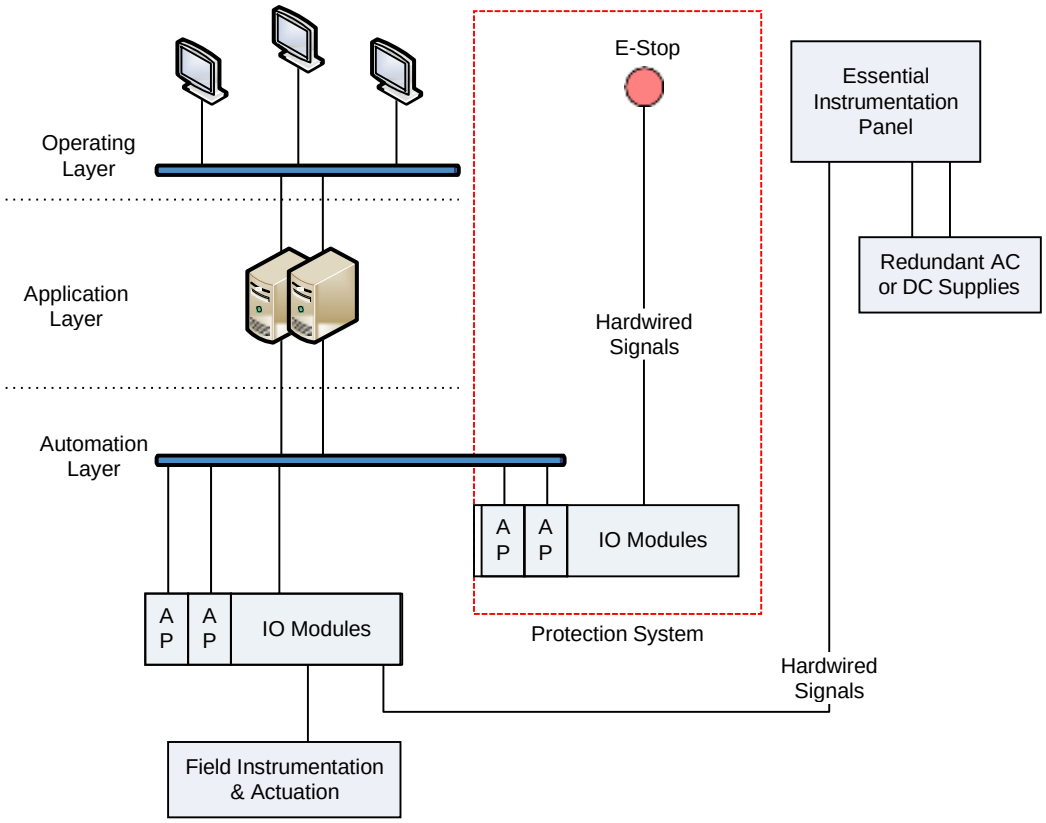

Figure 1 – Essential Instrumentation Panel (Hardwired from the Automation Layer)

As a result, the role of plant operators has changed to rely entirely on the HMI for the control and operation of the plant. Therefore, HMI systems form vital infrastructure to meet the complexity of power plant automation systems and the adverse effects of HMI failure should be well mitigated through design.

Figure 1 illustrates the design concept for the essential instrumentation display. The display shall be wired from the Automation Layer of the control system or DCS and hardwired in the form of

binary and analogue signals. The display shall operate independently of the HMI system (or Application and Operating Layers) of the DCS.

Also shown in Figure 1 is the Emergency Stop, which is defined as a fail-safe control switch, which will stop operations of the Unit and shut the plant down. In the event of a complete HMI failure, the plant operator has the facility to shut down the plant safely and independently from the HMI system.

All hardwired signals shall be loop powered as far as practically is possible. This would depend upon the digital displays selected during the detailed design of the Essential Instrumentation Panel. However, if external power supply is required, the following design principles shall be considered:

1. External Direct Current (DC) power supplies shall be redundantly configured, supplied from redundant battery charges.
2. Equipment requiring Alternating Current (AC) supplies shall be supplied by redundant Uninterruptible Power Supplies (UPS's).
3. The power distribution circuitry shall be appropriately designed to meet the design requirements of the panel, in terms of power supply sizing calculations, cabling calculations and also of appropriate sizing of circuit breakers for system isolation and protection.

In some cases, it may be preferable to provide a networked Essential Instrumentation Display, according to Figure 2. The networked communication for the Essential Instrumentation Display shall be redundantly configured from the Automation Layer, and entirely separate from the Operating and Application networks.

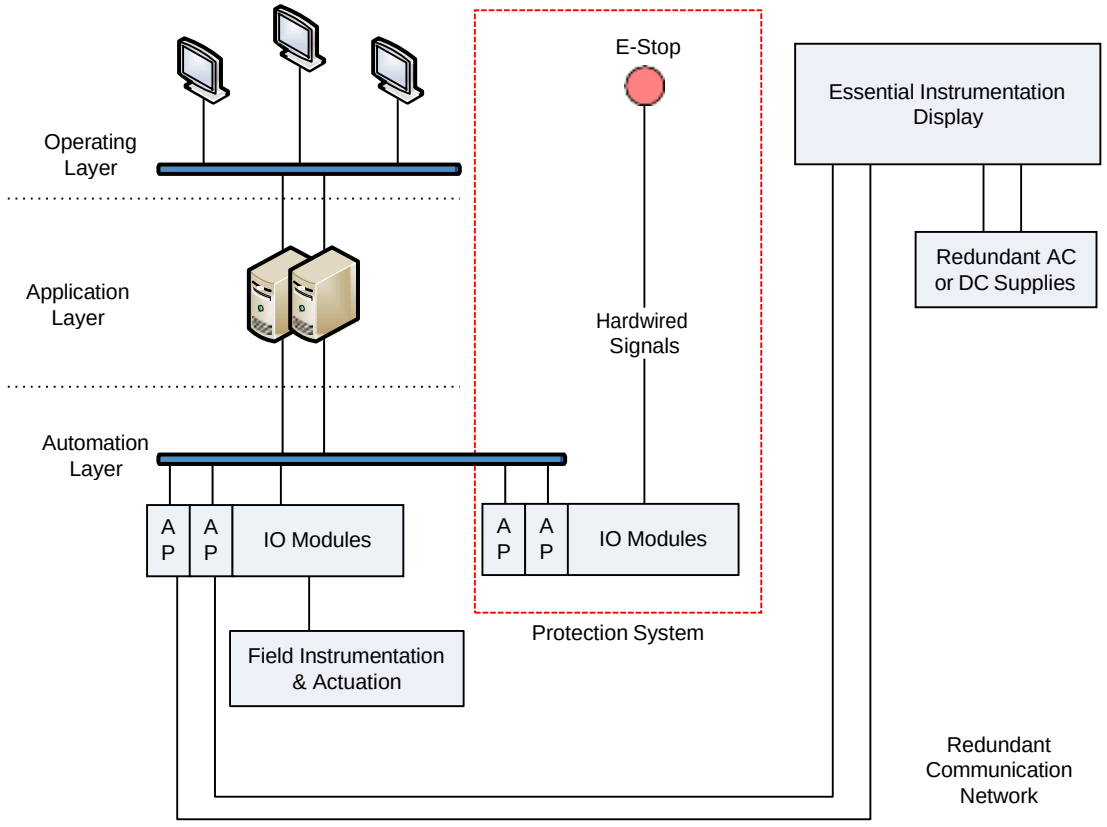

Figure 2 – Essential Instrumentation Display (Networked from the Automation Layer)

3.2 GENERAL REQUIREMENTS FOR ESSENTIAL INSTRUMENTATION DISPLAYS

The Distributed Control System (DCS) fulfils the requirements for operator functions for operating, monitoring, closed loop and open loop control and the protection of boiler and turbine plant. In the event of HMI failure or loss of the HMI application servers, networks or power supply, the operating HMI is inoperable and presents a risk to plant operation.

It is a requirement of the Eskom fossil fuel firing regulation, [2] 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.

Therefore, to ensure that plant information is available to the plant operator in the event of HMI failure, the following forms general requirements to Essential Instrumentation Displays:

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 regulation, 36-680.
2. The information presented on the essential instrumentation displays shall be accurate, useful for the current moment and display information unambiguously.
3. The essential instrumentation displays shall be designed to represent appropriate information of plant statuses to allow plant operators to make informed decisions on the state of plant and to apply remedial operator action according to defined operating protocols.
4. The essential instrumentation displays shall consist of essential alarms and measurements of plant data to enable a reliable and a clear understanding of plant conditions and on the health of critical systems, such as boiler protection and turbine protection systems.
5. The essential instrumentation display shall be a hardwired mimic panel, designed to display specific information to provide a safe and efficient operator interface giving the plant operator an awareness of plant conditions, a perception of risk and also of warning relating to critical systems failures.
6. The essential instrumentation display shall be clear, intuitive and easy to understand in situations of system failure and critical plant conditions. All information shall be displayed in a coordinated manner, prioritised for urgency and filtered to avoid an “overload” of information; it should be specific to relay targeted information of plant conditions.
7. 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.
8. The essential measurement panel shall be located at the operator desk.
9. The essential measurement panel shall consist of the following:
    a. Binary indications;
    b. Analogue indications.
10. The binary and analogue indications of the essential measurement panel shall be hardwired to the process automation system.
11. The essential measurement panel shall be fully independent of the operator clients and control system servers.
12. Analogue indications shall be dynamically presented.
13. Binary indications shall be dynamically presented with information matched to the current situation and shall clearly distinguish between different alarm priorities.

3.3 SPECIFIC DESIGN REQUIREMENTS

The overall requirements to the design of the essential instrumentation display are presented in this section of the document. It describes specific functional requirements for the hardware design of the display to mitigate HMI system failure and also gives requirements for enhancing system reliability through redundancy.

The power plant control system (DCS) architecture provides an integrated monitoring, control and automation platform for power plant control functions for boiler and turbine control. Functions include modulating analogue and binary control, protection and interlocking functions, which is controlled by the plant operator via the HMI system.

Due to the complexity of the HMI system, and in the event of HMI system failure, the essential display forms a tentative process monitoring system for informed operator decision making and does not form an operator control station.

The design of the essential display shall conform to the specific requirements as listed below:

1) Normal Operation

   a. The HMI system is used to operate the plant as per normal operating protocol, and shall ensure a safe and efficient operating practice. All aspects of the HMI system are health and functioning correctly.

   b. The essential instrumentation display shall be operational during normal plant operations (which include run-ups, shut-downs and steady state plant conditions). It should be noted though, that the Essential Instruments Panel (Display) is not required to be used by the plant operator to perform any operations.

2) Operation during HMI System Failure

   a. HMI System Failure – HMI system failure can be caused due to many conditions, which can be planned or unplanned. During HMI failure, the total HMI can failure (HMI servers, HMI networks or HMI power supply). Typically these systems are redundantly configured, but their specific level of failure can results in total HMI failure. Total HMI failure may include partial system failure, loss of HMI screens and loss of all indications and control.

   b. Operator Action during HMI System Failure – Standard operational protocol shall be followed in the in event of HMI failure, and every endeavour shall be made to recover the HMI to full operational status as soon as possible, by calling out relevant technical personnel to fault find and to restore operation functions of the HMI system.

   c. The essential instrumentation display shall be operational during critical HMI system failure, and shall operate / display information independently from the HMI system. The Essential Measurements Panel shall be used by the operator to decide on whether to continue running the plant or to trip the plant using the Emergency Push Button.

3) Design of the Essential Display

   a. The design of the display shall be compatible with the level of performance required by the plant operator to perform monitoring functions for informed decision making on the Unit. Information on the display shall bare the following characteristics:

   b. The essential instrumentation display shall be designed with the plant operator in mind, and on displaying information which facilitate effective operator actions, ergonomically forms part of the operating desk / control room, to allow for a safe and accessible location and to allow for expected operational requirements.

   c. The essential instrumentation display shall be designed to provide an overview of key process information that can be scanned by the plant operator to gain a rapid appraisal of

the plant status, critical parameters and conditions. This display shall allow plant operators to have a common understanding of plant conditions.

d. Especially in the event of critical HMI system failure, the essential display becomes the focal point of plant monitoring, where the intended purpose is to enable the plant operator to evaluate the process condition.

e. Monitoring information shall be clearly defined and as a minimum shall consist of the following categories of information:

   i. Critical Process Signals.

   ii. Critical Alarms (indicating automation system health and protection system health as a minimum).

   iii. Specific information relating to process conditions.

It is important to note that the essential display is not just a mere listing of process signals, but that it should form a concise and specific representation of plant conditions and should not be “clouded” with a large listing of redundant process information. Therefore, the information is displayed specifically and methodically to convey targeted information.

The DCS system forms the main plant control and data acquisition system for power plant automation, fulfilling functions for operating, control and protective functions. With failure of the HMI system, the aforementioned information is not visible to the plant operator, and therefore, one of the motivating factors for the Essential Instrumentation Panel (or Display) is to give assurance that the control and protective functions of the DCS system is fully operational. Therefore, the following plant conditions, especially of control equipment shall be fully operational and functional in the event of HMI failure.

Plant conditions to be monitored include:

1) Boiler Control Health.

2) Burner Management System Health.

3) Turbo-Generator Health.

4) Turbine Control / Turbine EHC Health.

5) Automation Network Health.

The number of signals displayed shall not be excessive. It is preferred that the number of signals be optimised and range in the order of 20 to about 30 analogues, with a minimum set of binary signals for alarms or status indication. Where binary signals are configured for alarms, forming part of the Essential Instrumentation Panel, alarms can be configured via lamps (labelled). The rationalisation of the signals shall be adequately documented.

Table 1 below gives an overview of the minimum signals to be displayed as part of the essential instrumentation panel. The signals are based upon the FFFR listing of essential instrumentation; see section 3.1.12 of FFFR Standard [2]. The signals are aimed at giving a holistic picture of the real-time status of the power plant. It should be noted, that each power plant shall uniquely define their respective signal requirements for the display but as a minimum, the information presented in the table is mandatory. Display information as a minimum shall consist of the following signals:

Table 1 – Signals Required for the Essential Display

#	Signal	Signal Type
1.	Electrical Generated Load	Analogue
2.	Boiler Outlet Steam Flow	Analogue
3.	Boiler Outlet Steam Pressures	Analogue
4.	Boiler Outlet Steam Temperature	Analogue
5.	Feed Water Flow or Economiser Flow	Analogue
6.	Drum Level (where applicable)	Analogue
7.	Attemporator 1.1 Temperature or Evaporator Outlet Temperature (where applicable)	Analogue
8.	Total Combustion Air Flow	Analogue
9.	Furnace Flame Failure Monitor (or Pyrometers)	Analogue
10.	Furnace Pressure	Analogue
11.	Total Fuel Flow*	Analogue
12.	Total Coal Flow*	Analogue
13.	Total Oil Flow*	Analogue
14.	Propane Gas*	Analogue
15.	Oxygen (O_2) Measurement at the Economiser	Analogue
16.	Unit Control Air Supply at the Unit	Analogue
17.	Main Turbine Speed	Analogue
18.	Condenser Pressure	Analogue
19.	Generator Abnormal	Binary
20.	Boiler Protection Health	Binary
21.	Turbine Protection Health	Binary
22.	Automation System Heath	Binary

(* where **Co-Firing** exists, all **Fuels Shall** be indicated separately)

3.4 HARDWARE DESIGN CONSIDERATIONS

The following are design considerations for essential displays.

1) Analogue and Digital Displays – Due to accuracy concerns with analogue displays, the essential displays shall use digital displays. Displays shall be configured for a “one sensor / one display” design approach, where information shall be presented at the lowest level of detail possible.
2) Real Time Accuracy of Displays – Digital displays shall provide good performance, and perform over extended periods of time and shall display information in real time.

3) Compact Size and Systematic Layout – The essential display shall have a compact size and shall present information in an intuitive and systematic layout.

4) Good Sense of Design and Good Visibility – The displays shall be easy to read, even from a wide range of view angles. Due to the fact that display panels are not always viewable directly from the front, a wide viewing angle is important. It is recommended that display devices shall display characters with white or yellow colour with a black background. The colour yellow draws attention better.

5) In many instances, HMI design is a contributing cause to HMI failures. Loss of HMI systems has a significant impact on the operational safety of the power plant; therefore the essential HMI shall be independent from the operator HMI system.

6) The hardware design of the Essential Instrumentation Panel (or Display) shall follow a functional design methodology. The functional design basis of the control room and of the HMI, shall integrate the Essential Instrumentation Panel as part of the detailed design of the control room, HMI and room design.

3.4.1 Essential Instrumentation Panels and Displays

Figure 3, Figure 4 and Figure 5 illustrates typical instrumentation panel/display installations. General specifications for the display range are 4 digits, -1999 to 9999, with a 0.1% accuracy of full scale. Typical indicator dimensions shall be of the order, 24mm (H) x 48mm (W).

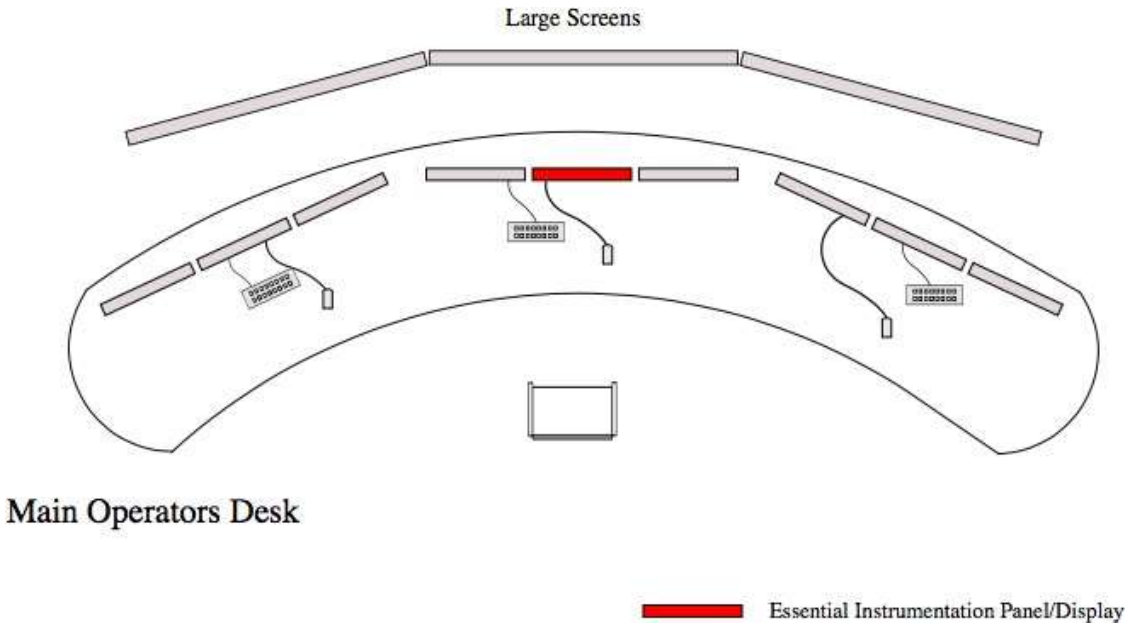

Figure 3 – Typical Location of the Essential Instrument Panel/Display

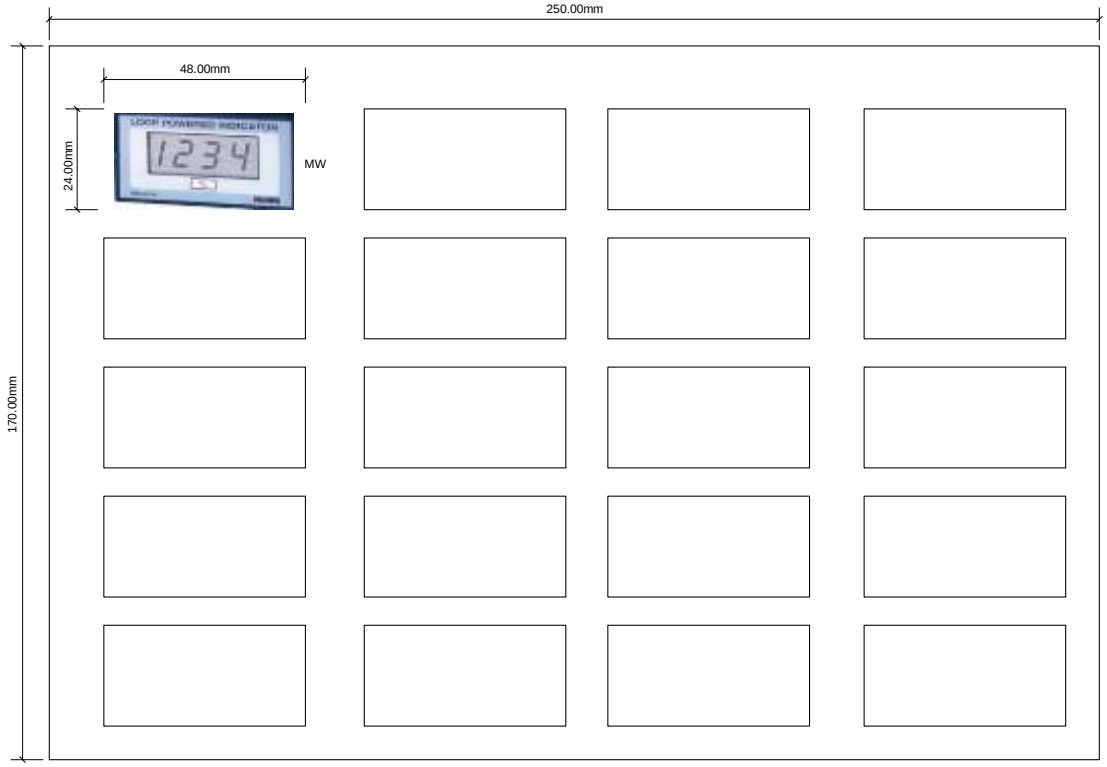

Figure 4 – Typical Dimensions of an Essential Instrumentation Panel

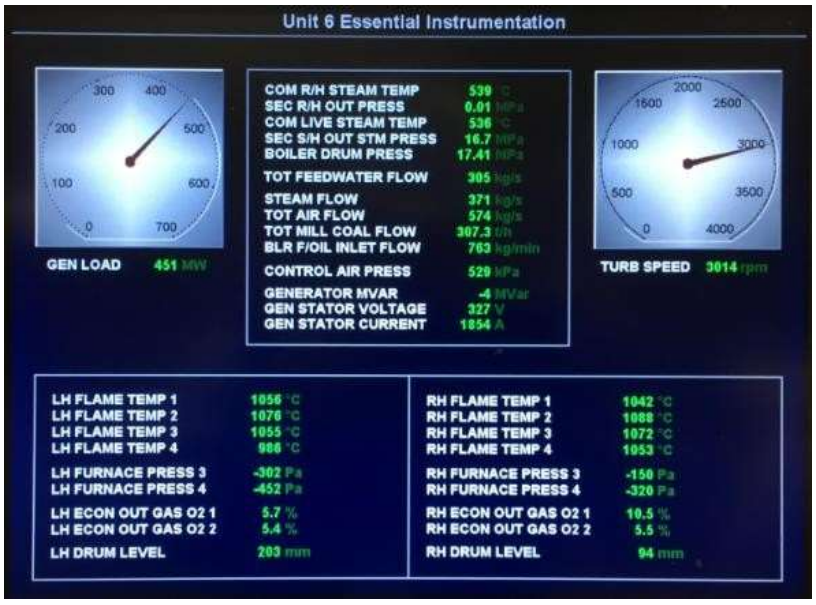

Figure 5 – Typical Networked Essential Instrumentation Display (source: Arnot PS)

3.5 IO MODULE DIVERSITY

In order to provide greater availability of the essential instrumentation display, the principles of diversity of IO modules shall be applied to all signals, following the principles as described in [3].

As far as is practically possible, the signals shown in Table 1 shall be driven by independent IO modules.

As a minimum, IO modules from two Application Processors (AP's) shall be used, one for Turbine monitoring and the other for Boiler monitoring. Diverse IO modules shall also be used to distribute the IO. See Figure 6. It may also be desirable to allocate IO according to Functional Group allocations, in this instance, IO's are driven from the cabinets where the signals are being used. As an example, if furnace pressure is used in the draft group AP then this AP sends output to the essential panel.

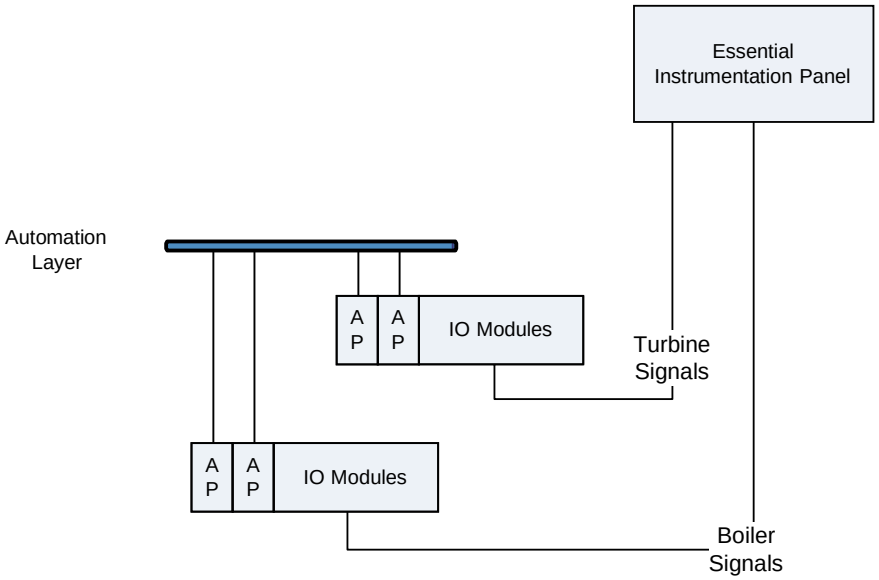

Figure 6 – IO Module Diversity Principle

3.6 LOGICAL DESIGN CONSIDERATIONS

It is not possible to display all process variables and plant statuses within the essential instrumentation panel, but to allow for reliable and accurate display of selected plant parameters. Therefore, to assist in the optimisation of the information displayed, the following logical functionality shall be required.

1) Use of Average Values shall be used to display plant parameters (such as 2oo3, 1oo2 etc.).
2) In cases where signals are designated LHS and RHS, where both averages of LH and RH signals can be accommodated within the display panel, both LHS and RHS values are to be display. Where there are space restrictions on the physical size of the panel, any average values shall be displayed.

4. CONCLUSION

The essential instrumentation display forms a FFFR requirement, and presented in this document are some guidelines which need to be considered as part of the design requirements.

5. AUTHORISATION

This document has been seen and accepted by:

Name & Surname	Designation
	Chief Engineer C&I Plant CoE (Governance)
	Acting Middle Manager C&I Plant CoE (Governance)
	Senior Manager EC&I
	Senior Consultant C&I PEIC
	Senior Manager PEIC C&I and Electrical (Acting)
	Chief Technologist C&I PEIC
	Chief Engineer C&I Plant CoE (Governance)

6. REVISIONS

Date	Rev.	Compiler	Remarks
24/01/2018	0.0		First Draft for SC Final Review
3/04/2018	1		Final Document for Authorisation and Publication

7. DEVELOPMENT TEAM

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

- [redacted]
- [redacted]

8. ACKNOWLEDGEMENTS

- C&I Study Committee members for their respective comments and input.