

	Standard	Technology
---	----------	------------

Title: **Power Plant Controls & Instrumentation; Control Systems; Distributed Control Systems (DCS); Part 1: General Standard**

Unique Identifier: **240-132042241**

Alternative Reference Number: **N/A**

Area of Applicability: **Engineering**

Documentation Type: **Standard**

Revision: **1**

Total Pages: **31**

APPROVED FOR AUTHORISATION

☒ TECHNOLOGY ENGINEERING
DOCUMENT CENTRE ☎ X4962

Next Review Date: **January 2024**

Disclosure Classification: **CONTROLLED DISCLOSURE**

Compiled by



P. Govender
Chief Engineer, C&I Plant

Date: 22/01/2019

Approved by



M. Nkumbule
Middle Manager, C&I Plant
(Acting)

Date: 01/02/2019

Authorised by



P. Madiba
Senior Manager, EC&I

Date: 2019/02/01

Supported by SCOT/SC/TC



C. Boesack
Chairperson, Power Plant
C&I SC

Date: 23/01/2019

PCM Reference: **240-53458811**

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

CONTENTS

	Page
1. INTRODUCTION	3
2. SUPPORTING CLAUSES.....	5
2.1 SCOPE	5
2.2 NORMATIVE/INFORMATIVE REFERENCES.....	5
2.3 DEFINITIONS.....	5
2.4 ABBREVIATIONS.....	16
2.5 ROLES AND RESPONSIBILITIES.....	18
2.6 PROCESS FOR MONITORING.....	18
2.7 RELATED/SUPPORTING DOCUMENTS.....	18
3. CONFORMANCE TO THIS DOCUMENT.....	19
4. OVERALL REQUIREMENTS	20
4.1 GENERAL.....	21
5. KEY PERFORMANCE REQUIREMENTS.....	23
5.1 PROVEN-IN-USE	23
5.2 AVAILABILITY	23
5.3 RELIABILITY	23
5.4 MAINTAINABILITY	24
5.5 SEGREGATION	24
5.6 EXTERNAL SIGNAL EXCHANGE	24
5.7 INTERNAL SIGNAL ACQUISITION	26
5.8 LIFE EXPECTANCY.....	26
5.9 SUPPORTABILITY.....	26
5.10 OEM INVOLVEMENT.....	27
5.11 ENVIRONMENTAL CONDITIONS.....	27
5.12 INTEGRATION AND CONSISTENCY OF DESIGN	27
5.13 STANDARDISATION	27
5.14 RESPONSE TIMES.....	28
5.15 CONTROL TASKS	29
6. AUTHORISATION.....	31
7. REVISIONS	31
8. DEVELOPMENT TEAM	31
9. ACKNOWLEDGEMENTS	31

FIGURES

Figure 1: Overall framework of this multipart document.....	4
Figure 2: Typical breakdown of a power plant into control islands.....	7
Figure 3: Typical breakdown of a C&I system	8
Figure 4: A typical DCS structure	20
Figure 5: Definition of the DCS subsystems.....	22
Figure 6: Typical forms of external signal exchange	25
Figure 7: Illustration of response times in a DCS	29

TABLES

Table 1: Overall framework of this multipart document.....	3
--	---

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 1: General**. 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 [This Part]	Overall requirements, framework and definitions
2	Operator & Supervisor System	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.

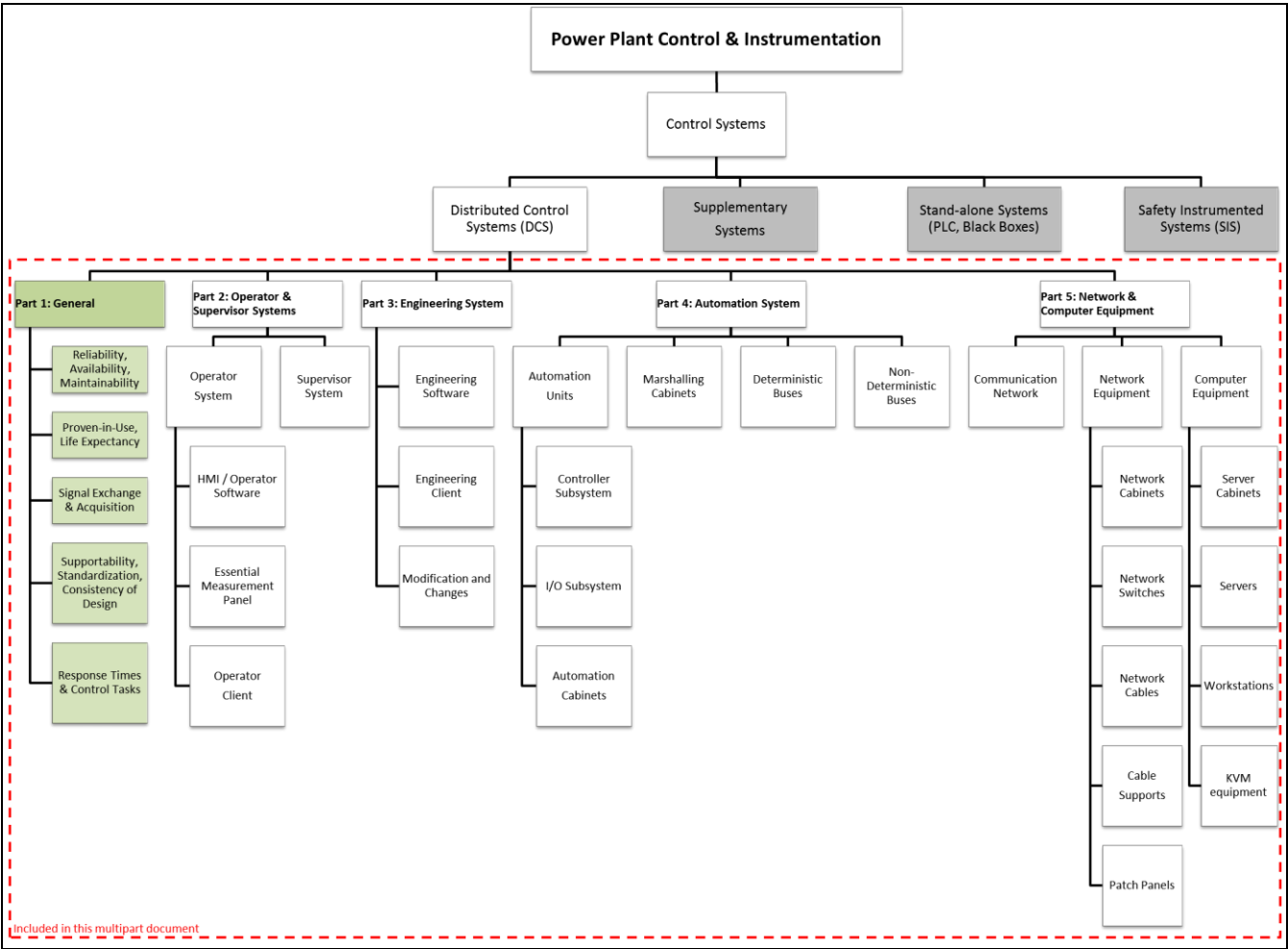


Figure 1: Overall framework of this multipart document

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 1: General**; the scope of which is the specification of the structure, definitions and overall requirements of a DCS.

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 B2e: VGB PowerTech; Design standards for Instrumentation and Control Equipment: Automation Function.
- [2] 240-56355731: Eskom; Environmental Conditions for Process Control Equipment Used at Power Stations standard.

2.2.2 Informative

Not applicable.

2.3 DEFINITIONS

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

2.3.1 Document conformance definitions

D.1. Capability

It refers to functions and abilities that are available to a user of this document. It is necessary for capabilities to be followed to conform to this document. Capabilities are identified with the verbal forms "can" and "cannot".

D.2. Controlled disclosure

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

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.

D.3. Permission

It refers to 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”.

D.4. Possibility

See definition of capability.

D.5. Recommendation

It refers to 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”.

D.6. Requirement

It refers to mandatory provisions, conditions and functions. It is necessary for requirements to be strictly followed to conform to this document. Requirements are identified with the verbal forms “shall” and “shall not”.

2.3.2 General definitions

D.7. Active phase

It refers to the product life cycle phase in which the product is continually being manufactured, is actively marketed and is available for both sale and support.

D.8. Available

It is the when a system, component or equipment is in the up state, i.e. in service, operational and able to perform as required.

D.9. Balance of Plant (BOP)

It consists of a power plant's auxiliary plant systems that are required to support the power island(s), e.g. fuel processing systems, cooling systems, water treatment, material handling, etc. The specific set of plant systems that form the balance of plant is dependent on the applicable power plant's configuration and design.

D.10. Black-box

It is a standalone device or group of devices that is independent of the DCS. The black-box may perform process interface, control and/or supervision tasks; all of which are performed independently of the DCS.

A black-box is typically supplied by a mechanical/electrical plant supplier as part of a process skid system (e.g. lube oil system, compressors, etc.). It contains the control tasks for the specific process plant concerned.

D.11. Black-box interface

It is the signal exchange between a black-box and the main control system. This signal exchange may be hardwired signals, software signals, or a combination of both.

D.12. Centralised system

The centralised system contains the management and supervision services and functions (supplementary systems) that are common across multiple control islands. The centralised service does not perform any control or operational functions, and as such does not include an automation system or any black-box interfaces. These are implemented in the applicable control island. The relationship between the centralised system and the control islands is shown in Figure 2.

D.13. Control Island

It is a group or set of plant and C&I systems that together form an autonomous and integrated system that can be operated and controlled independently (i.e. as an island). The systems that are grouped together to form a control island will differ from power plant to power plant since it is dependent on the

applicable power plant's configuration, production and operational requirements. An example of the breakdown of a power plant into control islands is shown in Figure 2.

D.14. C&I room

It refers to any room in which C&I equipment is installed such as the equipment room, control room, engineering room, etc.

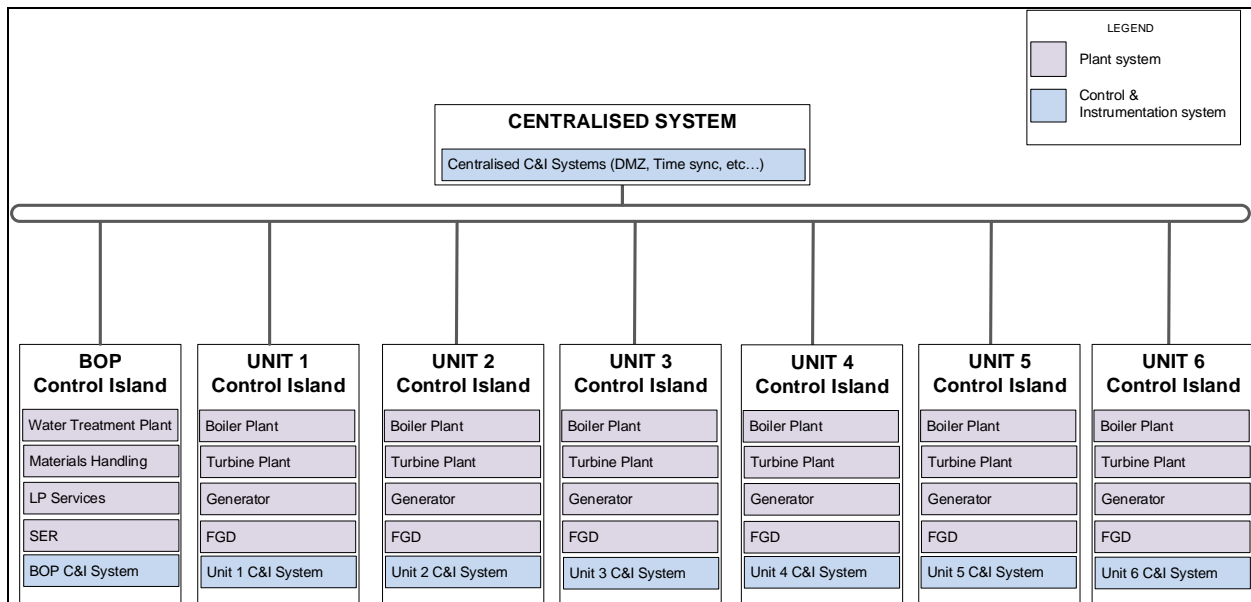


Figure 2: Typical breakdown of a power plant into control islands

D.15. C&I system

Refers to the complete system used to control and operate the power plant. It is inclusive of the control system (DCS and/or black-box systems), field equipment (cabling, instruments, actuators, junction boxes, etc.) and power distribution systems. The C&I system is sub-divided into multiple independent subsystems for each control island. See [Figure 2](#) and [Figure 3](#).

D.16. Control system

It is an electronic based system to control and operate process plant. It is a system that responds to inputs from the process and/or from an operator and generates outputs that cause the process to operate in the desired manner. The two main types of control systems used in the process industry are distributed control systems (DCS) and programmable logic controllers (PLC).

D.17. Customer

Eskom, being the end user.

D.18. DIN rail

A DIN rail is a metal rail in a cabinet for internally mounting industrial equipment such as circuit breakers, network switches, terminal blocks, etc.

D.19. Disrupt

It is to have a negative impact or results in incorrect behaviour. This may be in the form of incorrect acquisition of input signals, incorrect display of signals, incorrect output of signals, tripping of plant, loss of control, loss of protection, freezing of the HMI, etc.

D.20. Distributed control system (DCS)

It is a type of control system; one that is used in the process industry for the supervision, control and protection of process plant requiring complex control functions. The main elements of a DCS are the

microprocessor-based controllers (which are functionally and/or geographically distributed); input/output (I/O) cards; communication networks; and the operator system.

D.21. Dynamic

Refers to the real-time status based on the actual state of the plant and C&I system.

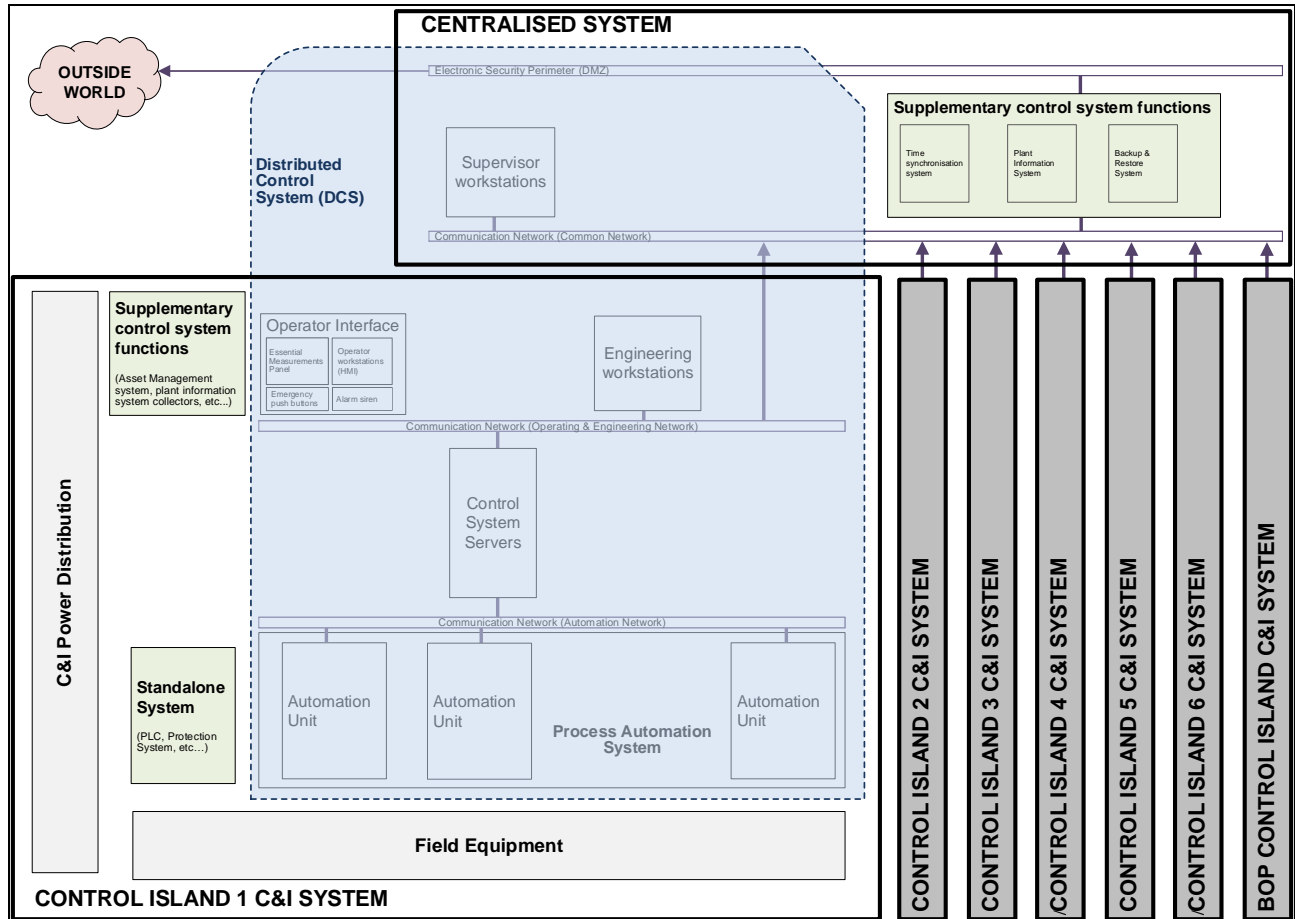


Figure 3: Typical breakdown of a C&I system

D.22. Factory acceptance test (FAT)

It is an activity that demonstrates that the control system complies with its specification(s).

D.23. Failure

It is the loss of ability of a system, component or equipment to perform as required.

D.24. Field device

It refers to all local control, measuring and actuating devices in the process plant. It is inclusive of all transmitters, switches, analysers, actuators, solenoids, motors, drives and local control stations.

D.25. Functional specification

It is a document that describes how the supplier shall configure the control system to provide each requirement defined in the specification by the customer. The functional specification is usually created during the design and engineering phase of the project.

D.26. Hot swappable

It is when the equipment concerned can be safely replaced while the system to which it belongs is operational. The replacement does not disrupt the operation of the system, nor the plant under control. The equipment replaced can be made fully operational without restarting or rebooting the system.

CONTROLLED DISCLOSURE

D.27. KVM module

It is a device or set of devices that allows the input/output devices of a workstation – i.e. the keyboards, video monitors and mouse – to be physically removed from the workstation computer such that workstation computer shall be remotely accessed.

D.28. Input signal

It refers to any input acquired by the DCS. It is inclusive of inputs hardwired to the DCS via input cards as well as signals acquired by the DCS via black-box interfaces.

D.29. On-load

It is when the plant is in operation.

D.30. Original equipment manufacturer

It is the internationally registered legal entity who owns the rights for the manufacture, design and repair of the distributed control system.

D.31. Output signal

It refers to any output sent by the DCS. It is inclusive of outputs hardwired from the DCS via output cards as well as signals sent by the DCS via black-box interfaces.

D.32. Power Island

It consists of the core generation components of a power plant e.g. the boiler, turbine, and generator systems. The specific set of plant systems that form a power island is dependent on the applicable power plant's configuration and design.

D.33. Programmable logic controller (PLC)

It is a type of control system; one that is used in the automation industry for simple and/or sequential control applications. The main elements of a PLC are the microprocessor-based controllers and input/output (I/O) cards. It is a standalone automation system usually dedicated to the control and protection of small auxiliary plant systems. It does not contain an operator or communication network within itself and is usually interfaced to other systems (e.g. a SCADA system or DCS) when remote operating capability is required.

D.34. Specification

It defines the technical requirements, features, and functions that the control system must provide. The specification is generally contained with contractual documents such as the Employer's requirements or Works Information.

D.35. Supervised fully automatic

It refers to a control mode during which the operator monitors the steps of a fully automatic start-up or shut-down sequence. Each sequence step has hold points at which the operator can verify essential plant parameters and the critical actions to be taken.

D.36. Supplementary systems

It is the management and support layer of the control system; this being control system equipment via which system administrators perform control system management tasks and auxiliary equipment required to support the core control system functions. It does not contain any systems required to perform the core DCS functions (that of control, supervision, engineering and diagnostics). It may include systems such as the backup & restore system, central update system asset management system, time synchronisation system and plant information system. Note the scope of this multipart document excludes the supplementary systems. This is specified in other Eskom standards and guidelines.

D.37. Supplier

It is the company, agent or entity that supplies the applicable technology or product.

CONTROLLED DISCLOSURE

D.38. Tag identifier

It is the power plant's coding system identification code of a particular device, e.g. the KKS identifier or AKZ identifier.

D.39. Version

It is a term used to define the revision of a software package or hardware module e.g. in the instance of Software X V1.2, the version number is 1.2.

2.3.3 Operator & supervisor system definitions

D.40. Alarm types

A specific alarm on a measurement (e.g. MAX1, MAX2, MIN1 or a discrepancy alarm).

D.41. Essential measurement panel

It is a panel on the operator desk which displays the essential measurements of the control island.

D.42. Human machine interface (HMI)

"The human machine interface is the software package on the operator [client] via which the plant operator interacts (operates & monitors) the process plant. The HMI is inclusive of all HMI graphics, alarm lists, event lists, trends, plots, and other elements that form part of the software package used to operate and monitor the plant" – from Eskom standard 240-56355728.

D.43. Mimic

It is a graphical representation of a particular system in the power plant (e.g. the feedwater system). It contains dynamic and static elements that visually depict the configuration and status of equipment in the subsystem concerned.

D.44. Faceplate

"The interface or window of a particular component in an HMI graphic page through which the said component is operated and monitored in detail" – from Eskom standard 240-56355728.

D.45. Operator software

It is the software through which the plant operator monitors and operates the power plant. The term is used interchangeably with human machine interface (HMI). See also the definition of HMI.

D.46. Operator desk

It is the desk from which, the plant operator supervises the control island. The operator client is accessible from the operator desk. The essential measurement panel and emergency push buttons are located on the operator desk.

D.47. Operator server software

It is the server software via which communication occurs between the automation system and the operator software. It includes the operator database and contains all necessary interfaces and configuration settings to perform its function.

D.48. Operator system

It is the supervision layer of the control system; this being the control system equipment via which the plant operator supervises the control island. The operator system is inclusive of the operator clients, portions of the communication network, and portions of the control system servers.

D.49. Operator client

It is the computer via which the operator software is accessed. It is the primary interface of plant operators.

D.50. Process alarms

It is one category of alarms; being alarms that are generated from malfunctions of plant equipment or process deviations. These are separate and distinct from system alarms.

CONTROLLED DISCLOSURE

D.51. System alarms

It is one category of alarms; being alarms that are generated from notifications or malfunctions of C&I system equipment (hardware or software). These are separate and distinct from process alarms.

D.52. Supervisor system

It is the observation layer of the control system; this being the control system equipment via which the supervisor monitors multiple control islands. The supervisor system is inclusive of the supervisor clients and portions of the communication network.

D.53. Supervisor client

It is the computer via which the supervisor software is accessed. It is the primary interface of plant supervisors.

2.3.4 Engineering system definitions

D.54. Application software

It is the project specific logic, configuration data and software programs that are executed in the control system to protect, control, monitor and operate the plant. It is inclusive of all logic and software programs required to execute the protection tasks, control tasks and operate the plant such as the sequence control logic, closed loop control logic, permissives, alarm logic and HMI graphics.

D.55. Engineering server software

It is the server software via which communication occurs between the automation system and the engineering software. It includes the engineering database and contains all necessary interfaces and configuration settings to perform its function.

D.56. Engineering software

It is the software through which engineers and technicians configure, maintain and troubleshoot the C&I system. It is inclusive of all diagnostic, maintenance, configuration and engineering software of the C&I system. It includes the application engineering software, hardware engineering software, and any software used in the design of the C&I system.

D.57. Engineering system

Refers to the engineering & diagnostic layer of the control system; this being the control system equipment via which engineers and technicians configure, maintain and troubleshoot the C&I system itself. The engineering system is inclusive of the engineering clients, portions of the communication network and portions of the control system servers.

D.58. Engineering client

It is the computer via which the engineering software is accessed. It is the primary interface of plant engineers and technicians.

D.59. Field engineering

It is the engineering and design of field equipment and its configuration.

D.60. Force

It is the replacement, substitution or simulation of a signal value with a user defined value.

D.61. Functional diagram

It is a graphical representation of the control tasks at different detail levels (overview level, area level, individual level). It is also referred to as a functional block diagram.

D.62. Functional Logic

It is a subset of the application software; being the software that resides in the controllers. It is the term used to collectively refer to all functional diagrams in the controllers in the control system.

D.63. Functional unit (FU)

It is a group of control tasks for one or more plant systems that belong together, e.g. Mill 10 FU, Feedpump 1 FU, etc. The set of control tasks grouped within each functional unit is dependent on the process complexity, plant configuration and the required level of automation. It is also referred to as a function unit and is a subset of the functional logic.

D.64. Loop wiring diagram

It is a detailed drawing showing the electrical hook-up of a field device (instruments, actuators, drives, black-boxes, etc.) to the automation system. The loop wiring diagram shows the full wiring details from the source of all related signal(s) through all intermediate equipment (marshalling cabinets, junction boxes, field terminal blocks of the automation cabinet, etc.) up to the relevant channels of the I/O cards.

D.65. Permissive

It refers to the preconditions necessary for an operation or event to occur. Specifically, it is a subset of logic that prevents an operation or event from occurring when the preconditions are not met. It includes ON releases, OFF releases, protection ON, protection OFF, AUTO releases, etc.

D.66. Signal identifier

It is the unique tag via which the signal is referenced, identified or labelled, e.g. XG01.

2.3.5 Automation system definitions

D.67. Automation cabinet

It is the physical cabinet(s)/housing of an automation unit. It is inclusive of all internal cabinet mechanical housings and passive components such as the I/O racks, controller racks, terminal blocks and cable supports.

D.68. Automation system

It refers to the automation layer of the control system; this being the control system equipment that performs the control tasks (closed loop control, sequence control, permissives, etc.) and process interface tasks (signal acquisition and commands). The automation system is inclusive of the automation units, the portions of the communication network used for communication between automation units, and all marshalling (if any).

D.69. Automation unit (AU)

It is a self-contained, autonomous entity dedicated to the process interface and control tasks of a particular plant system, e.g.: Mill 10. The automation unit contains all automation equipment necessary to independently execute its assigned control tasks and is inclusive of the controller subsystem, I/O subsystems (I/O cards and I/O buses), black-box interfaces (if any), and automation cabinet(s).

D.70. Cabinet auxiliary equipment

It is the auxiliary equipment internal to an automation cabinet. It consists of the active components in the cabinet that are not part of the controller subsystem, I/O subsystems or cabinet power supply. It is inclusive of components such as fans, door contacts, temperature switches, interposing relays, galvanic isolators, media converters, etc.

D.71. Cabinet power supply

It is the automation cabinet's internal power supply and distribution equipment. It is inclusive of all diodes, breakers, bus bars, monitoring relays, etc. that are used for the distribution and monitoring of power within the cabinet.

D.72. Card

It is electronic assembly or module that occupies one or more slots in an automation rack, e.g. an I/O card, controller card, communication card, etc. It is also referred to as automation card.

CONTROLLED DISCLOSURE

D.73. Controller

It is an independent fully programmable microprocessor based computing unit in which the functional logic is executed to perform plant control and process interface tasks.

D.74. Controller subsystem

It consists of the controller rack, the controllers and its' supporting cards (such as the controller rack communication cards and controller rack power supply cards).

D.75. Cross-wiring

It refers to the wiring used to interconnect trunk cables terminated on the field terminal blocks of the automation cabinets to the I/O cards in the I/O racks. It may also refer to the wiring used in a marshalling cabinet to interconnect the field terminal blocks (on which the incoming trunk cables are terminated) to the automation terminal blocks (on which the outgoing system cables to the control system are terminated).

D.76. Extension cabinet

It is an automation cabinet that does not contain any controllers or controller subsystem. It contains auxiliary equipment, I/O subsystems black-box interfaces (if any). The I/O subsystems in the extension cabinet communicate with controllers in the main cabinet.

D.77. Galvanic isolation

It is the electrical isolation of two systems such that no direct electrical connection exists between the two systems. Usually galvanic isolation between automation systems is achieved using opto-couplers and electromechanical relays (i.e. interposing relays).

D.78. I/O subsystem

It refers to the I/O cards and the I/O communication bus between the controllers and the I/O cards. It consists of multiple I/O racks, the I/O bus cables, I/O cards, and the I/O support cards (such as the I/O bus communication cards and I/O rack power supply cards).

D.79. Main cabinet

It is an automation cabinet which contains the controllers and controller subsystem. It may additionally contain some I/O subsystems and black-boxes interfaces. The I/O subsystems may be expanded to include I/O racks contained in an extension cabinet.

D.80. Marshalling

It refers to the termination assemblies (or terminal blocks) used to logically order or restructure the manner in which the trunk cables (from the field and black-boxes) are connected to the automation system. There are typically two sets of terminal blocks involved in marshalling (collectively referred to as marshalling terminal blocks); the field terminal blocks onto which the trunk cables from the field and black-boxes are terminated; and the automation terminal blocks onto which the system cables to/from the automation system are terminated. Cross-wiring is used to interconnect the two terminal blocks in a logical and structured manner.

D.81. Marshalling cabinet

It refers to a cabinet that contains marshalling terminal blocks.

D.82. Power cable

It is a cable over which power is distributed.

D.83. Process automation system

It is the main type of automation system of the DCS. One that performs most of the control tasks required (as opposed to protection automation systems).

D.84. Protection automation system

It is a type of automation system dedicated to the safe shutdown of the process in emergency conditions. It performs critical safety functions, e.g. the boiler protection system or turbine protection system.

CONTROLLED DISCLOSURE

D.85. Rack

It is a physical housing or assembly into which the automation cards slot into. It may contain a PCB and backplane for internal rack communication and power distribution.

D.86. Signal wire

It is a wire over which a discrete analog or binary value is transmitted.

D.87. Trunk cable

It is a collection or group of signal wires within one cable.

2.3.6 Network & computer equipment definitions

D.88. Automation network

It is a subsystem of the communication network and refers specifically to the communication layers used for inter-controller communication.

D.89. Cable support

It is a rigid or flexible support structure use to route, manage and support one or more cables. It is inclusive of cable supports internal to cabinets (such as trunking, flexible conduits and cable arms) and external support structures (such as primary racks, secondary racks and trunking).

D.90. Centralised system server

It refers to any physical server in the centralised system.

D.91. Cluster

It refers to a group of servers that act like a single system and provide high availability.

D.92. Computer

It refers to a workstation and server.

D.93. Communication network

It refers to the communication layers of the control system; this being the control system equipment used for inter-controller communication, operator system communication, engineering system communication and communication between control islands. The communication network is inclusive of network switches, network cabling, patch panels, cable supports, etc. It excludes all fieldbuses and automation I/O buses.

D.94. Control system server

It refers to any physical server on which engineering server software or operator server software is hosted.

D.95. High availability

It refers to an availability of 99,999% or better. This translates into a downtime, including both scheduled and unscheduled maintenance of less than 5 minutes per year.

D.96. Network & computer equipment

It collectively refers to the network and computer equipment used in the DCS.

D.97. Network cabling

It refers to all the cabling that forms part of the communication networks.

D.98. Network equipment

It collectively refers to network switches, media converters, and patch panels.

D.99. Operating and engineering network

It is a subsystem of the communication network and refers specifically to the communication layers through which the operator system communication and engineering system communication occurs. The

CONTROLLED DISCLOSURE

operating & engineering network and automation network may be integrated such that both networks use the same physical network.

D.100. Operational technology

It refers to the equipment used to operate, monitor and control the process plant. It collectively refers to all control system technologies, including DCS, PLC, SCADA and SIS.

D.101. Patch cable

It is flexible network cable with connectors on both ends that is used to connect a network device to a patch panel. Patch cables are usually relatively short (generally no more than two metres in length).

D.102. Patch panel

It is a cable management hardware device via which infrastructure or backbone cables are interconnected to patch cables.

D.103. Supplementary system server

It refers to any physical server on which supplementary system server software is hosted.

2.4 ABBREVIATIONS

The abbreviations provided in this section apply throughout this multipart document.

Abbreviation	Explanation
24/7	24 hours a day, 7 days a week
AI	Analog input
AKZ	"Anlagenkennzeichnungssystem" (Plant Designation System)
ALMS	Alarm management system
AO	Analog output
ASMS	Asset management system
AU	Automation unit
BI	Binary input
BO	Binary output
BOP	Balance of plant
BPS	Boiler protection system
C&I	Control and instrumentation
COTS	Commercial-off-the-shelf
CPU	Central processing unit
DCOM	Distributed component object model
DCS	Distributed control system
DMS	Document management system
DMZ	Demilitarised zone
DVD	Digital versatile disc
ELSP	Electronic security perimeter
FAT	Factory acceptance test
FG	Function group
FMEA	Failure mode and effects analysis
FMECA	Failure mode, effects and criticality analysis
F/O	Fibre optic
GA	General Arrangement
GC	Group control
GPS	Global positioning satellite
GUI	Graphical user interface
HDD	Hard disk drive
HIDS	Host intrusion detection system
HMI	Human machine interface
HVAC	Heating, ventilation and air conditioning
IO or I/O	Input / output
IP	Ingress Protection
IPS	In-plane switching
KKS	Kraftwerk kennzeichen power plant coding system

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.

Abbreviation	Explanation
LAN	Local area network
LCC	Life cycle costing
LCD	Liquid crystal display
LCP	Local control panel
LCS	Local control station
MCR	Maximum continuous rating
MDT	Mean down time
MTBF	Mean time between failures
MTTF	Mean time to failure
MTTR	Mean time to repair
NIDS	Network intrusion detection system
ODBC	Open database connectivity
OEM	Original equipment manufacturer
OPC	Object linking and embedding for process control
OT	Operational Technology
PC	Personal computer
PDU	Power distribution unit
PI	Power Island
PIS	Plant information system
PLC	Programmable logic controller
PS	Power station
RAID	Redundant array of independent disks
RAM	Reliability, availability, maintainability
SAN	Storage area network
SCADA	Supervisory control and data acquisition
SER	Station electrical reticulation
SIF	Safety instrumented function
SIL	Safety integrity level
SIS	Safety instrumented system
SNTP	Simple network time protocol
SQL	Structured query language
TCP/IP	Transmission control protocol/internet protocol
TPS	Turbine protection system
UPS	220V Uninterruptible power supply
USB	Universal serial bus
UTC	Coordinated universal time
UTM	Unified threat manager
VLAN	Virtual local area network
WAN	Wide area network
WLAN	Wireless local area network

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.

Abbreviation	Explanation
WTP	Water Treatment Plant

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. OVERALL REQUIREMENTS

What is a DCS?

A distributed control system (DCS) consists of multiple control, operating and communication elements that are interconnected to provide an integrated control and operating platform for a process plant. The main elements of a DCS are the microprocessor-based controllers (which are functionally and/or geographically distributed); input/output (I/O) cards; communication networks; and the human-machine interface (HMI). In a DCS control tasks are usually distributed amongst multiple controllers and the process is supervised via operators through the HMI. Communication between the DCS and the physically plant (sensors, actuators, motors, etc.) typically occurs through the I/O cards. A DCS is usually designed with redundant components to enhance the reliability and availability of the control system. Figure 4 illustrates the basic configuration and components of a DCS. It shows an overview of a typical DCS, including the major subsystems, and division between the centralised and control island dedicated DCS equipment.

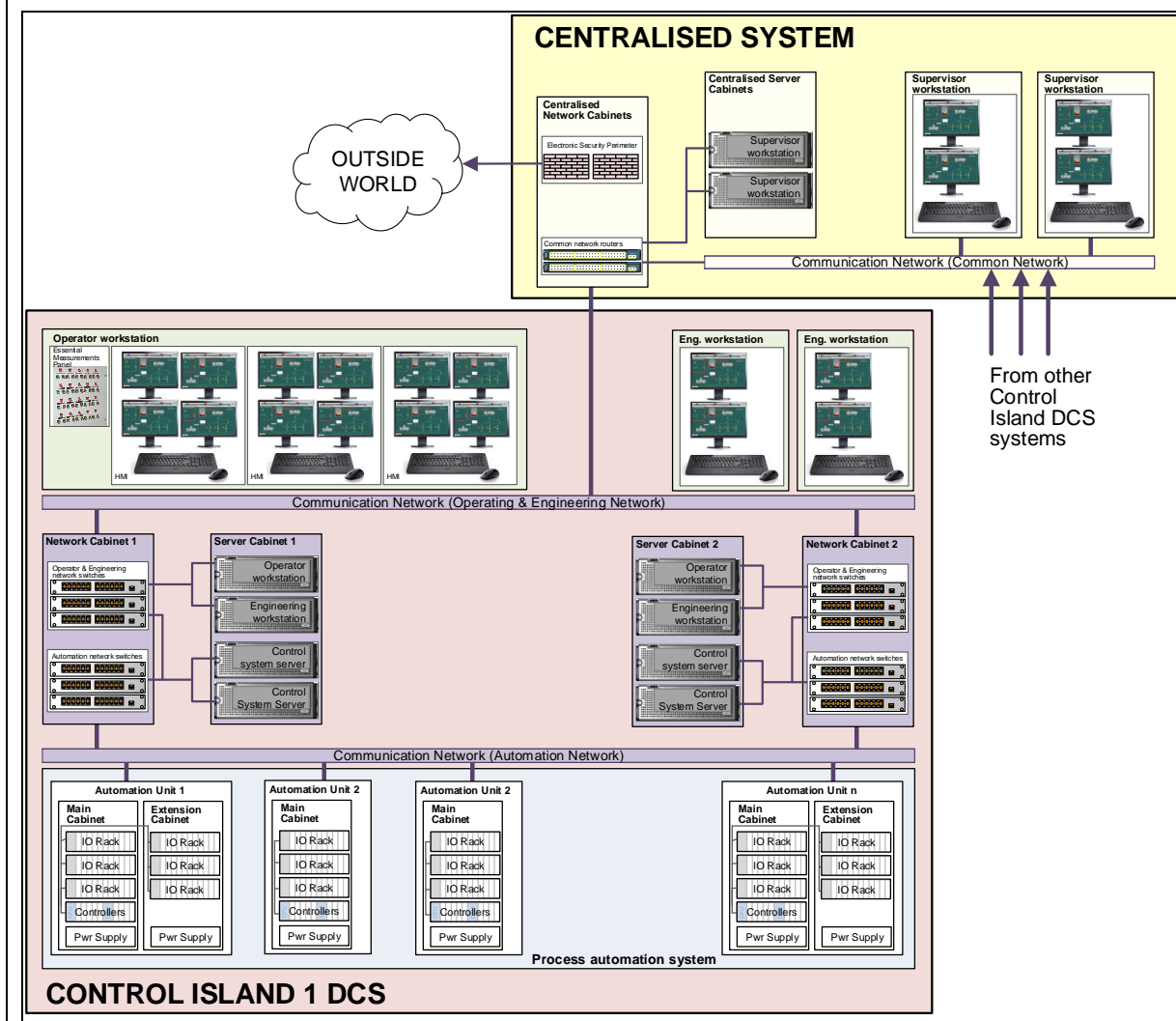


Figure 4: A typical DCS structure

The terms shown in Figure 4 are defined in section 3.2 of this 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.

4.1 GENERAL

4.1.1 The DCS should be a fully operational control system that is functional in all aspects and that is implemented in a consistent and integrated manner.

4.1.2 The DCS can protect, control and operate the power plant in all operating modes.

4.1.3 The DCS should comply with professional engineering practices and standards for control systems used in the process industry.

4.1.4 The DCS can perform the following functions:

- a. Signal acquisition, conditioning and validation;
- b. Process interlocking and plant protection;
- c. Closed loop, open loop, sequence and group control;
- d. Signal exchange with external systems;
- e. Process supervision and monitoring;
- f. Alarm handling and management;
- g. Engineering and diagnostics.

4.1.5 The DCS shall consist of the following subsystems as shown in Figure 5:

- a. Operator system (specified in Part 2);
- b. Supervisor system (specified in Part 2);
- c. Engineering system (specified in Part 3);
- d. Automation system (specified in Part 4);
- e. Network and computer equipment (specified in Part 5);

4.1.6 Subsystems for supplementary control system functions may also be integrated within the DCS.

Example 1

An *asset management system*, *time synchronisation system*, *plant information system* and *backup & restore system* are some examples of additional subsystems whose functions may be integrated into a DCS. These systems are not required to perform the core DCS functions (that of control, supervision, engineering and diagnostics) and are therefore considered auxiliary or supplementary DCS subsystems.

4.1.7 The DCS may also contain protection automation systems dedicated to the protection of specific areas of plant.

Example 1

The *boiler protection system* and *turbine protection system* are examples of dedicated safety systems. Depending on the capabilities of the DCS supplier, the configuration and need of the power plant concerned, and the specific functions required of the protection automation system; these systems may be contained within the DCS or be external to the DCS (i.e. provided as a standalone system).

CONTROLLED DISCLOSURE

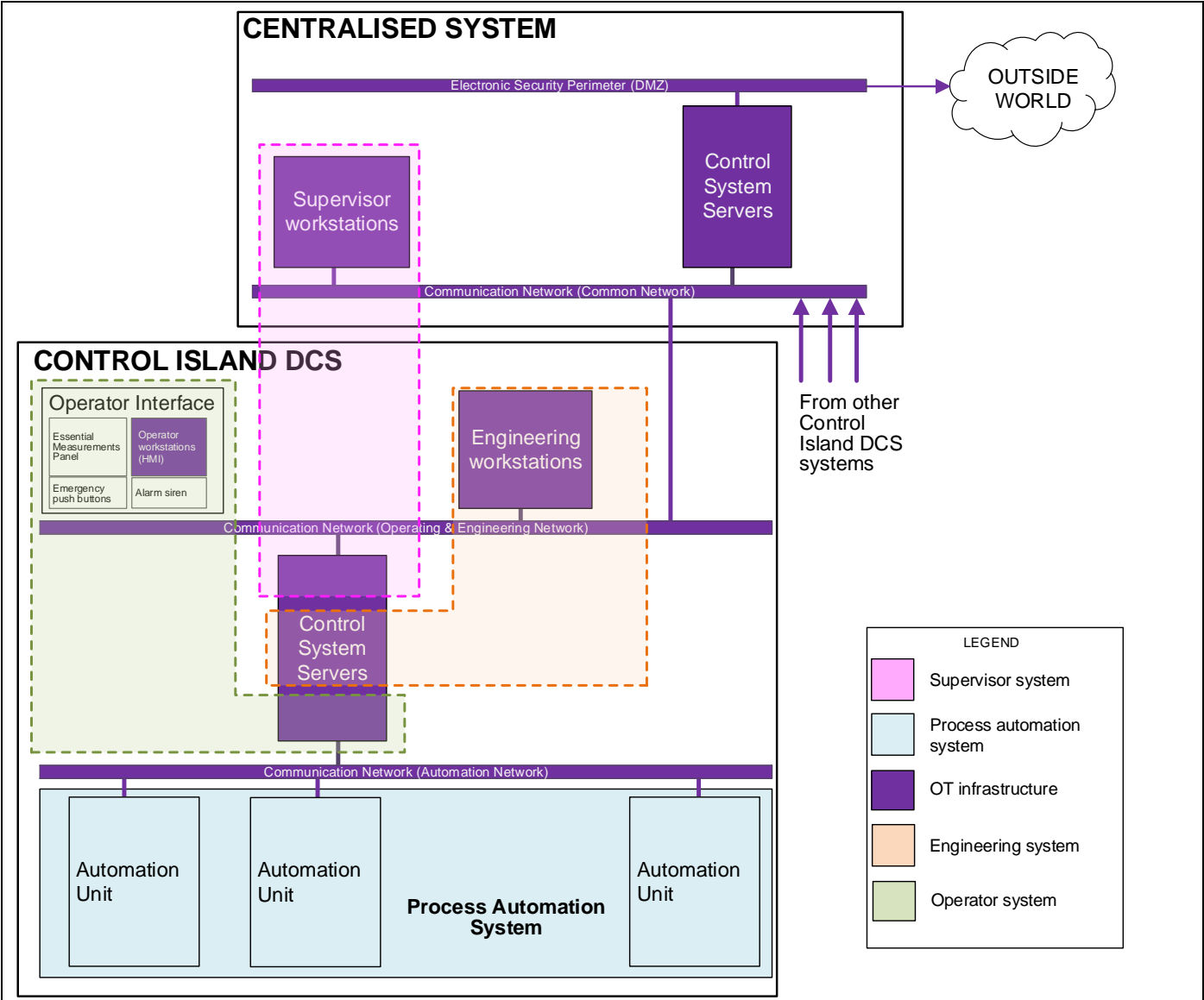


Figure 5: Definition of the DCS subsystems

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. KEY PERFORMANCE REQUIREMENTS

5.1 PROVEN-IN-USE

5.1.1 The DCS shall be a proven-in-use power plant control system that has an installed base of more than three year in the following subsystems of commercially operated power plants:

- a. 600MW or larger Boiler/Steam-generators and related auxiliaries;
- b. 600MW or larger Turbo-generator auxiliaries;
- c. Water treatment and distribution systems;
- d. Coal and ash handling systems.

5.1.2 No technology or equipment unproven in a commercially operated power plant shall be used within the DCS.

5.2 AVAILABILITY

5.2.1 A single failure in the DCS shall not:

- a. Endanger the safety of people or plant;
- b. Cause a load loss of more than 50% MCR in a power island;
- c. Result in a discretionary power island trip by a plant operator;
- d. Result in the loss of balance of plant services to a power island.

5.2.2 Any two failures in the DCS shall not:

- a. Cause the trip of two or more power islands within a one hour window.

To achieve this requirement, particular care must be taken in the design of the balance of plant DCS to ensure that any critical plant systems (being BOP services which if lost, could result in multi-unit trips e.g. cooling water) are adequately segregated (i.e. separated from each other) and functionally distributed within the DCS.

5.3 RELIABILITY

5.3.1 The availability of the DCS over its life in percentage of time shall be 99.99% or greater measured annually. The DCS is only considered available when it does not disrupt the plant or result in a load loss.

An availability of 99.99% translates to a downtime or unavailability of the DCS for 52.56 minutes per year.

5.3.2 The redundancy scheme of redundant equipment is self-monitoring such that the transfer to the back-up shall be bump-less, seamless and shall occur without human intervention; without disruption to the C&I system and/or plant; and without loss of any information.

5.3.3 The DCS shall be designed on the basis of a MTTR of:

- a. 24 hours for all servers and computers;
- b. 8 hours for all other DCS equipment.

Achieving the above MTTR requires effective alarming, sufficient diagnostic functions, and a spares strategy which supports the required repair time. Another item to consider when designing the DCS solution is the required skills and knowledge. Sometimes an initially more expensive solution can be

CONTROLLED DISCLOSURE

more cost effective over the life of the product due to the reduced amount on required expertise and scarce resources to maintain the systems.

5.4 MAINTAINABILITY

5.4.1 The DCS shall be configured such that it can be maintained while on-load.

5.4.2 All redundant equipment shall be hot swappable and both the DCS and the on-load plant shall not be disrupted by the replacement of redundant equipment.

5.5 SEGREGATION

The objectives of these clauses are to ensure that each control island's DCS is self-contained and that no equipment is shared between control islands. The intent of which is to ensure that even in the event of multiple failures within a control island's DCS; the failures are contained within the control island concerned and do not compromise the performance of other control islands.

5.5.1 Each control island shall contain its own DCS.

5.5.2 Each control island's DCS shall be autonomous and shall not share any equipment with any other control island's DCS.

5.6 EXTERNAL SIGNAL EXCHANGE

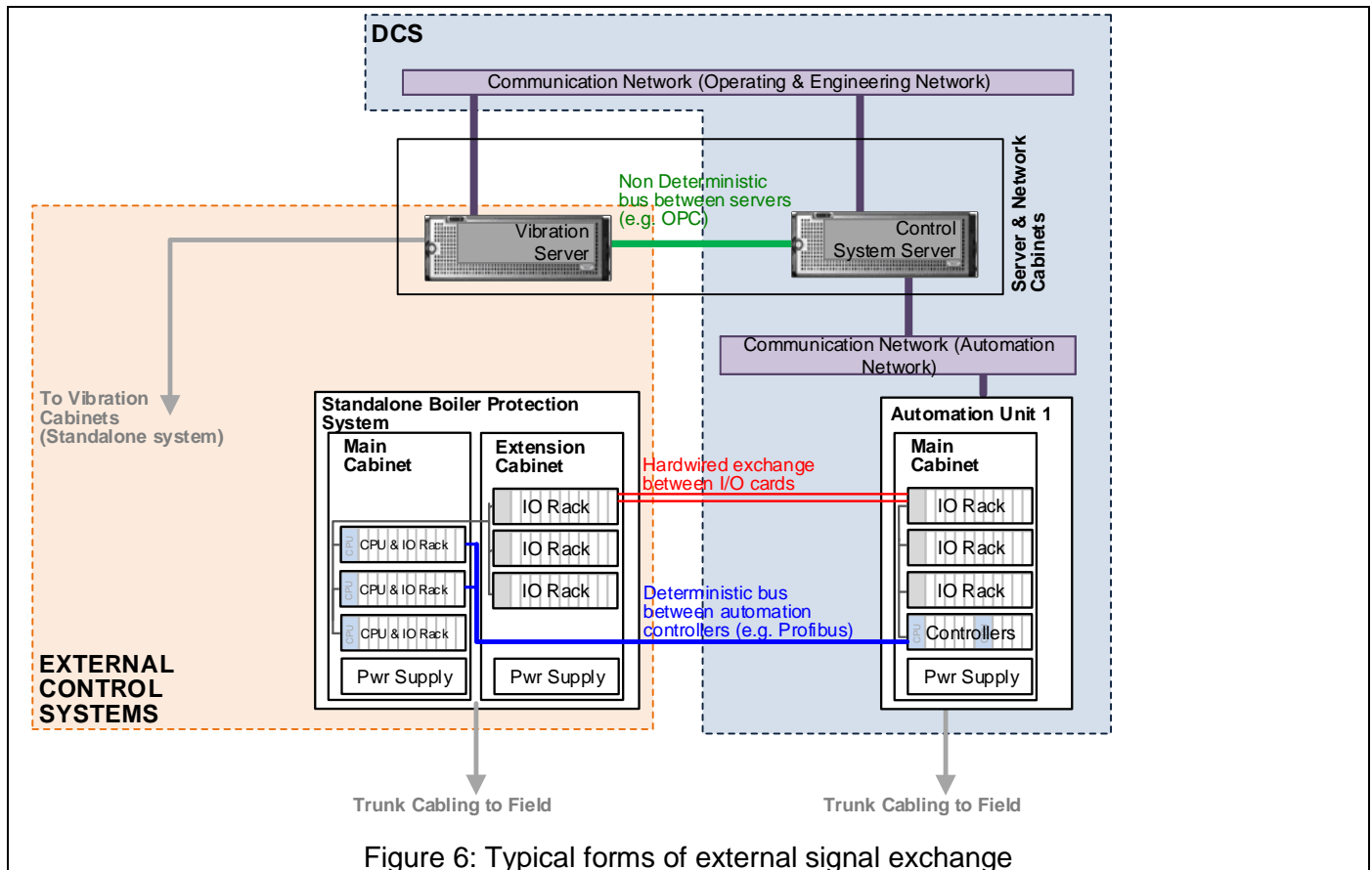
External signal exchange refers to signal exchanges between the DCS and a black-box. These signal exchanges can be required for a variety of reasons such as plant protection, control purposes, plant supervision, archiving or non-critical information display.

Ideally, signal exchange should occur at the automation layer directly between the automation systems. However, when the quantity of signals required to be exchanged is high this may be impractical and a layered approach to signal exchange is needed; with the most critical signals being exchanged at the lowest layer (automation layer), and least critical signals at higher layers (e.g. the communication layer). An example of the typical external signal exchanges that occur between a DCS and other control systems is shown in Figure 6.

The objective of the following clauses is to restrict the signal exchange to particular subsystems or communication medium depending on the criticality of the signal exchange and the consequence of failures in the signal exchange.

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.



5.6.1 Signals exchange between a DCS and a black-box shall be hardwired between the applicable automation units when it is for the purpose of:

- a. Plant protection;
- b. Closed loop control.

A black-box may be another DCS or a standalone system:

Example 1: The signal exchange between the Unit 1 DCS and BOP DCS (each DCS being a black-box in reference to each other).

Example 2: The signal exchange between the Unit 1 DCS and Unit 1 Turbine standalone protection system.

5.6.2 Signals exchange between a DCS and a black-box shall be hardwired or through a redundant deterministic bus between the applicable automation units when it is for the purpose of:

- a. Sequence control;
- b. Group control.

"Deterministic" means that the worst-case response time of the signal transmission is known. The Profibus and Modbus communication protocols are generally considered as deterministic. To ensure the integrity of the control tasks, it is important that this signal exchange occurs over a deterministic bus and that it occurs at the automation layer.

5.6.3 Signals exchange between a DCS and a black-box may occur through a redundant non-deterministic bus when it is for the purpose of:

- a. Alarms;

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.

- b. Operator commands;
- c. Operator feedbacks;
- d. Information and archiving.

5.6.4 Signals exchanged between a DCS and a black-box shall be galvanically isolated.

5.7 INTERNAL SIGNAL ACQUISITION

Internal signal acquisition refers to signals directly exchanged between the DCS and field devices (actuators, instruments, switchgear, etc....) with no black-box involved in the loop.

5.7.1 Signals exchanged between field devices and the DCS shall be hardwired.

5.7.2 Signals exchanged between the switchgear and the DCS shall be hardwired to the applicable automation units when it is for the purpose of:

- a. Plant protection;
- b. Closed loop control;
- c. Sequence control;
- d. Group control;
- e. Operator commands;
- f. Operator feedbacks.

5.7.3 Signals from the switchgear to the DCS may be acquired through a communication network when it is for the purpose of:

- a. Alarms;
- b. Information and archiving.

Why a different approach to the acquisition of field devices/switchgear signals from that of external systems?

In a power plant there are typically a few black-boxes (typically < 10 per control island), each with a high quantity of I/O (typically hundreds). Conversely, there are usually a high quantity of field devices (typically thousands) and switchgear (typically hundreds) each with few I/O (typically < 10 per device). Therefore, to reduce design complexity the interface between field devices/switchgear and the DCS are standardised regardless of how the signals from the devices are used. Standardisation of the interfaces means simpler designs and reduced human errors during maintenance.

5.8 LIFE EXPECTANCY

5.8.1 All DCS equipment shall be supported and maintainable for a minimum of 15 years after the start of commercial operation.

5.8.2 At the start of commercial operation, the DCS shall be in the active phase of its product life cycle.

5.8.3 At the start of commercial operation, no DCS equipment shall be in the end of life or obsolescence phase of its product life cycle.

5.9 SUPPORTABILITY

5.9.1 The DCS shall not be modified or adapted from its standard and proven configurations to the extent that future upgrades require customisation and special adaptations before implementation.

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.

5.9.2 The DCS shall be configured in accordance with its product specifications and the OEM's design guides and standards.

5.10 OEM INVOLVEMENT

The objectives of these clauses are to ensure to the original equipment manufacturer (OEM) of the DCS takes full ownership of the design, engineering, technology selection and integration of the DCS with the specific intent of reducing the risk of non-performance of the DCS and its subsequent detrimental impact on the power plant.

5.10.1 The OEM's representatives shall be directly involved in the engineering, testing and installation of the DCS and the application software.

5.10.2 The OEM shall take overall accountability for the DCS and the engineered application software.

5.11 ENVIRONMENTAL CONDITIONS

Only the functional environmental requirements are provided here. The rooms available to house DCS equipment will vary at each power plant. As such, the specific requirements related to room locations have not been specified in this document and should be specified elsewhere.

5.11.1 In addition to the requirements specified in this document, the environmental conditions under which the DCS is operated and stored shall comply with the requirements of the Eskom environmental conditions for process control Equipment standard, 240-56355731.

5.11.2 The ingress protection (IP) rating of all enclosures in which DCS equipment is installed shall be IP52 or better.

IP52 requires the enclosures to be dust protected and protected against dripping water when tilted up to 15°.

5.12 INTEGRATION AND CONSISTENCY OF DESIGN

5.12.1 The subsystems of the DCS should be seamlessly integrated such that from a user perspective it is one system.

5.12.2 Uniformed signal descriptions and abbreviations shall be used throughout the DCS.

5.12.3 Any configuration changes to a signal's properties such as the KKS code; signal long description, signal short description, I/O assignment, threshold(s), state message(s), alarm level(s) and range(s) shall be made once and reflected correctly in all subsystems (operator system, supervisor system, engineering system and the automation system).

5.13 STANDARDISATION

5.13.1.1 The DCS equipment should be standardised to the extent possible, while still ensuring proven products are used and the performance characteristics of the DCS are not compromised.

5.13.1.2 Only one version of each type of equipment shall be used in the DCS.

This does not mean that different models or variations of a product cannot be used. For example both an 8-channel BI card model and a 16-channel BI card model can be used in the DCS. What the above clause requires is that the hardware and software version of each 8-channel BI card used is the same

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.

throughout the DCS. For example it is not allowed that some 8-channel BI cards have hardware version 1.1 and the remaining 8-channel BI cards have hardware version 1.2.

5.13.1.3 The objectives of standardisation shall be as follows:

- a. Reduced life cycle cost/cost of ownership cost.
- b. Interchangeability of equipment.
- c. Reduced spares holding requirements.
- d. Reduced training requirements of different systems.

5.13.1.4 The following equipment should be standardised to one product or one family of products:

- a. Small & large screens;
- b. KVMs;
- c. Workstations;
- d. Control system servers;
- e. Network switches;
- f. Network cables;
- g. Cabinets, patch panels, marshalling cabinets;
- h. Controllers;
- i. I/O cards;
- j. Cabinet power supplies and power distribution facilities.

5.14 RESPONSE TIMES

The following clauses define the response times required from the DCS to ensure the operability of the plant. The input display time is the time delay from the acquisition of a signal by the DCS (through an input card) until it is displayed to the operator. The output command time is the time delay from the issuing of a command from the operator until it is outputted from the DCS (through an output card or drive card). Note the time delay between the I/O cards and the field devices are negligible in that these are direct hardwired links. The response times are diagrammatically illustrated in Figure 7.

5.14.1 The output command time, being the total time taken from the issuing of an operator command via a faceplate to a signal change on the output card shall not exceed 0.5 seconds.

5.14.2 The input display time, being the total time taken from a signal change on a binary or analog input card to the update of the relevant HMI graphics page(s) shall not exceed 1.5 seconds.

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.

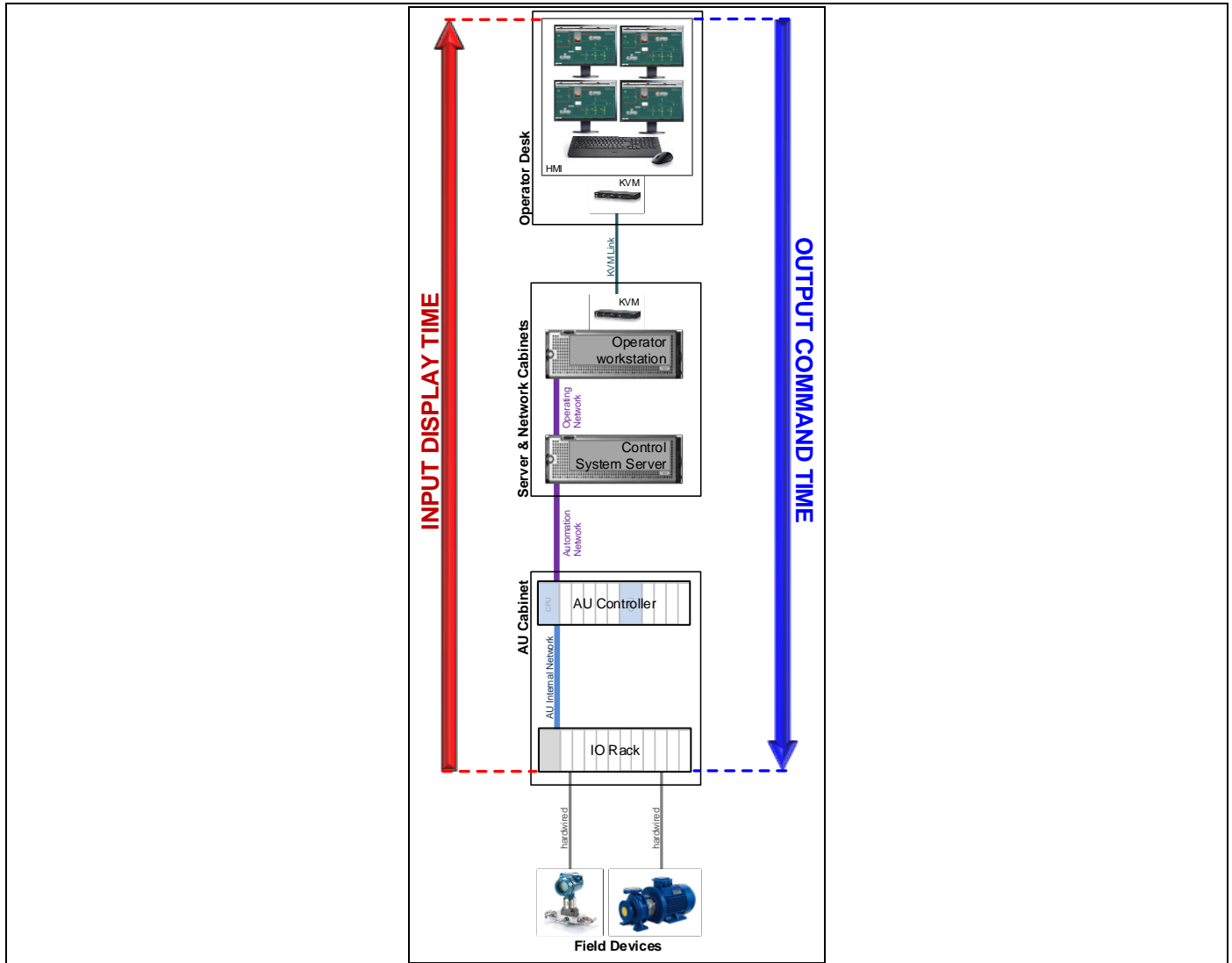


Figure 7: Illustration of response times in a DCS

The above is required to take into account peak traffic periods in the DCS such as power island disturbances and unit trips.

5.15 CONTROL TASKS

5.15.1 In addition to the requirements specified in this document, control tasks shall comply with the requirements and recommendations of the VGB automation function design standard, VGB R 170 B2e.

5.15.2 The DCS shall include control tasks that can protect, control, operate and supervise the power plant in all operating modes, including the following:

- Preparation for start-up;
- Start-up (cold, warm or hot);
- On-load;

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.

- d. Shut-down;
 - e. Operation during incidents, namely:
 - i. Grid incidents (high power demand, house-load operation and full load rejection);
 - ii. Turbine tripping;
 - iii. Failure of a major auxiliary leading to runbacks;
 - iv. Station blackout;
 - v. Under-voltage.
- 5.15.3 The control tasks can maintain control of the process within the normal operating envelope of the plant and shall alarm the operator when the process deviates from the operating envelope limits.
- 5.15.4 All control tasks for closed loop control shall be executed at the automation layer within the automation system.
- 5.15.5 The control tasks can be executed in a supervised fully automatic control mode.

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
P. Madiba	Senior Manager, EC&I
M. Khumalo	Senior Manager, Electrical and C&I PEI (Acting)
C. Boesack	Chairperson, Power Plant C&I SC
X. Sibozza	Middle Manager, C&I Design Application
P. du Plessis	Chief Technologist, PEIC C&I

7. REVISIONS

Date	Rev.	Compiler	Remarks
November 2016	0.2	P Govender	Draft of this document circulated for first round of comments.
November 2016	0.3	P Govender	Main changes made: <ul style="list-style-type: none">Added a block diagram to explain external signal exchange.Added a block diagram to explain response times.Added a section on internal signal acquisition.
November 2017	0.4	P Govender	Main changes made: <ul style="list-style-type: none">Updated the document with comments received.Renamed Part 5 and redefined some terminology based on changes to other parts.
February 2018	0.5	P Govender	Main changes made: <ul style="list-style-type: none">Updated the document with comments received.
November 2018	0.6	P Govender	Main changes made: <ul style="list-style-type: none">Revised, reformatted, updated with comments.Added document number.
January 2019	1	P Govender	Final Document for Authorisation and Publication

8. DEVELOPMENT TEAM

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

- Pravin Govender

9. ACKNOWLEDGEMENTS

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

- Cornelius Visagie;
- Jorge Nunes;
- Nerino Barrufa;
- Paul Du Plessis.

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.