Eskom	Specification	Generation

Title:	**Kusile Smart Plant Digitalisation and Artificial Intelligence**	Unique Identifier:	**KUS-20251198**
		Alternative Reference Number:	**N/A**
		Area of Applicability:	**Engineering**
		Documentation Type:	**Functional Specification**
		Revision:	**2**
		Total Pages:	**49**
		Next Review Date:	**as required**
		Disclosure Classification:	**CONTROLLED DISCLOSURE**

Compiled by	**Functional Responsibility**	**Authorised by**
……..	……..	……..
Date: ……	Date: ……	Date: ……

CONTENTS

Page

1. INTRODUCTION 4

1.1 STRATEGIC OBJECTIVES 4
1.2 BACKGROUND OF KUSILE POWER STATION 4
1.3 TECHNOLOGY AVAILABLE AT KUSILE POWER STATION 5

2. SUPPORTING CLAUSES 6

2.1 SCOPE 6
2.1.1 Purpose 6
2.1.2 Applicability 6
2.2 NORMATIVE/INFORMATIVE REFERENCES 6
2.2.1 Normative 6
2.2.2 Informative 7
2.3 DEFINITIONS 7
2.3.1 Disclosure Classification 9
2.4 ABBREVIATIONS 9
2.5 ROLES AND RESPONSIBILITIES 11
2.6 PROCESS FOR MONITORING 12
2.7 RELATED/SUPPORTING DOCUMENTS 12

3. ENGINEERING AND THE *CONTRACTOR*'S DESIGN 12

3.1 *EMPLOYER*'S DESIGN 12
3.1.1 Engineering and Design 12
3.1.2 Construction and Commissioning 12
3.1.3 Operations and Maintenance 12
3.1.4 Asset Performance Management (APM) 12
3.1.5 Cybersecurity and Data Integrity 13
3.1.6 Digitalisation Strategy Framework 13
3.2 PARTS OF THE *WORKS* WHICH THE *CONTRACTOR* IS TO DESIGN 13
3.2.1 System Architecture and Integration 13
3.2.1.1 Pillar 1: Network and Infrastructure 13
3.2.1.2 Technical Requirements 14
3.2.1.2.1 Technical Requirements for network infrastructure 14
3.2.1.2.2 Technical Requirements for cloud storage 16
3.2.1.2.3 Key Deliverables 17
3.2.1.3 Pillar 2: Intelligent Inspection and Digital Interaction 18
3.2.1.3.1 Technical Requirements 18
3.2.1.3.2 Key Deliverables 21
3.2.1.4 Pillar 3: Digital Twin Interface and Integration 22
3.2.1.4.1 Technical Requirements 22
3.2.2 Key Deliverables 24
3.2.2.1 Pillar 4: Paperless Operations / Digitalised Routine Work Management (RWM) and Outage Functions 25
3.2.2.1.1 Technical Requirements 25
3.2.2.1.2 Key Deliverables 27
3.2.2.2 Pillar 5: Digitization of Existing Plant Documents and Data Books 28
3.2.2.2.1 Technical Requirements 28
3.2.2.2.2 Key Deliverables 30
3.2.2.3 Functional and Non-Functional Requirements 31
3.2.2.3.1 Global Market and Standards Compliance 31
3.2.2.3.2 International Standards Compliance 31
3.2.2.3.3 Technology Agnosticism 32
3.2.2.3.4 Multi-language Support 32
3.3 CONTRACTOR DESIGN, DOCUMENTATION AND ACCEPTANCE REQUIREMENTS 32

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.

3.4 MONITORING, BENEFITS AND KPI REQUIREMENTS 33
3.5 INTELLECTUAL PROPERTY (IP) AND AI APPRENTICESHIP PROGRAMME (AIAP) 34
3.5.1 IP Ownership and Criteria 35
3.5.2 AI Apprenticeship Programme (AIAP) Integration 36
3.6 NON-FUNCTIONAL REQUIREMENTS 38
3.6.1 Interfaces 39
3.6.2 Expected Benefits and KPIs 39
3.7 PROCEDURE FOR SUBMISSION AND ACCEPTANCE OF *CONTRACTOR*'S DESIGN 40
3.7.1 Documentation Requirements 40
3.7.2 The Contractor shall ensure that documents have the following minimum attributes on the cover page: 40
3.7.3 The following additional attributes are important for technical documents: 41
3.7.4 Format and Layout of Documents 41
3.7.5 Layout and Typography 41
3.7.6 Document Headers 41
3.7.7 Naming of files 41
3.7.8 Documentation Submissions 41
3.8 OTHER REQUIREMENTS OF THE *CONTRACTOR*'S DESIGN 46
3.9 USE OF *CONTRACTOR*'S DESIGN AND INTELLECTUAL PROPERTY 46
3.10 DESIGN OF EQUIPMENT 47
3.11 EQUIPMENT REQUIRED TO BE INCLUDED IN THE *WORKS* 47
3.12 AS-BUILT DRAWINGS, OPERATING MANUALS AND MAINTENANCE SCHEDULES 47
3.13 TRANSMITTAL NUMBER PLANT AND MATERIALS 48
3.13.1 Quality 48
3.13.2 Plant and Materials provided "free issue" by the *Employer* 48
3.13.3 Spares and consumables 48

4. AUTHORISATION 48

5. REVISIONS 49

6. DEVELOPMENT TEAM 49

7. ACKNOWLEDGEMENTS 49

FIGURES

Figure 1: Kusile Power Station 5

TABLES

Table 1: Technology Available at Kusile Power Station 5

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

This document outlines the Scope of Work (SOW) and the Execution Plan for the Smart Plant Digitalisation Initiative. The purpose is to provide a comprehensive technical and strategic framework for potential service providers to submit proposals for the design, implementation, and integration of advanced digital technologies at Kusile Power Station.

The Smart Plant Initiative establishes a fully integrated digital ecosystem across engineering, control, and business systems. This ecosystem leverages real-time data acquisition, artificial intelligence-based analytics, and immersive technologies to enable predictive and prescriptive maintenance, enhance operational efficiency, improve safety compliance, and develop a highly skilled and adaptable workforce.

1.1 Strategic Objectives

This initiative addresses five core strategic objectives:

- **Operational Efficiency**: Reduce unplanned downtime through predictive maintenance capabilities, optimise resource allocation, and streamline maintenance workflows through digital processes.
- **Safety and Compliance:** Enhance safety protocols through automated inspection systems, real-time monitoring, and compliance tracking, while maintaining comprehensive audit trails for regulatory requirements.
- **Data-Driven Decision Making:** Establish a unified data platform that integrates operational, maintenance, and business data, enabling informed decision-making at all organisational levels.
- **Workforce Development (Digital transformation):** Provide immersive training experiences through virtual reality and augmented reality platforms, enabling rapid skill development and knowledge transfer across the organisation.
- **Future-Ready Infrastructure:** Implement a scalable, standards-compliant technology foundation that supports future innovations and integrates seamlessly with existing enterprise systems.

1.2 Background of Kusile Power Station

The Kusile Power Station is a cornerstone of South Africa's energy infrastructure, representing a significant investment in modern, high-capacity coal-fired generation. Its design incorporates advanced technologies that set it apart from older facilities, and it is a key component in the broader strategy by Eskom to modernise the national grid through digitalization and the transition to a "smart plant" operational model.

Located in the Mpumalanga Province of South Africa, Kusile is one of the largest coal-fired power stations globally and was the country's largest infrastructure project during its construction. The station, operated by Eskom, has a total installed capacity of 4,800 MW, generated by six individual units, each rated at 800 MW.

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: Kusile Power Station

The project reached a major milestone with the commercial operation of its final unit (Unit 6) in late September 2025, completing the station. Kusile is designed for a substantial operational lifespan of approximately 50 years, underscoring its long-term role in South Africa's energy security.

1.3 Technology Available at Kusile Power Station

Kusile's technology is notable for its focus on high efficiency and reduced environmental impact, making it a benchmark for cleaner coal technology on the African continent. The two most critical technologies employed are Supercritical (USC) steam generation and Flue Gas Desulphurisation (FGD).

Table 1: Technology Available at Kusile Power Station

Technology	Description	Significance
Supercritical (SC) Technology	The station utilises SC boilers, which operate at extremely high pressures and temperatures, exceeding the critical point of water.	This high-efficiency operation allows the plant to generate more power with less coal consumption, resulting in a lower carbon footprint and reduced greenhouse gas emissions per megawatt-hour compared to older sub-critical power plants.
Wet Flue Gas Desulphurisation (WFGD)	Kusile is the first power station in South Africa to be fitted with WFGD technology. This process uses a wet limestone-gypsum mixture to chemically remove up to 90% of sulphur dioxide from the flue gas before it is released.	The implementation of WFGD is a critical step in aligning the station with stringent national and international air quality standards, significantly reducing a major source of air pollution.
Fabric Filter Plants	High-resistant fabric filter bags are installed to capture particulate matter (fly ash) from the flue gas.	This ensures compliance with air quality regulations by minimising the release of solid particles into the atmosphere.

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 Statement of Work includes the design, procurement, implementation, integration, testing, training, and handover of five integrated technology pillars, which will be delivered in sequential phases as outlined below:

Phase 1:

- Network & Infrastructure.
- Intelligent Inspection and Digital Integration.
- Digital Twin Interface.

Phase 2:

- Paperless Operations (Digitised Routine Work Management) with integration into SAP Functions (PM/MM).
- Digitization of Existing Plant Documents and Data Books

The scope covers all necessary hardware, software, professional services, and training required to achieve full operational capability. The costing and deliverables should be phased. Ongoing operational support beyond the initial three-month post-go-live period is not included and will be addressed through separate service level agreements.

2.1.1 Purpose

The purpose of the functional specifications is to:

- Create a fully integrated digital ecosystem across engineering, control, and business systems.
- Implement real-time plant monitoring and AI-based analytics for predictive and prescriptive maintenance. Interface of related history into SAP and existing plant forms to be in place
- Enable mobile and remote access to live plant data for engineering and maintenance teams with authorised controlled access.
- Improve data governance, cybersecurity, and traceability of operational decisions.

2.1.2 Applicability

This document shall apply throughout Kusile Power Station.

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] ISO 9001 Quality Management Systems.

[2] IEC 62443 Cyber Security Standard.

[3] IEC 62351 Secure utility communications.

[4] IEC 62264 OT/IT Integration.

[5] IEC 62541 Industrial Interoperability.

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] IEC 61850 Electrical Integration.

[7] IEC 62351 Utility Communications Security.

[8] IEC 61511 Functional Safety.

[9] IEC 60870-5-104 Existing Eskom interfaces.

[10] ISO 55001 Asset Management.

[11] ISO 27001 Information Security.

[12] 240-44175132 Eskom Personal Protective Equipment (PPE)

2.2.2 Informative

[13] 240-71432150: Plant Labelling and Equipment Standard.

[14] 240-76992014: Project/Plant Specific Technical Documents and Records Management Work Instruction.

[15] 240-53113685: Generation Design Review Procedure.

[16] 240-86973501: Engineering Drawing Standard Common Requirements.

2.3 Definitions

Definition	Description
Digital Twin	A virtual representation of a physical asset or process used for monitoring, simulation, and optimization.
Digitization	A process of converting information, signals, or physical assets from an analog or physical format into a digital format that can be stored, processed, transmitted, and analyzed by computers.
Predictive Maintenance	Maintenance strategy that uses condition monitoring and analytics to predict equipment failures before they occur.
Edge Computing	Processing data close to the source of generation rather than in a centralized data center.
Historian	A database that stores time-series operational data from industrial control systems.
Digitalisation / Smart Plant Digitalisation	The process of integrating digital technologies such as sensors, AI, and analytics into power plant operations to improve performance, reliability, and efficiency.
Asset Performance Management (APM)	A suite of tools that optimize asset reliability, availability, and performance using analytics and maintenance data.
Certificate of Compliance (CoC)	A document confirming that installations or equipment comply with applicable codes and standards.
Change Management	A systematic approach to controlling modifications to design, scope, or project configuration.
CMMS (Computerized Maintenance Management System)	Software used to plan, track, and manage maintenance activities and work orders.
Cybersecurity / Data Integrity	Protection of systems and data from unauthorized access, ensuring accuracy and trustworthiness of information.

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.

Definition	Description
Data Governance	The framework of policies and standards that ensure data integrity, quality, and security across the plant systems.
Data Lake	A centralized repository that stores structured and unstructured data for analysis and integration.
Demilitarized Zone (DMZ)	A secure network segment that isolates operational technology from external networks for cybersecurity purposes.
Design Authority	The party responsible for ensuring design quality, integrity, and compliance with standards.
Design Review Procedure	A formal process to assess and verify design compliance, functionality, and quality before approval.
Digital Twin	A virtual replica of physical assets, systems, or processes used to simulate, analyse, and optimize real-world performance.
Engineering Database	A structured digital repository for storing engineering data, drawings, and metadata.
Free Issue Material	Material or equipment provided by the employer to the contractor at no cost for project use.
Intelligent Inspection	Automated or semi-automated monitoring using sensors, cameras, and analytics for plant and safety inspections.
OLEDB	A Microsoft data access interface used to connect and retrieve data from different databases.
OPC UA / Modbus / MQTT	Communication protocols used for secure and reliable data exchange between devices and systems.
OSIsoft PI System	A real-time data infrastructure platform that collects, stores, and analyses operational data.
Paperless Operations / Digitalised Routine Work Management (RWM)	Use of handheld and digital tools to manage maintenance and operational tasks electronically, reducing manual paperwork.
PI Vision	A visualization tool from OSIsoft used to display real-time plant and equipment performance data.
Power BI	A business analytics tool used for creating interactive visual reports and dashboards.
Predictive Analytics	Data-driven analysis used to forecast potential failures or performance issues before they occur.
Prescriptive Maintenance	An advanced maintenance approach that uses AI to recommend optimal maintenance actions based on predictive insights.
REST API	An interface that allows communication between software systems using standard HTTP methods.
SAP (PM/MM/CMMS modules)	Enterprise software modules used for plant maintenance, materials management, and computerized maintenance management.
Unified Data Backbone	The integrated data framework that connects all systems from sensors to enterprise-level analytics.

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.

Definition	Description
Version Control	The management of multiple iterations or versions of a document or file to maintain accuracy and traceability.

2.3.1 Disclosure Classification

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

2.4 Abbreviations

The following abbreviations, glossary terms and preferred terminology apply throughout this document. They are included to ensure consistent interpretation of the Smart Plant Digitalisation Initiative, its technical requirements, governance obligations and delivery expectations.

Abbreviation / Term	Meaning / Definition
AI	Artificial Intelligence; computer-based methods that analyse data and perform tasks such as recognising images, detecting anomalies, forecasting outcomes, optimising processes and supporting decisions.
AIAP	Artificial Intelligence Apprenticeship Programme; a structured supplier-led programme that transfers practical AI, data, cloud, integration, cybersecurity and Smart Plant operating skills to Eskom personnel.
API	Application Programming Interface; a documented set of rules that enables software systems to exchange data and functions securely.
APM	Asset Performance Management; the use of asset data, condition monitoring, reliability models and analytics to improve reliability, availability, maintainability and lifecycle performance.
CADD	Computer-Aided Design and Drafting; software-based creation, modification and management of engineering drawings and models.
CoC	Certificate of Compliance; formal evidence that specified equipment, installation or work complies with applicable requirements, codes or standards.
DCS	Distributed Control System; the plant control environment used to monitor process conditions, execute control logic and operate plant equipment.
Digital Twin	A governed digital representation of plant assets and systems that combines engineering information and operational data to support visualisation, analysis, simulation, predictive maintenance and decision-making.
Digitalisation	The use of digital technologies, data and integrated workflows to improve plant processes, maintenance execution, governance, decision-making and performance.
Digitisation	The conversion of physical or analogue records into searchable digital files through scanning, optical character recognition, metadata capture, quality checks and controlled repository storage.
DMZ	Demilitarised Zone; a secured network segment that separates operational technology from enterprise or external networks and controls data exchanged between them.
EDMS	Enterprise Document Management System; a controlled platform for creating, numbering, storing, searching, revising, approving, retaining and auditing documents and records.
EDWL	Engineering Design Work Lead; the person accountable for coordinating engineering design work and maintaining design quality and technical integration.
ERP	Enterprise Resource Planning

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.

FGD	Flue Gas Desulphurisation; a process that removes sulphur dioxide from boiler flue gas before atmospheric release.
FMEA	Failure Modes and Effects Analysis; a systematic method for identifying possible failures and assessing their effects on equipment or system performance.
FMECA	Failure Modes, Effects and Criticality Analysis; an extension of FMEA that also ranks failure modes according to risk or criticality.
Foreground IP	Intellectual property newly created, configured, trained, customised or documented specifically for the Kusile Smart Plant Digitalisation Initiative.
GA	General Arrangement drawing; an engineering drawing showing the overall layout, location and relationship of equipment or structures.
HAZOP	Hazard and Operability Study; a structured review used to identify process hazards, operational deviations and required safeguards.
IEC 62443	An international standard series for securing industrial automation and control systems through measures such as zones, conduits, access control, segmentation and lifecycle security management.
IED	Intelligent Electronic Device; a microprocessor-based device that monitors, protects, controls or communicates information about electrical or plant equipment.
IOM	Installation, Operation and Maintenance Manual; controlled instructions for installing, operating, inspecting and maintaining equipment or systems safely.
IP	Intellectual Property; legally protectable outputs such as software, models, algorithms, configurations, workflows, documentation and data structures.
KPI	Key Performance Indicator; a measurable value used to assess progress, performance or achievement against an agreed target.
MCC	Motor Control Centre; an assembly that houses equipment used to control, protect and monitor electric motors.
MQTT	Message Queuing Telemetry Transport; a lightweight publish-and-subscribe messaging protocol used to exchange industrial and Internet of Things data.
MW	Megawatt; a unit of power equal to one million watts.
OCR	Optical Character Recognition; technology that converts text in scanned images or PDF files into searchable, machine-readable text.
OEM	Original Equipment Manufacturer; the organisation that originally designs and manufactures specified equipment or components.
OPC UA	Open Platform Communications Unified Architecture; an open industrial interoperability standard for secure, structured exchange of data between devices, control systems and applications.
P&ID	Piping and Instrumentation Diagram; an engineering drawing showing process equipment, piping, instruments and control relationships.
PEC	Professional Engineering Certificate; formal certification by an appropriately registered engineering professional that specified engineering work meets the applicable requirements.
PI System / Historian	A time-series operational data platform that collects, stores, contextualises and displays plant process and equipment data for monitoring, analysis and integration.
PLC	Programmable Logic Controller; an industrial computer that executes control logic to automate and monitor plant equipment or processes.
POPIA	Protection of Personal Information Act, 2013 (Act No. 4 of 2013); South African legislation governing the lawful and secure processing of personal information.
Private Cloud	An Eskom-controlled computing and storage environment used to host approved Smart Plant data, applications, video, AI artefacts, document services and integration workloads.

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.

QCP	Quality Control Plan; a documented plan that defines inspections, tests, hold points, responsibilities, acceptance criteria and required quality evidence.
Responsible AI	A governance approach that requires AI systems to be risk assessed, validated, secure, monitored, auditable and subject to accountable human oversight throughout their lifecycle.
RWM	Routine Work Management; the controlled planning, assignment, execution, supervision, recording and close-out of routine maintenance and operational work.
SAP PM/MM	SAP Plant Maintenance and Materials Management modules used to manage work orders, notifications, equipment history, maintenance confirmations, material reservations and goods movements.
Smart Plant ecosystem	The integrated environment of networks, private cloud, storage, intelligent inspection, Digital Twin, EDMS, mobile work management, SAP integration, dashboards, cybersecurity controls and approved AI analytics delivered by the initiative.
SOW	Scope of Work; the contractual statement of required work, deliverables, responsibilities, acceptance requirements, assumptions and exclusions.
USC	Ultra-Supercritical; steam-generation technology that operates at very high pressure and temperature to improve thermal efficiency and reduce fuel use per unit of electricity generated.

2.5 Roles and Responsibilities

2.5.1 Technical Team:

Technical authority for integration of digital systems with plant, ensure accurate data acquisition from field devices and integration into digital platforms. The responsibilities include:

a) Manage engineering design, data architecture, and digital twin integration.
b) Oversee CADD, P&ID digitisation, and GA model updates.
c) Ensure engineering data integrity and interoperability with DCS, PLC, and APM systems.
d) Work with IT/OT specialists to ensure data accuracy and cybersecurity.
e) Configure alarms, setpoints, and condition monitoring points.
f) Collaborate with AI and analytics team for predictive insights.
g) Ensure minimal disruption to live control systems during integration.
h) Maintain connectivity and redundancy for smart plant systems.
i) Ensure uptime and performance of data servers and historians.
j) Define critical assets and risk prioritisation matrix.
k) Configure reliability models and maintenance strategies.
l) Coordinate with AI engineers for predictive alerts.
m) Track asset KPIs and integrate results into maintenance planning.
n) Support field validation of predictive model outcomes.
o) Oversee operator training and human–machine interface optimization.
p) Validate process data and digital dashboards.
q) Participate in HAZOP and CoC verification for new digital systems.

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.

2.6 Process for monitoring

Monitoring shall be conducted under four key pillars:

Pillar	Focus Area	Description
Technical Performance Monitoring	System functionality, uptime, response times, data accuracy.	Evaluate all integrated systems (DCS, APM, Digital Twin, Historian) to ensure they meet design specifications and data fidelity requirements.
Operational Monitoring	Maintenance efficiency, operator adoption, process optimization.	Track the use of digital tools by maintenance and operations personnel, including CMMS integration, predictive maintenance triggers, and AI-based decision support.
Cybersecurity and Network Monitoring	OT/IT network integrity, DMZ security, access control.	Ensure the system complies with Eskom's cybersecurity framework and IEC 62443 standards; monitor for unauthorized access or data anomalies.
Programme Performance Monitoring	Project milestones, budget, risk, change management.	Use dashboards to track schedule adherence, cost variance, and delivery of defined functional outcomes.

2.7 Related/Supporting Documents

N/A

3. Engineering and the *Contractor*'s design

3.1 *Employer*'s design

3.1.1 Engineering and Design

- Centralized engineering database (3D model, P&IDs, datasheets).
- Integration with construction data and version control.
- Digital handover of "As-Built" data into the operational digital twin.

3.1.2 Construction and Commissioning

- Use of mobile digital commissioning checklists.
- Cloud-based progress dashboards and issue tracking.
- Integration with DCS testing and loop-check databases.

3.1.3 Operations and Maintenance

- Real-time equipment health dashboards using PI Vision.
- Predictive analytics models for key assets (boiler, turbine, generator, pumps, fans, FGD).
- Mobile maintenance applications (Maximo Mobile).
- AI-driven fault diagnostics and work-order recommendations.

3.1.4 Asset Performance Management (APM)

- KPI monitoring (availability, reliability, heat rate, auxiliary power).

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.

- Digital twin for simulation of operational scenarios. Provision of or interfacing with existing plat form for simulation of operational scenarios
- Life-cycle cost tracking and optimization via SAP integration.

3.1.5 Cybersecurity and Data Integrity

- Implementation of IEC 62443-based cybersecurity zones.
- Data encryption at rest and in transit.
- Secure demilitarized zone (DMZ) for external data access.

3.1.6 Digitalisation Strategy Framework

Layer	Function	Examples of Tools/Systems
Field Layer	Smart sensors, smart MCCs, PLC/IEDs collecting process data	Siemens, ABB, Schneider, Yokogawa PLCs
Control Layer	Real-time process control and automation	DCS, SCADA, PLC networks
Information Layer	Data aggregation and historian storage	OSIsoft PI System, SQL, Data Lakes
Application Layer	Asset management, maintenance, performance analytics	SAP PM, APM tools
Enterprise and AI Layer	Predictive analytics, digital twins, dashboards	Power BI, Azure AI, MATLAB, Digital Twin Platforms

3.2 Parts of the *works* which the *Contractor* is to design

The proposed solution shall be supplied by a manufacturer recognised as a Leader in the latest applicable Gartner® Magic Quadrant™ reports for Enterprise Wired and Wireless LAN Infrastructure, Data Center Switching, and Enterprise Storage Platforms. The bidder shall provide verifiable evidence of such recognition, including the Gartner® report title, publication date, manufacturer name, and supporting documentation demonstrating the manufacturer's position in the Leaders Quadrant. The recognition shall serve as independent evidence of the manufacturer's demonstrated Ability to Execute and Completeness of Vision, ensuring that the proposed technology platform is supported by a proven market leader with established product maturity, innovation capability, scalability, long-term support, and a sustainable technology roadmap suitable for mission-critical power generation operations.

3.2.1 System Architecture and Integration

3.2.1.1 Pillar 1: Network and Infrastructure

The Network and Infrastructure pillar establishes the secure, resilient and scalable connectivity and compute foundation required for all smart plant capabilities, including intelligent inspection, Digital Twin integration, mobile work management, EDMS, video management, AI analytics, dashboards and future plant digitalisation use cases. The service provider must design and implement industrial-grade network, cybersecurity, private cloud, storage, video and management infrastructure that supports current scope requirements while allowing controlled expansion without avoidable vendor lock-in.

The infrastructure must operate as an Eskom-controlled private cloud and network environment, with data hosted on approved infrastructure under Eskom control and governed by South African law. The architecture must provide high availability, disaster recovery, network segmentation, secure authentication, encryption, monitoring, audit logging, change control, lifecycle management and

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.

supportability. AI-enabled network management, video analytics or optimisation functionality must comply with Eskom's Responsible AI governance requirements, including inventory registration, validation evidence, human oversight, monitoring and revalidation where applicable.

3.2.1.2 Technical Requirements

3.2.1.2.1 Technical Requirements for network infrastructure

Component	Specification	Justification
Industrial Access Network	Provide industrial-grade access switching suitable for plant environments, with appropriate ingress protection, wide operating-temperature range, redundant power where required, PoE/PoE++ support, Layer 2/Layer 3 capabilities, secure management and sufficient copper and fibre uplinks for cameras, access points, sensors, smart field devices and edge equipment.	Provides reliable field connectivity for inspection cameras, mobile users and IoT devices in harsh plant areas.
Industrial Wireless Network	Deploy industrial wireless access points supporting current enterprise Wi-Fi standards, secure authentication, encryption, roaming, quality of service, ruggedised environmental ratings and sufficient capacity for mobile work management, smart helmets, handheld devices, inspection support and collaboration use cases.	Supports low-latency mobile connectivity and reliable field workflows.
Access Network	Provide standard access switches featuring redundant power supplies where required, PoE/PoE++ support, Layer 2/Layer 3 capabilities, and sufficient interfaces for device connectivity.	Ensures sufficient interfaces to accommodate device connections.
Aggregation and Core Network	Provide high-capacity aggregation and core switching with redundant power, high-speed fibre uplinks, segmentation, resilient routing, traffic prioritisation, secure management and capacity headroom to support video streams, sensors, EDMS access, Digital Twin integration, dashboards and future expansion.	Provides the resilient high-throughput backbone required for smart plant operations.
Access Controller	The AC should support independent wireless controller functionality, with a capacity to manage at least 3,000 APs. It should comply with IEEE 802.11n/ac/ax/be standards and be equipped with pluggable power supplies.	Provides a WAC that complies with IEEE 802.11n/ac/ax/be standards and is capable of managing a sufficient number of APs.

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.

Data Centre Switching	Provide spine-and-leaf or equivalent data centre switching with high-speed east-west and north-south traffic capacity, secure segmentation, redundant uplinks, resilient forwarding, encryption where required and integration with the private cloud, storage and video management platforms.	Enables scalable cloud, storage, AI inference and application workloads.
Network Management and Monitoring	Provide a centralised network management system with topology visibility, device inventory, configuration backup, fault alarms, performance dashboards, capacity monitoring, security status, user/device visibility, audit logs, change records and reporting. AI-assisted diagnostics may be used only with approved governance, validation and human oversight.	Simplifies operations and provides audit evidence for configuration, performance and security assurance.
Capacity and Scalability	Support at least 500 concurrent connected devices at initial deployment, including handheld devices, cameras, IoT sensors, access points and smart field devices, with minimum 50% capacity headroom for future expansion unless otherwise agreed by Eskom.	Ensures the infrastructure can scale as additional smart plant use cases are introduced.
Redundancy and Availability	Design critical network services with redundant paths, automatic failover, resilient power, backup configurations, monitored service health and defined recovery targets, with a minimum target availability of 99.9% for agreed critical services.	Supports continuity of plant monitoring, mobile work management and operational visibility.
Integration with Existing Networks	Integrate with approved existing plant networks, monitoring systems and enterprise services through documented interfaces, approved security zones, firewall rules, routing design, change control and test evidence. No unmanaged connection to OT or enterprise systems may be introduced.	Enables interoperability while protecting existing Eskom systems and operational boundaries.
Cybersecurity Architecture	Implement IEC 62443-aligned segmentation, secure zones and conduits, firewalling, secure remote access, least-privilege access, multi-factor authentication where required, encryption, logging.	Protects critical infrastructure, operational data and connected plant systems from unauthorised access or manipulation.

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.

Bandwidth and Quality of Service	Provide sufficient aggregate bandwidth, traffic prioritisation and quality-of-service controls for simultaneous video streaming, sensor data, AI inference, mobile synchronisation, dashboards, EDMS access and business applications, with documented performance testing against agreed acceptance criteria.	Ensures reliable performance for real-time and near-real-time smart plant use cases.
Point-to-Point (P2P) Microwave Radio Connections	The equipment for biding must be fully outdoor design and support 7~38GHz frequency bands. The switching capacity of offer equipment shall not be less than 60Gbit/s, Dual RF ports ODU should be supported, each RF port should support carrier aggregation (CA) which can be used to combine two dispersed frequency channels even under different channel spacing. XPIC function must be supported.	Provide a stable and reliable wireless connection from the site to the backbone transmission network

3.2.1.2.2 Technical Requirements for cloud storage

Component	Specification	Justification
Cloud Server	Provide enterprise-grade servers based on x86 or other suitable processor architectures, appropriately sized and configured for their designated roles, including Management Nodes, Network Nodes, and Computing Nodes for hosting business workloads. The servers shall provide hardware redundancy, scalable compute and memory capacity, high-speed network and storage connectivity, and support for future capacity expansion.	Provides a reliable, scalable and flexible server infrastructure to support different infrastructure roles, while delivering sufficient computing capacity for business workloads and future growth.
Private Cloud Management Software	The private cloud management software must provide resource pooling, provisioning, orchestration, virtualisation, container or bare-metal support where required, software-defined networking, role-based administration, logging, monitoring, lifecycle management, backup integration and API-based integration with approved Eskom systems.	Enables controlled allocation of compute and storage resources while supporting maintainability and auditability.
Cloud Storage	Provide scalable, resilient storage with a minimum usable capacity of 200 TB at initial deployment, support for structured and unstructured data, data protection,	Supports diverse enterprise data workloads, including document repositories, analytics datasets, AI

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.

	encryption, access control, snapshots or equivalent recovery capability, policy-based data protection and retention and future expansion without disruptive redesign.	artefacts, logs and operational records.
Video Management System	Provide a video management platform that supports secure camera onboarding, live view, PTZ control, playback, alarm handling, evidence capture, electronic maps, retention management, access control, audit logging, integration with AI analytics and approved dashboard or operations-centre visualisation.	Provides governed video monitoring and evidence management for inspection, safety and security use cases.
Video Storage	Provide enterprise-grade video storage sized for the agreed number of cameras, resolutions, frame rates and retention periods, with redundancy, health monitoring, access control, and open interfaces for integration with video management and analytics platforms.	Ensures reliable storage of video, images and evidence required for operations, safety, security and audit review.
Sovereign Data Hosting and Compliance	All operational data, video, images, AI training datasets, model artefacts, logs, EDMS data and integration records must be hosted on Eskom-approved infrastructure under Eskom control. Any external access, support connection or data transfer must be explicitly approved, logged and governed by Eskom security and data governance requirements.	Protects Eskom data sovereignty, intellectual property and controlled-disclosure information.

3.2.1.2.3 Key Deliverables

- Network and Private Cloud Architecture Design Document: target architecture, topology diagrams, system boundaries, security zones, data flows, capacity plan, resilience design, integration points and deployment assumptions.
- Site Survey and Coverage Assessment: RF survey, heatmaps, access-point placement, cable routes, cabinet locations, power requirements, environmental constraints and installation recommendations.
- Cybersecurity Architecture and Hardening Plan: IEC 62443-aligned zones and conduits, firewall rules, secure remote access, authentication controls, encryption, logging,
- Bill of Materials and Licensing Register: complete hardware, software, licensing, warranty, support, spares and capacity information with quantities, specifications, assumptions and procurement timelines.
- Network Configuration and Commissioning Pack: switch, wireless, firewall, controller, routing, segmentation, quality-of-service, monitoring, backup and configuration-baseline records.

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.

- Private Cloud and Storage Configuration Pack: compute, storage, virtualisation, container or bare-metal configuration where applicable, backup, disaster recovery, monitoring, patching, access control and lifecycle management settings.
- Video Management and Video Storage Configuration Pack: camera onboarding, live view, playback, retention, evidence export, alarm handling, audit logging, AI analytics integration and operations-centre visualisation settings.
- Integration and Acceptance Test Report: performance tests, failover tests, cybersecurity tests, coverage validation, bandwidth validation, data-flow testing, monitoring checks, defect logs, corrective actions and user acceptance sign-off.
- Operations, Monitoring and Handover Manual: administration procedures, monitoring dashboards, troubleshooting guide, backup and restore procedures, patching process, support model, escalation routes, knowledge-transfer evidence and final handover acceptance records.
- The proposed solution shall implement a secure and segmented OT cybersecurity architecture, including an Industrial DMZ, dual firewalls, VLAN-based network segmentation, role-based access control, and continuous OT network monitoring. Direct communication between ERP and DCS environments, as well as direct Internet access from the OT network, shall be prohibited. Remote access to OT systems shall be permitted only through secure jump servers, with appropriate controls in place to ensure secure and controlled access across security zones.

3.2.1.3 Pillar 2: Intelligent Inspection and Digital Interaction

The Intelligent Inspection and Digital Interaction pillar deploys AI-enabled computer vision, industrial cameras, smart field devices, sensors and collaboration platforms to improve plant monitoring, safety compliance, security response, anomaly detection and remote expert support. The solution must provide governed video capture, AI inference, inspection task management, alerting, evidence retention and integration with the wider smart plant ecosystem, including the Digital Twin, EDMS, mobile work management, dashboards, network infrastructure and approved analytics platforms. All AI-enabled inspection functions must be implemented with human oversight, auditable validation evidence, secure data handling, Eskom ownership of inspection data and AI outputs, and lifecycle governance aligned with Eskom's Responsible AI requirements.

3.2.1.3.1 Technical Requirements

Component	Specification	Justification
AI-Enabled Inspection Cameras	The solution must include industrial-grade AI cameras suitable for critical plant and safety-sensitive areas, including explosion-proof, PTZ, bullet, IR and white-light camera options where required. Cameras must support high-resolution video, secure connectivity, edge or central inference integration, time synchronisation, tamper detection and environmental ratings suitable for the installation location.	Provides reliable visual coverage of priority assets, hazardous areas and safety-critical operating zones.

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.

AI Computer Vision and Analytics	Computer vision models must support approved use cases such as oil, steam and water leak detection; equipment condition recognition; meter and indicator reading; PPE compliance; intrusion detection; conveyor monitoring; flame and smoke detection; falling-person detection; and other Eskom-approved anomaly detection scenarios. Model performance must be validated against agreed acceptance criteria before production use.	Automates inspection, improves early detection and reduces manual observation workload.
Responsible AI Governance and Human Oversight	All AI inspection functions must be registered in Eskom's AI inventory, risk assessed, validated, approved through lifecycle gates and monitored in operation. AI outputs must remain decision-support inputs unless Eskom formally approves otherwise, and safety, security or maintenance actions must remain subject to accountable human review.	Ensures AI inspection is safe, accountable, auditable and aligned with Eskom governance.
Inspection Task and Algorithm Management	The platform must support creation, modification, suspension, deletion and scheduling of inspection tasks; configuration of approved algorithms; live video with AI overlays; alert thresholds; exception handling; user permissions; and complete task history with audit trails.	Provides controlled configuration and traceability of inspection tasks and AI analytics.
AI Inference Computing Platform	The supplier must provide an appropriately sized AI inference platform capable of processing the agreed camera channels, video resolution and frame rates, with GPU or accelerator capacity, secure deployment, monitoring, redundancy, software and firmware maintenance capabilities, and open interfaces for integration with approved storage, video analytics and dashboard platforms.	Ensures sufficient compute capacity for reliable video analytics and scalable AI inference.
Perimeter, Security and Safety Monitoring	Perimeter monitoring and safety surveillance shall support the integrated use of distributed fiber-optic sensing, video surveillance cameras and other approved security systems, enabling sensing-triggered video verification, automatic camera linkage and event visualization for	Strengthens plant security, situational awareness and safety response.

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.

	perimeter intrusion detection, area monitoring, emergency alerts, incident review and escalation workflows. The solution shall provide coordinated event management while maintaining clear segregation between security, safety and operational monitoring use cases.	
Digital Interaction and Remote Collaboration	The solution must support secure video conferencing, remote expert support, smart helmet connectivity, body camera or mobile device access where approved, broadcast messaging, two-way communication, whiteboarding where required and controlled recording or evidence capture in accordance with Eskom security and privacy requirements.	Improves remote troubleshooting, acceptance, emergency coordination and field support.
Integrated Operations Centre Visualisation	The supplier must provide integrated visualisation through dashboards and smart screens for live feeds, alerts, inspection status, system health, safety events, historical evidence and escalation status, subject to the approved operating model and access controls. The proposed smart screens shall be interactive displays supporting touch-based operation and real-time user interaction, with seamless integration with the large LED IOC screen to enable coordinated display, content sharing and interactive control.	Provides a single operational view for plant monitoring, alerts and decision support.
Smart Helmet (All hard hats must meet the requirements listed in Eskom Personal Protective Equipment – PPE)	Supply, installation, configuration, testing, and commissioning of Smart safety helmet with expert remote support to enable site operates to imitate real-time audio/video connections with backend experts via dispatch centre for remote guidance and fault diagnosis. Features with and including, built-in camera, microphone, speaker, Wi-Fi and LTE modules, SIM card and TF card slots, Integrated display for battery level, device status, and network status. Complete setup and	A convenient tool for on-site work collaboration and record keeping, improving the efficiency of field support.

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.

	commissioning in accordance with approved technical specifications. Complete setup and commissioning in accordance with approved technical specifications.	
Central Monitoring Platform	The Central Monitoring Platform shall support integrated visualisation through dashboards and 3D digital twin models for real-time data feeds, alarms, equipment status, patrol tracking, system health, and safety events, with adaptive rendering performance and bidirectional data linkage, subject to approved access controls and operating procedures, to enable comprehensive plant monitoring, coordinated response, and informed decision-making.	Provides a unified operational view that combines alarm handling, asset management, digital twin simulation, and real-time data integration, enhancing situational awareness and operational efficiency.
Video Storage and Analytics Platform	The solution must include an AI-enabled NVR suitable for large-scale video surveillance applications, supporting high-density IP camera access, high-bandwidth video recording, multi-channel playback, local AI video and image analytics, and scalable storage expansion. The NVR must provide sufficient computing, memory, network and storage capacity to support reliable 24/7 operation and future system expansion.	Provides reliable video recording, AI-assisted analysis and scalable storage to support continuous surveillance and efficient incident review.

3.2.1.3.2 Key Deliverables

- Camera, Sensor and Field Device Deployment Plan: location plan, coverage analysis, device schedule, environmental suitability, network connectivity, power requirements, installation assumptions and integration architecture.
- AI Inspection Use-Case and Model Validation Pack: approved inspection use cases, training and validation approach, datasets, performance metrics, acceptance criteria, bias or error analysis, limitations and human-review requirements.
- Responsible AI Governance Pack: AI inventory inputs, risk and impact assessment records, lifecycle-gate evidence, model provenance, monitoring plan, drift triggers, incident escalation process and revalidation criteria.

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.

- Inspection Task and Algorithm Configuration Pack: task schedules, algorithm settings, alert thresholds, user roles, exception workflows, live-overlay configuration and task audit-trail settings.
- Central Monitoring and Visualisation Dashboard: configured dashboards for live feeds, alerts, inspection outcomes, safety events, system health, evidence retrieval and management reporting.
- Alert and Escalation Configuration: alert categories, severity levels, notification routing, escalation matrix, acknowledgement workflow, exception handling and reporting templates.
- Digital Interaction and Remote Collaboration System: configured video conferencing, smart helmet connectivity, mobile or body-camera access where approved, broadcast messaging, remote expert support and secure recording controls.
- Smart Plant Integration Specification: documented APIs, data mappings, security controls and test evidence for integration with the Digital Twin, EDMS, mobile work management, dashboards, network management and approved analytics platforms.
- Security, Privacy and Audit Configuration Pack: role-based access model, authentication controls, encryption approach, device hardening, audit-log configuration, POPIA-aligned safeguards, evidence retention and export controls.
- Testing, Training and Handover Pack: User Acceptance Testing, model validation results, user acceptance evidence, training material, administrator guidance, troubleshooting procedures, knowledge-transfer evidence and final handover acceptance records.

3.2.1.4 Pillar 3: Digital Twin Interface and Integration

The Digital Twin Interface and Integration pillar establishes the standards-based integration layer between the Digital Twin and the wider smart plant ecosystem, including intelligent inspection, mobile work management, SAP PM/MM, EDMS, dashboards, sensors, plant networks and approved AI analytics. The solution must provide secure, governed and low-latency data exchange using open standards and documented APIs, while preserving Eskom ownership of data, models, configurations and operational insights. The Digital Twin must support engineering analysis, operational visualisation, predictive maintenance, simulation, decision support and asset information management without introducing unmanaged interfaces, vendor lock-in or unauthorised data movement.

3.2.1.4.1 Technical Requirements

Component	Specification	Justification
Data Interoperability Standards	The Digital Twin integration layer must use open and documented standards, including OPC UA and ISO 23247 where applicable, for structured data modelling, asset context, event exchange and vendor-neutral interoperability.	Prevents vendor lock-in and enables scalable integration across current and future Eskom systems.
Integration Architecture and APIs	The supplier must provide documented APIs, interface specifications, data mappings, authentication requirements, error-handling rules and integration patterns for SAP PM/MM, EDMS, inspection systems, mobile work management,	Creates a controlled integration baseline and supports maintainability, auditability and future extension.

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.

	dashboards, plant historians, sensors and approved analytics platforms.	
Real-Time and Near-Real-Time Data Streaming	The solution must support low-latency data streaming from approved sensors, cameras, systems and operational data sources into the Digital Twin, with performance targets, buffering rules, prioritisation, retry mechanisms and documented acceptance criteria.	Enables timely visualisation, condition monitoring, predictive analytics and operational decision support.
Data Quality, Lineage and Reconciliation	The integration must include automated validation, data-quality rules, time-stamping, source identification, lineage tracking, reconciliation, exception handling and error reporting for all material data exchanged with the Digital Twin.	Protects the accuracy, reliability and traceability of data used for engineering analysis and predictive models.
Synchronisation and Change Control	Bi-directional synchronisation must be governed through approved data ownership rules, conflict-resolution logic, configuration baselines, change-control records and version management for Digital Twin models, interfaces, tags, mappings and asset hierarchies.	Maintains integrity between the Digital Twin and authoritative source systems.
EDMS and Asset Information Linkage	The Digital Twin must link to approved EDMS records, including drawings, manuals, data books, inspection reports, procedures and asset documentation, using controlled metadata, document status, access rules and information classification.	Ensures that users access current and approved asset information from within Digital Twin workflows.
Responsible AI and Analytics Governance	Any AI, optimisation, predictive-maintenance or simulation functionality connected to the Digital Twin must support AI inventory registration, risk and impact assessment, human oversight, validation evidence, model provenance, monitoring, drift detection, incident escalation and revalidation when data, models or operating conditions materially change.	Aligns Digital Twin analytics with Eskom's Responsible AI governance and operational accountability requirements.
Cybersecurity and Access Control	All interfaces must apply secure authentication, authorisation, encryption, role-based access control, network segmentation, least-privilege	Protects critical operational data, plant interfaces and Digital Twin

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.

	access, audit logging and approved change control in line with Eskom IT/OT security requirements and IEC 62443 principles.	assets from unauthorised access or manipulation.
Performance Monitoring and Auditability	The supplier must provide monitoring of latency, throughput, interface health, data completeness, synchronisation status, integration errors, user access, configuration changes and service availability, supported by dashboards, logs and compliance evidence.	Provides evidence for operational assurance, SLA monitoring, troubleshooting and audit review.

3.2.2 Key Deliverables

- Digital Twin Integration Architecture Document: target architecture, interface landscape, system boundaries, integration patterns, data ownership rules, security zones and dependencies across SAP PM/MM, EDMS, inspection systems, mobile work management, dashboards, historians and approved analytics platforms.
- Data Interoperability and Asset Information Model: OPC UA and ISO 23247 alignment, asset hierarchy, tag mapping, metadata model, event model, document linkage and standards compliance evidence.
- API and Interface Specification Pack: documented APIs, data mappings, authentication rules, authorisation model, error-handling rules, retry logic, reconciliation approach and interface test cases.
- Data Quality and Lineage Plan: validation rules, source-system mapping, time-stamping, data lineage, exception handling, reconciliation controls, data-quality thresholds and reporting dashboards.
- Synchronisation and Change-Control Configuration: configuration baselines, version-control records, conflict-resolution rules, tag and model change process, approval workflow and rollback procedure.
- Responsible AI and Analytics Governance Pack: AI inventory inputs, risk and impact assessment records, validation evidence, model provenance, monitoring requirements, drift triggers, human-oversight controls and revalidation criteria for any AI-enabled Digital Twin analytics.

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.

- Cybersecurity and Access-Control Configuration Pack: role-based access model, secure authentication, encryption approach, segmentation controls, audit logging, privileged-access process and IEC 62443-aligned security evidence.
- Integration Testing and Performance Report: latency measurements, throughput validation, data completeness, interface availability, synchronisation results, error logs, corrective actions and user acceptance sign-off.
- Operations and Handover Manual: monitoring dashboards, support procedures, troubleshooting guide, backup and recovery approach, knowledge-transfer evidence, administrator guidance and final handover acceptance records.

3.2.2.1 Pillar 4: Paperless Operations / Digitalised Routine Work Management (RWM) and Outage Functions

The Paperless Operations pillar transforms Routine Work Management (RWM), outage execution and field maintenance activities from paper-based processes into controlled, mobile-enabled digital workflows. The solution must support end-to-end work order execution, task initiation, supervision, acceptance, record keeping, evidence capture and close-out, with secure bi-directional integration to SAP PM/MM and governed access to approved technical documents through the EDMS. This pillar improves work order cycle time, data accuracy, field productivity, outage coordination, auditability and real-time visibility of maintenance execution. It must also preserve Eskom ownership of operational data, enforce role-based controls, and provide a complete audit trail for all material workflow, approval, data and close-out actions.

3.2.2.1.1 Technical Requirements

Component	Specification	Justification
Mobile Work Management Application	The solution must provide a secure Android mobile application for field users, with offline capability, synchronisation when connectivity is restored, role-based work queues, device-level security controls and support for at least 100 concurrent users.	Enables field teams to execute work reliably in plant areas with intermittent connectivity.
RWM Task Management	The system must support digital work order receipt, task initiation, execution, supervision, acceptance, record keeping, query, close-out and exception management. It must include guided procedures, checklists, multimedia instructions, photo and video evidence capture, electronic signatures, timestamps, geolocation where approved, and real-time status updates.	Replaces paper-based execution with controlled digital workflows and a complete execution audit trail.

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.

SAP PM/MM Integration	The solution must provide secure bi-directional integration with SAP PM/MM for work orders, notifications, equipment history, functional locations, maintenance confirmations, material reservations, goods movements, status updates and close-out information using documented APIs, data mapping and reconciliation controls.	Maintains master-data consistency and reduces duplicate manual entry between field execution and SAP.
EDMS and Technical Document Access	Field users must be able to retrieve approved drawings, procedures, manuals, data books, checklists and historical records from the EDMS through controlled links or approved integration mechanisms, with access governed by document status, user role and information classification.	Ensures technicians use current, approved information during work execution.
Outage Management	The solution must support outage planning, scope definition, work packaging, resource levelling, progress tracking, hold-point management, daily reporting, constraints management, risk and issue logging, handover and close-out reporting.	Improves coordination and visibility during complex outage execution.
User Management and Access Control	The system must apply role-based access control for technicians, artisans, supervisors, planners, engineers, outage coordinators, administrators and approvers. Access rights must align with user responsibilities, segregation of duties, Eskom security requirements and approval authority.	Ensures appropriate data access, workflow enforcement and accountability.
Reporting and Analytics	Dashboards must provide near-real-time visibility of work order status, backlog, resource utilisation, overdue actions, outage progress, constraints, equipment downtime, material status, maintenance cost indicators and exception trends.	Provides operational visibility for supervisors, planners and management decision-making.

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.

Data Governance and Security	The solution must apply encryption, secure authentication, multi-factor authentication where required, device management, role-based access control, audit logging, information classification, POPIA-aligned handling of personal information and protection of operationally sensitive data.	Protects Eskom operational data and ensures traceable, authorised use of the system.
Auditability and Compliance Evidence	The system must retain auditable records for work order receipt, task assignment, field execution, evidence capture, approvals, rework, exceptions, material movements, synchronisation events, close-out and user access changes.	Provides defensible evidence for operational assurance, audit review and compliance reporting.
Ruggedized Mobile Devices (Handhelds)	The screen is no smaller than 5.0 inches with a resolution of 1920*1080.The battery capacity is greater than or equal to 5100 mAH. Supports DMO (Direct Mobile Operation) mode and is compatible with both analogue and digital modes. Support dual sim functionality for both public and private networks. A dual charger is required to charge the terminal and the backup battery at the same time.	Handheld terminals are provided to run dedicated service software, implementing mobile service office and communication.

3.2.2.1.2 Key Deliverables

- Mobile Work Management Application: configured Android application with offline capability, secure authentication, role-based work queues, evidence capture, synchronisation and field-user functionality.
- RWM Workflow Configuration Pack: configured workflows for task initiation, execution, supervision, acceptance, exception management, record keeping, query and close-out.
- SAP PM/MM Integration Specification: documented APIs, data mappings, interface controls, reconciliation rules, integration test evidence and error-handling procedures for work orders, notifications, materials, confirmations and close-out data.
- EDMS Integration Specification: controlled document-access model, approved integration mechanism, metadata linkage, user access rules and test evidence for retrieval of approved drawings, procedures, manuals and technical records.
- Outage Management Configuration: configured outage planning, work packaging, progress tracking, constraints management, daily reporting, handover and close-out reporting functions.

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.

- User Acceptance Testing Plan and Results: test scenarios, user feedback, defects, corrective actions, retest evidence and sign-off documentation.
- Mobile Device Management Configuration: device enrolment, application distribution, security policies, access controls, remote wipe capability and support procedures.
- Security and Audit Configuration Pack: role-based access model, authentication configuration, audit-log settings, data-handling controls, information classification mapping and POPIA-aligned safeguards.
- Training Materials and User Guides: administrator guides, end-user guides, quick-reference material, training videos where applicable, standard operating procedures and role-specific learning content.
- Operations and Handover Manual: administration, monitoring, troubleshooting, backup, restore, support model, maintenance procedures, knowledge-transfer evidence and final handover acceptance records.

3.2.2.2 Pillar 5: Digitization of Existing Plant Documents and Data Books

The Document Digitisation pillar establishes a controlled digital repository for Kusile's technical and non-technical records, including plant documents, engineering drawings, technical manuals, data books, maintenance records, operational procedures and supporting business records currently stored across distributed document centres. This pillar is critical for knowledge preservation, rapid information access, auditability and integration with the smart plant ecosystem. By digitising, indexing and governing these records through an enterprise document management system (EDMS), Kusile will enable engineers, technicians and authorised users to access approved information in near real time, reduce troubleshooting time, improve maintenance decision-making and strengthen document control.

The scope covers more than 1 000 000 pages held across the station's distributed document centres. The digitisation process must include document inventory, preparation, scanning, optical character recognition (OCR), metadata tagging, quality assurance, secure storage, version control, retention management and migration into an EDMS with full-text search and controlled integration with the relevant smart plant use cases, including mobile work management, SAP PM/MM, digital twin interfaces and AI-assisted search or retrieval where approved.

Digitalisation extends beyond scanning by using trusted digital information to improve document creation, review, approval, routing, retrieval and lifecycle management. Where AI-assisted document classification, extraction, summarisation or document generation is proposed, it must be governed through Eskom's Responsible AI requirements, including inventory registration, risk assessment, human oversight, validation evidence, audit trails and approved deployment controls. The EDMS must generate or manage unique document numbers in accordance with Eskom metadata requirements, support OCR for all converted PDF records, enable automated routing and electronic approval, and notify accountable document owners at least 60 days before the next review date.

3.2.2.2.1 Technical Requirements

Component	Specification	Justification
Document Scope and Inventory	Digitisation of more than 1 000 000 pages across distributed document centres, including technical manuals, engineering drawings, data books, maintenance records, operational procedures, spare-parts catalogues, business records and legacy plant documentation. The supplier must	Establishes a complete baseline for planning, tracking, reconciliation,

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.

	complete a verified document inventory before bulk scanning commences.	quality control and audit evidence.
Scanning Quality	High-resolution scanning at a minimum of 300 DPI for standard documents and 600 DPI or higher for technical drawings, diagrams and specifications. Colour scanning must be used where colour conveys technical meaning, and all scanned records must be checked for completeness, orientation, legibility and page order.	Ensures technical records remain readable, reliable and suitable for engineering reference.
OCR, Metadata and Indexing	All converted PDF records must be OCR-enabled for full-text search. Metadata must comply with Eskom requirements and include, as applicable, document number, title, discipline, equipment tag, system, document type, revision, status, owner, review date, retention class and source location. Text recognition accuracy ≥ 90%. Outputs two-layer PDF documents to support full-text search. AI-assisted classification may be used only with human verification and approved governance controls.	Enables accurate retrieval, lifecycle control, compliance reporting and integration with engineering and maintenance processes.
Enterprise Document Management System	The EDMS must provide controlled document creation, unique document numbering, version and revision control, workflow routing, electronic approval, access control, full-text search, audit logging, retention management, reporting and integration with approved Eskom systems.	Provides a single governed repository for approved records and strengthens document control.
Multi-Site Coordination	Scanning operations across all document centres must be coordinated through a documented logistics, custody, tracking and reconciliation process, with centralised quality control and exception management.	Maintains chain of custody and consistent quality across distributed document locations.
Data Security and Compliance	The EDMS and digitisation process must apply encryption, secure authentication, role-based access control, audit logging, POPIA-aligned handling of personal information, Eskom information classification requirements and protection of confidential technical and operational records.	Protects controlled-disclosure information, operational data and records containing personal or commercially sensitive information.
Integration with Smart Plant Systems	The EDMS must expose documented APIs or approved integration mechanisms for mobile work management, SAP PM/MM, digital twin interfaces, dashboards and AI-assisted	Provides field users and engineers with governed access to relevant records within operational workflows.

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.

	retrieval functions, subject to Eskom approval and data governance controls.	
Digital Preservation and Retention	The solution must include long-term preservation controls, backup and disaster recovery procedures, retention rules, automated archiving, format standardisation and periodic accessibility checks for critical engineering and legal records.	Ensures records remain accessible, usable and defensible throughout their required retention period.
Automated Review Notifications	The EDMS must notify accountable document owners and reviewers at least 60 days before the next review date and must support escalation where review actions are overdue.	Supports document currency, governance compliance and timely review.
Automated Routing and Approval	The system must route documents to the correct stakeholders in the approved sequence for drafting, review, approval, authorisation and publication, with electronic approval records and full workflow audit trails.	Improves turnaround time while preserving accountability and approval traceability.
Auditability and Quality Evidence	The supplier must provide audit evidence for document custody, scanning batches, OCR accuracy checks, metadata validation, exception handling, security configuration, migration reconciliation, user access, workflow routing and final acceptance.	Creates defensible evidence that the digitisation process is complete, accurate, secure and fit for operational use.

3.2.2.2.2 Key Deliverables

- Document Inventory and Assessment Report: complete inventory of all documents across the distributed document centres, including volume estimates, condition assessment, source location, ownership, document type, retention class and digitisation priority.
- Digitisation Specification and Quality Plan: scanning parameters, OCR requirements, metadata schema, batch-control process, quality criteria, exception handling and acceptance thresholds.
- Configured Enterprise Document Management System: EDMS configured for unique document numbering, version control, workflow routing, electronic approval, full-text search, access control, review notifications, retention management and audit logging.
- Digitised Document Repository: complete set of scanned, OCR-enabled, metadata-tagged and quality-checked documents migrated into the approved repository. Including all the scanned TIF files, dual-layer PDFs, and metadata tables.
- Integration Specifications: documented APIs, data mappings and integration test evidence for approved interfaces with mobile work management, SAP PM/MM, EDMS, Digital Twin systems, dashboards and AI-assisted retrieval functionality where applicable.
- Security and Governance Configuration Pack: role-based access model, information classification mapping, POPIA-aligned handling requirements, audit-log configuration, retention rules, backup and disaster recovery procedures.

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.

- Data Migration and Reconciliation Report: evidence of migration from source locations into the central repository, including batch counts, exception logs, quality results and final acceptance reconciliation.
- User Training and Handover Pack: administrator guides, end-user guides, quick-reference material, operating procedures, support model, knowledge-transfer evidence and handover acceptance records.

3.2.2.3 Functional and Non-Functional Requirements

3.2.2.3.1 Global Market and Standards Compliance

The proposed solution must be suitable for both local and international service providers while remaining compliant with South African legislation, Eskom governance requirements and recognised international standards for industrial digitalisation, cybersecurity, data protection, interoperability and responsible AI. The technology stack must be market-agnostic, standards-based and capable of being supported, audited, maintained and extended without creating avoidable vendor lock-in or compromising Eskom's ownership of data, intellectual property, AI models or operational knowledge.

3.2.2.3.2 International Standards Compliance

- IEC 62443: industrial automation and control system cybersecurity requirements, including secure architecture, network segmentation, access control, vulnerability management and secure change control.
- ISO/IEC 27001: information security management requirements relevant to governance of information assets, access controls, risk treatment and security assurance.
- IEC 62264: enterprise-control system integration principles for structuring interfaces between control systems, manufacturing operations, maintenance systems and enterprise applications.
- OPC UA: open, secure and reliable data exchange between operational technology, sensors, plant systems, digital twin platforms and analytics layers.
- ISO 23247: digital twin framework and data interoperability principles to support structured, vendor-neutral exchange of manufacturing and plant data.
- ISO 9001: quality management requirements for the supplier's project delivery methodology, document control, testing, corrective action, acceptance and handover processes.
- Eskom Operational Technology cybersecurity and remote-access standards: the supplier must comply with applicable Eskom IT/OT cybersecurity, remote-access, plant labelling, design review, engineering drawing and technical document management requirements where relevant to the solution.
- POPIA and Eskom data governance requirements: lawful processing, purpose limitation, data minimisation, access control, retention, audit logging and protection of personal, operational and commercially sensitive information.
- Eskom Responsible AI governance requirements: AI inventory registration, risk and impact assessment, human oversight, lifecycle-gate approval, model provenance, monitoring, drift detection, incident escalation and revalidation before material change or deployment.
- Sovereign deployment and data localisation: all operational data, AI training datasets, inspection outputs, digitised records and model artefacts must be hosted on Eskom-approved infrastructure under Eskom control, unless Eskom provides explicit written approval for an alternative arrangement.

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.

3.2.2.3.3 Technology Agnosticism

The proposed hardware, software, interfaces and data models must be technology-agnostic, standards-based and supportable through documented APIs, open integration protocols and clearly defined configuration artefacts. The supplier must avoid unnecessary proprietary dependencies and must provide sufficient documentation, licences, escrow arrangements, configuration records and knowledge-transfer evidence to enable Eskom to operate, maintain, integrate and extend the solution independently or through approved third parties.

3.2.2.3.4 Multi-language Support

The user interface for the Mobile Work Management, virtual collaboration, inspection, document management and operational dashboard platforms must use English as the primary operating language and must be capable of supporting additional languages where required by Eskom. User-facing terminology, workflows, help functions and training materials must be clear, consistent and suitable for field, engineering, control-room and administrative users.

3.3 Contractor Design, Documentation and Acceptance Requirements

The supplier must prepare, submit and maintain all design, configuration, integration, testing, commissioning, training and handover documentation required for the Smart Plant scope. Documentation must support design review, interface management, quality assurance, operations, maintenance, cybersecurity assurance, knowledge transfer and final acceptance. All submissions must follow Eskom document-control requirements, use approved document numbers and revision history, and provide traceable responses to Eskom review comments.

- Design submissions must include applicable drawings, calculations, architecture diagrams, data-flow diagrams, interface specifications, cybersecurity design evidence, configuration baselines, test plans, quality plans, method statements, commissioning plans, operating procedures, training material and handover manuals.
- Each revision must include a revision history and a comment-response record showing how Eskom review comments were addressed.
- Technical documents must include, where applicable, project or package name, unit number, contractor name, contract number, plant identification codes, document owner, document status, revision, approval status and unique document identifier.
- The supplier must allow sufficient review time in the project schedule for Eskom review, comment consolidation, revision, resubmission and acceptance before implementation of design-dependent work.

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.

- As-built information, operating manuals, maintenance schedules, network architecture records, software licence records, loop diagrams, termination schedules, configuration files and support documentation must be delivered as part of final handover.
- No material deviation from the accepted design, interface baseline, cybersecurity architecture or data-governance approach may be implemented without formal change control and Eskom approval.

3.4 Monitoring, Benefits and KPI Requirements

The supplier must provide monitoring, reporting and benefits-realisation evidence for the implemented Smart Plant capabilities. Monitoring must cover technical performance, operational adoption, cybersecurity posture, data quality, AI model performance where applicable, programme delivery and handover readiness. KPIs must be baselined before implementation and tracked through commissioning, post-go-live stabilisation and handover.

Monitoring Area	Minimum Requirement
Technical Performance Monitoring	Monitor availability, latency, response times, throughput, synchronisation status, storage utilisation, interface health, data completeness, configuration changes and service incidents across the smart plant environment.
Operational Monitoring	Track adoption of mobile work management, inspection workflows, EDMS retrieval, dashboard usage, outage execution visibility, work order cycle time and operational exception trends.
Cybersecurity and Network Monitoring	Monitor network integrity, access-control events, security alarms, privileged access, vulnerability status, patch compliance, firewall changes, remote-access sessions and IEC 62443-aligned security controls.
Data and AI Monitoring	Track data quality, lineage, reconciliation errors, AI model performance, model drift, validation exceptions, false positives or false negatives for AI inspection use cases, and revalidation triggers.
Programme Performance Monitoring	Track milestones, deliverables, defects, risks, actions, change requests, test progress, acceptance status, training completion and handover readiness through approved reporting dashboards.

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.

3.5 Intellectual Property (IP) and AI Apprenticeship Programme (AIAP)

The service provider must comply with the Kusile Smart Plant Digitalisation Intellectual Property and Artificial Intelligence Action Plan Strategy. The purpose of this requirement is to ensure that all intellectual property, data, AI models, digital twin configurations, software integrations, digitised records and operational knowledge generated through the Smart Plant Initiative are protected as Eskom strategic assets, governed through Eskom's Responsible AI controls, and support the transfer of relevant capabilities into sustainable internal capability. The supplier's proposal and contract must therefore demonstrate clear alignment to Eskom ownership, data sovereignty, AI lifecycle governance, audit traceability, cyber-secure deployment, human accountability and structured knowledge transfer.

Requirement	Description
Eskom Ownership of Foreground IP	All custom-developed software, AI models, digital twin configurations, integration code, workflows, dashboards, technical documentation, digitised plant records and other IP created specifically for the Kusile Smart Plant Initiative must vest in Eskom from creation as project foreground IP.
Protection of Eskom Data and Training Datasets	All operational data, sensor data, inspection images, maintenance records, SAP PM/MM data, labelled datasets, model outputs and derived insights remain Eskom property. The supplier may only access or process this data for authorised Kusile contract purposes and may not retain, reuse, commercialise or train external models on Eskom data without Eskom's explicit written approval.
Responsible AI Governance	All AI-enabled functionality must be registered in Eskom's AI inventory, risk tiered, assessed for impact, approved through lifecycle gates, monitored in operation and revalidated when models, data, interfaces or operating conditions materially change. High and Critical AI use cases must remain subject to human oversight and formal Eskom approval before production deployment.
Sovereign Deployment and Audit Traceability	The solution must operate within the approved Kusile-owned environment, with data hosted on Eskom-controlled infrastructure and governed under South African law. The supplier must maintain audit trails, model provenance, version control, deployment records, training and validation evidence, monitoring logs and change-control records for all AI and digital systems.
Technology Transfer and AIAP	The supplier must implement a structured AI Apprenticeship Programme and knowledge-transfer plan that enables Eskom personnel to operate, configure, troubleshoot, govern, monitor and enhance the deployed smart plant systems without creating long-term dependency on the supplier.

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.

3.5.1 IP Ownership and Criteria

The Contractor must adopt an Eskom-first IP ownership model consistent with the Kusile IP and AI Action Plan. The model must distinguish supplier background IP from project foreground IP, while ensuring that Eskom retains ownership and control over all Kusile-specific customisations, operational data, AI training datasets, model outputs, digital twin configurations, digitised engineering records, SAP integrations and business process logic generated through the programme.

a. Background IP

Pre-existing technology, software, AI frameworks, algorithms, tools and platform components owned by the supplier before the contract remain the supplier's background IP. Eskom must receive a perpetual, non-assignable, non-transferable, irrevocable, royalty-free licence to use the background IP to the extent required for the Kusile programme, continued operation, support, maintenance, disaster recovery and future Eskom deployments where contractually agreed.

b. Foreground IP

All new IP developed, configured, trained, customised or documented specifically for the Smart Plant project must be treated as Eskom foreground IP. This includes custom software, SAP integration code, dashboards, APIs, AI models trained or fine-tuned on Kusile data, digital twin configurations, plant-specific algorithms, workflows, reports, metadata schemas and technical documentation. The supplier must not copy, reuse, commercialise, disclose or deploy this foreground IP outside the Kusile contract without Eskom's prior written consent.

c. Data IP

All raw data, processed data, labelled datasets, AI training datasets, inspection images, video analytics outputs, SAP PM/MM records, maintenance histories, sensor streams, Digital Twin outputs and derived operational insights remain the exclusive property of Eskom. The supplier may only access this data for approved contract purposes, must maintain a complete data inventory, must apply Eskom-approved security controls, and must delete all supplier-held copies at contract termination or when instructed by Eskom, supported by a written certificate of deletion.

d. Process IP

Custom workflows, standard operating procedures, business rules, mobile work management logic, outage management workflows, AI governance artefacts, acceptance criteria and operational processes created during the project must be owned by Eskom. Eskom must retain the right to modify, enhance, extend, maintain and reuse these processes internally or through approved third parties without additional supplier approval or licensing cost.

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.

Key IP, data and AI governance criteria to be addressed in the contract:

- Open standards compliance: all developed solutions must adhere to open industry standards such as OPC UA, ISO 23247 and relevant IEC 62443 controls to prevent vendor lock-in and ensure interoperability with current and future Eskom systems.
- AI inventory and lifecycle evidence: all AI-enabled functionality must be recorded in Eskom's AI inventory and supported by risk assessment, design evidence, test results, validation records, deployment approvals, monitoring thresholds, incident logs and revalidation triggers.
- Model provenance and traceability: the supplier must maintain version control, training data descriptions, validation results, model cards or equivalent documentation, deployment records, monitoring logs and change history for all AI models developed, configured or fine-tuned during the programme.
- Operational Continuity Requirements: For critical custom-developed software, AI models, configurations, integration components and technical documentation, the supplier must provide appropriate operational continuity measures to ensure that Eskom can continue to operate, maintain, restore and support the solution in the event of supplier insolvency, contract termination or prolonged support unavailability.
- Right to modify and extend: Eskom must retain the right to modify, enhance, extend, maintain, integrate and redeploy foreground IP internally or through approved third parties without additional supplier approval or licence fees.
- Restrictions on supplier reuse: the supplier must not use Eskom data, AI models, Kusile-specific configurations, digital twin logic, operational insights or confidential information for other customers, sites or products without Eskom's prior written consent.

3.5.2 AI Apprenticeship Programme (AIAP) Integration

The AI Apprenticeship Programme must be implemented as a formal technology-transfer and capability-development mechanism, not as optional training. The supplier must embed Eskom-nominated personnel in the implementation workstreams and progressively transfer the knowledge required to operate, administer, monitor, retrain, troubleshoot and govern the deployed AI, cloud, network, digital twin, inspection, document management and SAP-integrated systems.

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.

Benefits of AIAP Integration:

- Internal capability development: builds a core Eskom team with practical competence in AI model monitoring, data stewardship, digital twin integration, cloud administration, inspection analytics, workflow configuration and responsible AI governance.
- Reduced supplier dependency: enables Eskom personnel to perform routine administration, configuration, model-performance review, data-quality checks, first-line troubleshooting and minor enhancements without unnecessary reliance on the supplier.
- Sustainable governance: ensures that AI inventory updates, lifecycle evidence, human oversight, model drift monitoring, incident escalation and revalidation activities can be performed internally after project handover.
- Operational resilience: improves Eskom's ability to sustain the smart plant solution during outages, supplier support delays, cyber incidents, model degradation or future system changes.
- Continuous improvement: creates a structured pathway for Eskom engineers and technical staff to identify, test and safely scale future smart plant enhancements using approved governance and engineering controls.

Requirements for AIAP Integration:

- Apprentice placement: the supplier must accommodate Eskom-nominated apprentices or technical staff within relevant implementation workstreams for the full implementation period, including AI inspection, digital twin integration, data engineering, SAP integration, cloud administration, cybersecurity and document management.
- Structured learning plan: the supplier must submit an AIAP plan covering learning outcomes, curriculum, workstream placement, mentoring schedule, competency matrix, assessment approach and handover milestones.
- Mentorship and knowledge transfer: supplier technical leads must provide documented mentoring, workshops, configuration walkthroughs, design reviews, model-management sessions, troubleshooting exercises and system administration training.
- Project-based assignments: apprentices must be assigned meaningful tasks linked to deliverables, including data labelling, model validation support, dashboard configuration, integration testing, AI lifecycle evidence preparation, SOP drafting and operational handover documentation.

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.

- Competency assessment: the supplier must assess apprentice competence against agreed capability areas, including network and cloud administration, AI model monitoring, digital twin updates, SAP integration support, cyber hygiene, data governance and responsible AI compliance.
- Documentation and handover: the supplier must provide complete technical documentation, configuration records, source-code or model documentation where applicable, operations manuals, troubleshooting guides, training materials and knowledge-transfer completion evidence.
- Minimum continuity period: structured knowledge-transfer activities must continue for at least 12 months during implementation and must include a post-go-live support and shadowing period with measurable handover acceptance criteria.

3.6 Non-Functional Requirements

Requirement	Description
Data Governance, Ownership and Traceability	The solution must align with Eskom's data governance requirements by defining data ownership, stewardship, classification, retention, access rights, quality controls and full audit trails for operational data, AI training datasets, model outputs, document records, SAP integration data and all material data changes.
Cybersecurity and OT Security	The entire solution must comply with applicable industrial cybersecurity standards, including IEC 62443 principles, Eskom IT/OT security requirements, network segmentation, secure authentication, encryption, privileged-access control, vulnerability management, incident logging and secure change control for all connected systems.
Responsible AI Governance	All AI-enabled functionality must support Eskom's Responsible AI governance controls, including AI inventory registration, risk and impact assessment, human oversight, approval gates, model provenance, validation evidence, monitoring, drift detection, incident escalation and revalidation before material changes or production deployment.
Interoperability and Open Standards	The solution must interoperate with SAP PM/MM, the existing Digital Twin, mobile work management platforms, EDMS repositories, inspection systems and relevant plant networks using documented APIs and open standards such as OPC UA, ISO 23247 and other approved integration protocols to prevent vendor lock-in.
Sovereign Deployment and Data Localisation	All operational data, AI training data, inspection outputs, digitised records and model artefacts must be hosted on Eskom-approved infrastructure under Eskom control and governed by South African law, unless Eskom provides explicit written approval for an alternative arrangement.
Scalability	The solution must support current operations and accommodate future expansion across users, devices, cameras, sensors, AI models, documents, workflows, storage

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.

	and integration volumes, with a minimum 50% capacity headroom unless otherwise agreed by Eskom.
Reliability and Availability	Critical systems must be designed for high availability, resilient failover, recoverability and continuity of operations, with a minimum target availability of 99.9% for agreed critical services and defined recovery time and recovery point objectives.
Performance	The solution must provide fit-for-purpose performance for real-time and near-real-time use cases, including low-latency data exchange, responsive dashboards, reliable mobile synchronisation, timely AI inference, and documented performance testing against agreed acceptance criteria.
Usability and Accessibility	User interfaces must be intuitive, role-based, accessible to authorised users, suitable for field and control-room environments, and supported by training materials, quick-reference guides and help functions. English must be the primary operating language, with multi-language support where required.
Maintainability and Supportability	The solution must include administration tools, configuration documentation, monitoring dashboards, backup and restore procedures, patching guidance, troubleshooting procedures, support handover packs and knowledge-transfer evidence to enable Eskom to sustain the solution after implementation.
Auditability and Compliance Evidence	The supplier must provide auditable evidence for design decisions, configuration baselines, security controls, AI lifecycle approvals, model validation, testing, defects, corrective actions, acceptance results, data handling, user access and operational handover.

3.6.1 Interfaces

Interface	Purpose	Protocol/Method
DCS	Real-time data capture	OPC UA / Modbus / MQTT
APM/Analytics	Predictive analysis	REST API / Data Lake
SAP	Work order synchronization	BAPI / Web Services
Power BI	Dashboard visualization	OLEDB / REST
Twin	Model synchronization	API / MQTT Stream

3.6.2 Expected Benefits and KPIs

Category	KPI	Target
Plant Availability	Increase in availability	+3–5 %
Maintenance	Reduction in unplanned outages	−20 %

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.

Cost Efficiency	Reduction in maintenance cost	−10 %
Data Utilization	Centralized data points integrated	> 90 %
Cybersecurity	Compliance with IEC 62443	100 %

3.7 Procedure for submission and acceptance of *Contractor*'s design

3.7.1 Documentation Requirements

The *Contractor* ensures that the Technical Documents and Records Management Work Instruction, 240-76992014 is adhered to for all documentation requirements. The *Contractor* is responsible for the compilation and the supply of all documentation during the various project stages. The *Contractor* makes provision in their programme for the submission of design documentation. For consistency, it is important that all documents used within the project follow the same layout, style and formatting as described in the Technical Documents and Records Management Work Instruction, 240-76992014. Documents such as QCP's, Method Statements etc. that impact the project works to be approved by the *Employer* at least 3 working days prior to commencement of the works.

Each revision of a document or drawing shall be accompanied with a list of comments made by the *Employer* on previous revisions, if applicable. The responses/corrective actions taken by the *Contractor* to be recorded in a revision table contained in each drawing/document.

Documents and drawings to indicate the *Employer*'s unique identification number as allocated by the Employer. The *Contractor* may also have his own internal document or drawing number on the document or drawing.

The *Contractor* compiles a complete data book for all works performed during manufacturing, construction and commissioning. The data package to contain the following attributes as a minimum, where applicable:

- Design drawings used to execute the works.
- Approved construction/installation method statement.
- Approved QCP/ITPs.
- Material certificates/data sheets for all components.
- Test reports.
- Calibration certificates.
- Certificates of Completion (CoCs) or Professional Engineering Certificates (PECs).
- Operating and maintenance manuals.
- Spares catalogue.
- Storage, packing and transportation instructions.

3.7.2 The Contractor shall ensure that documents have the following minimum attributes on the cover page:

- Document title.
- Document unique identification number (Eskom number).
- Contractor document number, if applicable.
- Document status.
- Revision number.
- Document type.
- Document revision table/history.
- Page number on the footer.
- Document author/authoriser.
- Document originator.

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.

3.7.3 The following additional attributes are important for technical documents:

- Package/System name/sub-system name.
- Unit number.
- Contractor name.
- Contract number.
- Plant identification codes.

3.7.4 Format and Layout of Documents

For consistency, it is important that all documents used within a specific domain follow the same layout, style and formatting standard.

3.7.5 Layout and Typography

Every document should comply with the following font specifications:

- Font Colour: Black
- Main Headings Font Type: Arial, Bold, Capital Letters
- Main Heading Font Size: 12pt
- Sub Headings Font Type: Arial, Bold, Title Case
- Sub Headings Font Size: 11pt
- Body Font Type: Arial, Sentence Case i.e., only the first letter of the first word is a capital letter.
- Body Text Font size: 11pt
- Line Spacing: 1.5 line spacing
- Margins: Standard
- Alignment: Full justification to be used
- Paragraphing: One line skip between paragraphs
- Pagination: Centred page numbers (about 0.5 inches from bottom)
- Indentations: Standard tab for all paragraphs (about 0.4 to 0.5 inches)

3.7.6 Document Headers

The header should include the project name, document title, document number, revision number and page number.

3.7.7 Naming of files

The Contractor complies with the Eskom standard for naming documentation files. The standard is as follows:

- For documents that have an approval date and signature; (YYYYMMDD_DocType_DocumentTitle_UniqueIdentifier_Revision.FileExtention)
- For documents that do not necessarily require the ‘Approved Date’ and ‘Revision & Versioning’, use the date of update;
- (YYYYMMDD_DocType_DocumentTitle_UniqueIdentifier_Revision.FileExtention).

3.7.8 Documentation Submissions

The Contractor’s program to allow a minimum of 21 days for mailing, processing, and review of drawings and data by the Employer. All documents and records must be submitted and managed according to the Project/Plant Specific Technical Document and Records Management Procedure, 240-76992014 as well as the Generation (Gx) Projects Documentation Deliverable Requirements Specification,240-65459834.

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.

The Employer shall ensure that the Contractor is provided with the latest revisions of the mentioned documents.

a) Information Requirements

The *Employer* requires information and data from the *Contractor* for management and execution of the Contract as well as the operation, maintenance and support of the *works*. The *Contractor* to supply all information required in terms of the Contract including, whether or not specified in the Contract, all information necessary for:

- Design reviews and the interface management of the *works*,
- Quality assurance and control,
- Operations, maintenance and training

The scope of supply of information from the *Contractor*, to include the below document list, if applicable:

Typical Document Requirement List	
Document Group	**Description of document type (includes information data sets)**
General	• Equipment arrangement drawings • Piping & Instrument Diagrams (P&ID's) • Engineering and procurement schedule • Equipment list • Isometric drawings • Equipment specifications & data sheets • Drawings and data for all equipment and material • Installation, Operation, and Maintenance (IOM) Manuals • Spare parts list •
Quality Assurance	• Quality assurance manual • Quality control plans • Quality control reports • Weld summary index • Material traceability certificates • Manufacturing test reports • Manufacturing Non-Conformance Reports (NCR's)
Civils & Structures	• Building arrangement and floor layouts • Structural drawings • Architectural drawings • Structural analysis and design report • Foundation drawings • Structural support drawings • Access Platform/Walkway Drawings • Professional Engineering Certificates from Professionally Registered Engineers

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.

Typical Document Requirement List	
Document Group	**Description of document type (includes information data sets)**
Construction	• Transportability study/report (including heavy haul study) • Site management plan (QA, Safety, Environmental etc.) • Construction schedule • Site storage requirements for major equipment • Construction test records • Maintenance records for all equipment while stored on site • Constructability report
Commissioning	• Commissioning schedule • Commissioning procedures • Performance test procedure • Performance test reports • Field test reports and certificates
Operations	• Operating procedures • Plant operational documentation • Plant tech specs • Operating scenarios (for C&I control purposes)
Logistic Support	• Maintenance concept • Plant maintenance documentation • ISI plan/program • Spare parts assessment • Plant RAM analysis • Equipment access and removal paths assessment • Fault finding diagrams
Training	• Training plan • Training manuals and instructions
Safety & Protection	• Fire hazard analysis • Waste management plan
Design Analyses	• Reliability model and analysis • Transient / Transition Analysis • Flow dynamics analysis • Thermo-hydraulic analysis • Pipe Stress Analysis • Maintainability analysis • FMECA / FMEA analysis • HAZOP analysis • 3D model interference checks

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.

Typical Document Requirement List	
Document Group	**Description of document type (includes information data sets)**
Electrical	• Motor list • Electrical load list • Circuit list • Raceway list • Single line diagram • Protection schematic diagram • Electrical load flow and fault studies report • Cable block diagrams • Cable schedule • Cabling routing and cable racking layout diagrams • Cable termination diagrams • EMC and earthing standards report • Earthing layout drawings • Lighting layout drawings
C&I	• Alarm and set-point schedule • Instrument schedule • Instrument data sheets • Mechanical hook-up drawings • Electrical hook-up drawings • Cable Schedule • Termination Schedules • Junction Box GA and Internal Layout • Junction Box and Instrument location drawings • Instrument Stand GA • Maintenance Manuals and procedures • Operating and Control Philosophies • Functional Logic diagrams • Field device calibration certificates • Level measurement installation report
CBMS	• Alarm and set-point schedule • Instrument schedule • Instrument data sheets • Equipment layout drawings • Routing layout drawings • Cable schedules • Termination schedules • Junction Box GA and Internal Layout • Instrument Stand GA • Maintenance Manuals and procedures • Operating and Control Philosophies • Field device calibration certificates • Network architecture • Fire risk assessments

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) Drawings

The creation, issuing and control of all Engineering Drawings shall be in accordance with the latest revision

of the Engineering Drawing Standard, 240-86973501 - to be supplied as part of the enquiry documents. Drawings issued to the Employer will be a minimum of one hardcopy and an electronic copy. The Contractor is required to submit drawings electronically in both native CADD format and PDF format. Drawings issued to the Employer may not be “Right Protected” or encrypted.

c) Documentation Reviews

The Contactor shall conduct design reviews in accordance to the Employers Design Review Procedure,

240-53113685 and participate in all design reviews as specified by the Employer. The Employer shall review and consolidate review comments for submitted documentation by the Contactor. The Contactor shall also make the necessary revisions or rectify noted issues highlighted on the documentation by the Employer.

The Consultant must include the documentation reviews as part of the Design and Construction schedules and allocate appropriate timelines/durations for these activities.

d) Submission of the Contractor’s Design

- The *Contractor* submits all design documentation to the *Employer* for review. The documentation submitted to include all design elements i.e. drawings, calculations, reports etc.
- The *Employer* conducts a review of the design documentation. The *Employer* reserves the right to review any design in detail, where deemed necessary. The *Employer* accepts no accountability and liability due to the review of any designs.
- The *Contractor* is the Design Authority as defined in the Design Review Procedure, 240-53113685 for the *works*. The *Contractor* is responsible for following this design procedure and conducts all the design reviews as specified in this procedure.
- The following process will be followed for submission of documents:
  - The *Contractor* submits the documents/drawings to the *Project Manager*.
  - The *Project Manager* distributes the documents/drawings to all relevant parties within the *Employer’s* project team to review
  - The *Employer’s* project team reviews the documents/drawings and submit all comments or inputs to the *Project Manager*. The *Project Manager* submits the review comments to the *Contractor* for consideration.
  - If the *Employer* finds major deficiencies in the submitted documents/drawings, the *Contractor* revises the documents/drawings and resubmits to the *Project Manager*.
  - The *Employer* reviews the documents/drawings and if no major deficiencies are found, the *Contractor* organises a review session.
  - The *Employer* and the *Contractor* conduct a review.
  - If any fundamental errors are found in the review or further actions are required, the *Contractor* records all concerns raised and revises the documents/drawings accordingly.
  - The *Contractor* organises a review session once all documents/drawings have been revised
  - If no fundamental errors are found in the documents/drawings during the review session, the *Contractor* compiles the review minutes/report and submits to the *Employer*.

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.

- The *Employer's* project team reviews the *Contractor's* report/minutes. If the report/minutes are not acceptable, the *Contractor* revises the report/minutes and resubmits to the *Employer*.
- The *Employer* accepts the *Contractor*'s documents/drawings once the report/minutes are accepted by the *Employer's* project team.

e) Acceptance of the Contractor's Design

The *Contractor* is to implement the following activities for design acceptance:

a) The *Employer* accepts the *Contractor*'s design upon completion of reviews by the project team

b) The *Contractor* stamps, dates and signs his design drawings, to signify approval of his designs.

c) The *Contractor* informs the *Employer* in writing of any deviation in the *Contractor*'s drawings, from scope requirements.

3.8 Other requirements of the *Contractor*'s design

Plant material coding shall be done as per the Eskom Plant Labelling and Equipment Description Standard 240-71432150.

3.9 Use of *Contractor*'s design and Intellectual Property

The Contractor warrants that all designs, drawings, software, firmware, databases, algorithms, engineering calculations, documentation, specifications, reports, models, artificial intelligence (AI) models, machine learning models, interfaces, source data, configurations, and other deliverables developed or supplied under this Contract are either the original work of the Contractor or are lawfully licensed for the intended use. The Contractor shall indemnify Eskom against any claims arising from infringement of third-party intellectual property rights.

Unless otherwise agreed in writing, ownership of the Contractor's pre-existing intellectual property shall remain vested in the Contractor. However, the Contractor hereby grants Eskom a perpetual, irrevocable, non-assignable, non-transferable royalty-free, non-exclusive licence, with the right to sublicense within Eskom Holdings SOC Ltd and its successors, to use, operate, access, reproduce, modify, adapt, maintain, repair, enhance, integrate, duplicate for backup purposes, and further develop all deliverables provided under this Contract for Eskom's business purposes within South Africa.

Where the Contract includes software applications, AI models, predictive analytics, digital twins, historian integrations, edge computing platforms, or other digital solutions, the licence granted to Eskom shall include all configuration files, model parameters, interface definitions, APIs, metadata, documentation, training material, engineering databases, and all information reasonably necessary for Eskom to independently operate, administer, maintain, troubleshoot, migrate, upgrade and modify the system throughout its operational life.

The Contractor shall not incorporate any third-party software, libraries, open-source software, proprietary components, or intellectual property that imposes restrictions on Eskom's continued operation, maintenance, modification or future expansion of the system without Eskom's prior written approval. The Contractor shall provide a complete register of all third-party intellectual property incorporated into the solution together with the applicable licence terms.

All project-specific deliverables, including engineering drawings, functional design specifications, detailed design documentation, system architecture, configuration databases, asset registers, integration specifications, interface documentation, cybersecurity configurations, commissioning records, training documentation, maintenance procedures, operating manuals and other documentation prepared

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.

specifically for this Contract shall become the property of Eskom upon acceptance and payment, subject only to the Contractor's retained ownership of pre-existing intellectual property.

The Contractor shall not implement any technical protection mechanisms, licence restrictions, time-limited licences, hardware locks, encrypted access controls, remote disablement functionality, or other mechanisms that prevent Eskom from fully operating, maintaining or modifying the supplied system following Final Acceptance. Eskom shall receive all licences necessary for unlimited operational use throughout the expected service life of the installation.

Where source code, scripts, AI models, or software developed specifically for Eskom form part of the deliverables, Eskom shall receive unrestricted access to such source code and associated documentation. Where commercially available proprietary software is supplied, the Contractor shall provide all licences necessary for Eskom to use, maintain and upgrade the software in the contract period.

The Contractor shall ensure that the design enables interoperability with Eskom's existing Operational Technology (OT) and Information Technology (IT) environments, including historians, SCADA, DCS, CMMS/EAM systems, digital twin platforms, enterprise data platforms and future systems without creating vendor lock-in. All interfaces shall utilise recognised open standards where reasonably practicable.

The Contractor shall provide all documentation, engineering tools, configuration utilities, passwords, encryption keys (where operationally appropriate), administrator accounts and licences necessary to enable Eskom personnel or Eskom-appointed third parties to operate, maintain, modify and support the system independently after handover.

No intellectual property rights or licensing arrangements shall limit Eskom's ability to undertake future maintenance, extensions, upgrades, cybersecurity improvements, replacement of components, migration to new platforms or integration with future technologies.

The obligations contained in this clause shall survive completion, termination or expiry of the Contract.

3.10 Design of Equipment

None.

3.11 Equipment required to be included in the *works*

None.

3.12 As-built drawings, operating manuals and maintenance schedules

The Contractor is responsible to plan for the supply of the documentation during the design, supply, installation, testing, commissioning and handover of all the systems and document is thus any written or pictorial information describing, defining, specifying, or certifying activities, requirements, procedures and or results.

All documentation (entire architectural, layouts, diagrams, drawings, datasheets etc.) issued by the Employer for this contract is copyright protected and are not to be copied or distributed by the Contractor.

The Contractor shall submit all documentation on a formal transmittal form in triplicate to the Project Manager. All documents, reports and engineering documentation shall be compiled and presented in English language be in the required Microsoft Office Word, PowerPoint, Excel, PDF, MicroStation and or Project file extensions format.

The Contractor shall implement a legible, comprehensive, and complete documentation (control system), including their revision status and of the document status in relation to the "as designed" system status.

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.

Software licence, network architecture manuals and drawings, document control, loop diagrams, termination diagrams are included.

The drawing documentation format shall include:

Drawing number (Employer and makers number)

i. Revision.
ii. Approval status.
iii. Location of drawing at that stage.
iv. Drawing KKS number.
v. Drawing description.
vi. Sheet number.

3.13 Transmittal number Plant and Materials

3.13.1 Quality

a) The Contractor is responsible for defining the level of QA/QC (intervention Points) or inspection to be imposed on his Subcontractors and suppliers of material in the Quality Control Plans (QCPs).
b) The Contractor submits monthly, the following QA returns:
   - A register of Defects with those older than 30 days being flagged, and an explanation attached.
   - Register of accepted Defects.
   - A register of Non-Conformance Report.
   - Monthly Project Quality Report.
   - Monthly updated Site and pre-site programmes.
   - Inspection dates.
   - Site Acceptance Tests.
   - Inspections completed / outstanding.

3.13.2 Plant and Materials provided “free issue” by the *Employer*

None.

3.13.3 Spares and consumables

The Contractor shall provide local spare-parts support with on-site delivery capability within 24 hours and shall provide evidence of an established local spare-parts warehouse.

Authorisation

This document has been seen and accepted by:

Name and Surname	Designation

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. Revisions

Date	Rev.	Compiler	Remarks

5. Development team

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

Name	Designation

6. Acknowledgements

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.