Eskom	Report	Transmission

Title: **TRANSMISSION SECONDARY PLANT CONFIGURATION MANAGEMENT SOLUTION REQUEST FOR INFORMATION**

Unique Identifier:	**240- 171000306**
Alternative Reference Number:	**N/A**
Area of Applicability:	**Engineering**
Documentation Type:	**Report**
Revision:	**1**
Total Pages:	**36**
Next Review Date:	**n/a**
Disclosure Classification:	**Controlled Disclosure**

Compiled by	Functional Responsibility	Authorized by
Tjaart Visser	**Mpumelelo Mathe**	**Judith Malinga**
Senior Engineer – Control & Automation	**Manager - Control and Automation technology**	**Senior Manager – PTM&C**
Date: 12/12/2023	Date: 2023/12/12	Date: 12/12/2023

PCM Reference: **N/A**

SCOT Study Committee Number/Name: **N/A**

Content

Figures

Tables

1. Introduction

Eskom Transmission (TX) substations are populated with various equipment, configurable electronic devices, and Intelligent Electronic Devices (IEDs) from different Operational Technology (OT) business units, which collectively make up the secondary plant. Therefore, accurate configuration management of the secondary plant devices is critical in ensuring that primary plant and secondary plant are operating correctly.

TX Grid expansion and substation modernization are causing the amount and variety of secondary plant to continually increase. Furthermore, the secondary plant fleet is further complicated by multiple generations of the same IEDs running different firmware, configured with different versions of software tools and an increase in settings/configuration changes as TX maintains and continually improves its secondary plant. Driving the need for TX's configuration management to evolve.

A holistic Configuration Management Solution (CMS) is required to service the next evolution of TX's configuration management. A CMS that is a collective body of processes, activities, tools, methods, data and related documentation used to manage the configurations of grouped and individual devices throughout each device's operational life. The CMS needs to seamlessly integrate with TX's remote engineering solution to leverage the security framework and configuration related features.

This document details the Request for Information (RFI) from the market for such a CMS in terms of:

- Architecture Requirements (system architecture, system redundancy, Business Continuity Plans)
- Engineering Requirements
- Service Requirement
- Functional Requirements
- Project Requirements (Product Roadmap, Indicative Pricing, Training offered, Skills, Support and Industry Experience)

2. Supporting clauses

2.1 Scope

The objectives of this RFI are to:

- Develop an understanding of the Suppliers' (including their related experience) technology, products and/or functionality available for a Transmission CMS that can service all the layers of an Advanced Remote Engineering Platform (AREP) in OT.
- Understand the Suppliers' (including their related experience) technology and/or functionality for coupling configuration software tools server\s with configuration management.
- Understand service offerings around scoping, development, testing, deployment, and maintenance of both analytics and dashboards.

- Understand the suppliers' training, licensing, support and maintenance offerings; and
- Obtain indicative pricing. Costs shall be provided in ZAR excluding VAT. If costs are subject to exchange rate changes, the foreign portion and exchange rates used shall be provided.

It is imperative to note that this document does not necessarily imply a requirement for a single system solution. Details, technical and financial information shall be provided where third (3rd) party solutions are integrated in the CMS.

2.1.1 Purpose

The RFI scope is to enable the provision of a sustainable solution that consists of (but not limited to) a TX Configuration Management (CM) system, Configuration Management File Storage (CMFS) and a Configuration Tool Management System (CTMS). The CMS will be centrally located in the enterprise, servicing multiple TX business units that are distributed across South Africa. The solution shall also provide device data modelling facilities, as well as provide analytics and dashboard visualisation facilities.

Furthermore, the RFI shall inform the integration of the Transmission AREP, known as the Engineering server And Data concentrator Solution (EADS). The TX CMS users will be on Eskom's corporate network from where access to the CMS will be required.

2.1.2 Applicability

This document shall apply to the Eskom Transmission division.

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] 240-170000566: Telecontrol Equipment Configuration File Management Standard

[3] 240-77942896: Protection Equipment Configuration File Management Standard

[4] 240-55410927: Cyber Security Standard for Operational Technology

[5] 32-373: Information Security - IT/OT Remote Access Standard

[6] 240-91479924: Cyber Security Configuration Guidelines of Networking Equipment for Operational Technology

2.2.2 Informative

None

2.3 Definitions

2.3.1 General

Definition	Description
Application Server	Runs specific applications and provides services such as application hosting, middleware, and application execution.
Configuration	The arrangement, composition, or specific setup of components, elements, or parameters within a system, device, software, or any other organized structure. It can involve the way various parts or elements are organized or connected to achieve a specific function or purpose
Configuration Management	Its responsibility lies in capturing and preserving engineering data, encompassing functional and physical characteristics, design details, processes and operational information, throughout the entire lifespan of Eskom's transmission assets.
Database Server	Manages database operations, allowing clients to retrieve or store data in a database.
File Server	Stores and manages files, allowing clients to access and share data within a network.
Firewall	Network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It acts as a barrier between a trusted internal network and untrusted external networks, such as the internet. The primary purpose of a firewall is to establish a security perimeter that helps prevent unauthorized access.
Intelligent Electronic Device (IED)	An intelligent electronic device is an integrated microprocessor-based controller of power system equipment (primary plant), such as circuit breakers, transformers, isolators, etc.
Remote Engineering	Refers to the practice of performing engineering tasks, projects, or activities from a location that is separate from the physical site where the work is being carried out. In other words, engineers and engineering teams can collaborate and contribute to projects without being physically present in the same location.

2.3.2 Disclosure classification

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

2.4 Abbreviations

Abbreviation	Description
AREP	Advanced Remote Engineering Platform
CFMS	Configuration Files Management system
CM	Configuration Management
CMS	Configuration Management Solution
CTMS	Configuration Tools Management system
EADS	Engineering server And Data concentrator Solution
FAT	Factory Acceptance Test
GUI	Graphical User Interface

Abbreviation	Description
IED	Intelligent Electronic Device
IT	Information Technology
OT	Operational Technology
PTM&C	Protection, Telecommunications, Measurements & Control
RFI	Request for Information
SAT	Site Acceptance Test
URS	User Requirement Specification
VPN	Virtual Private Network
TX	Eskom Transmission

2.5 Roles and responsibilities

The Supplier is required to respond to the Standardisation, Information and Pricing schedules.

The guideline on how to complete the schedule, is included on a tab with the schedules. The numbering of the requested information shall be retained. The supplier shall include hyperlinks to supporting document paragraphs, on the electronic copy of the schedules.

Optionally, the Suppliers are encouraged to provide a demonstration of their products which form part of their configuration management solution on which the RFI submission is based. This demonstration shall be limited to a day demonstration, at a selected Eskom site (preferred) in Johannesburg. Suppliers shall be advised of their selection for the demonstration, the exact date and time of the demonstration two weeks prior to the demonstration. The Supplier is requested to respond to the questionnaire on the Demonstration schedule.

The supplier shall submit both electronic and hard copies of the schedules and additional supporting documents.

2.6 Process for monitoring

None.

2.7 Related/supporting documents.

None.

3. Configuration Management Solution (CMS)

3.1 Background

Eskom TX substations contain configurable secondary plant devices that perform various functions such as Protection, Metering, Telecontrol, and DC supply of the substation. Secondary plant device examples are: IEDs, Chargers, Meters, Transducers, Switches, Routers, Firewalls, Recorders, etc. Correct operation of these functions is reliant on these devices being correctly configured through configuration management. Configuration management is a process for establishing consistency of a product's attributes throughout its life cycle. These attributes include processes, activities, tools, documents and methods used through the products life cycle.

Eskom TX has been using Bentley Project Wise, an engineering drawing and document management system, as a configuration file repository. Together with supporting documentation prescribing governing processes and procedures, a basic configuration management system was established. Currently, OT secondary plant configuration files for protection and control equipment have not been adequately managed and controlled. In conjunction with Project Wise. Eskom TX uses Virtual Machines (VMs) to manage configuration tools which are unique for each department within TX. Virtual Machines are stored in users' own laptops and not centralised within any server. Eskom TX intends to have a centralised location to host VMs that will be used to grant CMS users access to configuration tools for the purpose of updating/changing configurations. Vastly reducing the need for untracked and unaccounted configurations to exist on technician laptops.

Unrelated to the existing configuration management, but applicable to the next evolution of the CMS, is the EADS system which is currently being finalised. The EADS system will enable Eskom TX to realise the benefits acquired by implementing a secure remote access system to its OT assets. The EADS solution will be based on a deployment of the enterprise engineering server (PowerSYSTEM Centre developed by SUBNET Solutions Inc.) with a high availability architecture. PowerSYSTEM Centre is SUBNET's Engineering Server that provides user access to connect to IEDs in the substation. Once connected to the devices remotely, users have the ability to interact and manage devices without being required to travel to the substation for local access. PowerSYSTEM Centre provides a secure remote proxy infrastructure to allow for users to access end devices with vendor-specific applications, removing the need for decentralised VMs for local IED configuration.

This document details Eskom's expectation with regard to all the components and sub-systems contributing to the Configuration Management Solution as well as the extent to which the integration of the components shall provide a transparent / seamless solution for the end-user.

3.1.1 Philosophy

The upgrade and/or migration of the Project Wise configuration management shall comprise of standard hardware and software with special developments being kept to a minimum. The life cycle of the CMS is 15 years. A single Graphical User Interface (GUI) for all services provided by the configuration management system is preferred. Where this is not possible, it should be clearly stipulated that additional GUI's are used.

Standardisation Schedule:

I. Special developments shall be clearly identified and documented as to their nature and depth in a delta design document.

II. GUI Interfaces should preferably be kept to single interface.

Information Schedule:

I. Describe how configuration tools are best used with a CM system. If not, how can this be achieved.

II. Indicate whether the CM system can manage the configuration tools as well.

3.2 Engineering Design Requirements

3.2.1 Architecture

The CMS architecture is not firm and can align to technology best practice deployment and service options in the market.

3.2.1.1 Criteria

The fundamental design criteria for the design and implementation of the CMS system are high availability, high reliability and maintainability:

Standardisation Schedule:

I. The desired high availability shall be achieved by means of hardware and software redundancy with failover and/or clustering mechanisms where this is practically achievable even during power system disturbance conditions.

II. High reliability shall be achieved through the installation of a field-proven system based on engineering best practices, principles and guidelines.

III. Maintainability shall be achieved through system monitoring and configuration management.

IV. Hardware components which are identified as critical shall be duplicated to allow for software and hardware upgrades without losing the overall redundancy criteria during the period of upgrade or failure.

V. It shall be possible to have a complete system recovery within an hour.

3.2.1.2 Redundancy

The configuration management system should ensure that established procedures for backups and archival are followed consistently and completely. Back-up copies should be taken regularly to ensure that a copy of the CMFS will be available in the event of a disaster. The historical data in the CMFS should also be archived according to the configuration management policy. The amount of data retained will depend on the value of information to the organisation.

Standardisation Schedule:

I. The full redundancy of the CMFS system shall be extended over two (2) separate installation instances.

II. The third (3rd) clustering / voting node, if required, shall be located outside the redundant configuration.

III. Redundancy shall be available for all data transfer done through a data gateway in the Demilitarized Zone (DMZ).

IV. Non-production servers (except for pre-production) in the development and testing environment shall be virtualised where feasible and run on common physical servers using virtualisation software.

V. The configuration management system shall be able to withstand regular loss of power, and to automatically restore to operational state, either as master or standby / reserve function without human intervention and/or data corruption.

Information Schedule:

I. Describe what the ideal CMS redundancy architecture should be for sub-systems of the CMS.

II. Indicate whether redundant configuration management systems should be considered.

III. Indicate how virtualising CMS software can be applied to reduce overall project cost.

IV. Indicate how virtualising CMS software can be applied to optimise CMS redundancy.

3.2.1.3 Business Continuity

The CMS shall have a single Disaster Recovery and Business Continuity Manual, which will ensure the solution complies with the requirements of the Cyber Security policy for Operational Technology.

Standardisation Schedule:

I. Backups for business continuity shall be done on the non-active CMFS system such that no functionality is lost during the backup and/or restore. Thus, when a single node is required for backup, a non-redundant CMFS system shall be available on the non-active system as a disaster recovery system.

II. Periodic system maintenance shall not reduce the efficiency of the system failure recovery.

III. There shall be a functionality to alarm any data mismatch between the redundant CMFS systems.

Information Schedule:

I. Describe which technologies/mechanisms are used to ensure that data shall not be lost during a failover and/or system switch-overs.

II. Provide information on expected availability / uptime of the solution

3.2.1.4 Network Segmentation

The CMS system operational network shall be segmented to control the data flow and/or access between users and/or processes in the different security zones.

Information Schedule:

I. Provide a description of the security zones used for all the servers/nodes of the CMS system and how the zones are physically and logically isolated.
II. Indicate how port numbers can be modified/configured not to use default/standard ports in the CMS.
III. Indicate how open ports can be limited.

3.2.1.5 Maintenance and Engineering Workstations for the CMS

Standardisation Schedule:

I. Maintenance workstations required for the maintenance and support of the CMS system has additional logical access control and cannot be used for secondary plant configuration management.
II. Remote workstations used for maintenance and support of the CMS system shall conform to all the Eskom remote access policies and standards.

3.2.2 Standards

The CMS system shall conform to international industry standards with respect to all hardware, software, operating systems and database implementations. An open architecture shall be provided, supporting the ongoing evolution of these standards, additional development of existing functionality provided by the CMS system and the integration of new functionality.

3.2.2.1 Licensing

The CMS system shall use Open Source Licensing where available. It is required to make use of existing corporate software and hardware licenses and maintenance agreements in adherence to Eskom policies and standards.

Information Schedule:

I. Describe the licensing model for the CMS and list the variable inputs used in the calculations.
II. Identify and list separately / individually all third (3rd) party software licences and maintenance agreements, required for the CMS system.
III. List all propriety licenses.

3.2.2.2 Technologies

The system shall comply with the recommended standards for technology in Eskom.

Information Schedule:

I.	Indicate where Open Source technologies are used in the CMS solution.

3.2.2.3 Enterprise Historian

Information Schedule:

I.	How does the CMS interface with third (3rd) party plant historians.
II.	What integration do you provide to an enterprise plant historian.

3.2.2.4 CMS Hardware

The hardware requirement includes all servers, network equipment and workstations. The hardware design specification shall include the calculation of CPU processing, power requirement, memory, I/O requirements, power requirements, network requirements, short term and long term storage solutions.

Eskom shall involve the approved hardware supplier during the initial work statement to finalise the hardware configuration and discuss the following issues:

- Certification of hardware with proposed operating systems and third (3rd) party software;
- Certification of hardware for any high availability cluster support; and
- Local support policies.

Standardisation Schedule:

I.	The computer system design shall comply with the physical redundancy of all hardware. The hardware redundancy ensures data redundancy on the database and file servers. A power failure to half the system, where the remaining half automatically takes over all functionality with no effect to the users, is a contingency for failure recovery. The network design shall also include redundancy between CMS sub-systems.
II.	Hardware supplied shall be part of a product range of compatible equipment, to minimise training and maintenance costs. All hardware used shall be supported by local agents.
III.	USB ports shall be disabled on all hardware.
IV.	It shall be possible to upgrade the hardware performing the critical cyber security function to facilitate the deployment of the latest firmware and patches.
V.	Although the hardware required for the CMS system shall be evaluated against the hardware standards from Eskom, it is required to deploy the system on native hardware. Virtualisation may be considered for CMS sub-systems.
VI.	The hardware, operating systems and third (3rd) party software shall be procured and installed directly by Eskom or its subcontractors with approval from the OEM.

VII. As part of the pre-installation of the CMS, a hardware validation and quality control / benchmark for performance shall be done.

Information Schedule:

I. Indicate how the hosting / deployment servers and software for third (3rd) party OS and anti-virus updates can be configured as part of the CMS configuration.

II. Indicate where blocking of USB ports can interfere with the operation of CMS.

III. Indicate how the hardware support from the vendor can be extended to align with the expected life cycle of the CMS system (15 years).

IV. Indicate how the hardware upgrades comply with the hardware vendor's support warranty in the event where the hardware support cannot be extended to align with the life cycle of the CMS system.

3.2.2.4.1 Network

The computer system design shall allow for the physical and logical isolation of areas by making use of multiple computer networks. The logical isolation of areas shall support the network layout as defined for the multiple demarcated security zones.

The system shall be able to be configured to a minimum operating and control system with all external connections disabled or disconnected. This shall be achieved with the use of intelligent network devices with filtering and cyber security features.

Standardisation Schedule:

I. The interconnections between different buildings and different floors / equipment rooms shall be based on fibre optic links between the switches.

II. The network shall be in a fully redundant configuration, as required to meet the performance requirements.

III. Failure of any single network segment shall not degrade system performance requirements. Thus, the network shall be configured for high availability and shall ensure that any single failure shall not impact performance.

IV. The removal, powering off, or malfunction of equipment connected to the network shall not interfere with operating of the CMS system.

V. Inter application communication within and to an external to a server, must have dedicated network ports, configurable by user. Third (3rd) party software that makes use of commonly known ports must pass through Intrusion Prevention Systems in-order to perform in-depth analysis of the data frame.

VI. The system shall have the functionality for configuration of priorities for quality of service and redundancy at all levels of the network OSI model.

VII. The network design and specification shall calculate bandwidth requirement for flows between applications, databases, servers and networking equipment for LAN and WAN zones.

VIII. Network traffic to remain within a security zone for redundancy communications.

Information Schedule:

I. Provide a schematic layout of the network split up into logical segments, in order for sections to be disconnected during periods of disturbances.

II. Indicate the bandwidth requirements to perform remote upgrades, real-time 3D graphic and video streams.

III. Provide information on the use of demarcated security zones in the CMS network configuration

3.2.2.4.2 Servers

Servers hosting more than one virtual machine shall be of a higher model than servers running a native operating system. For each server hosting more than one virtual machine, doubling the hardware specification is required.

Redundant database and file servers shall serve as the repositories for shared software, shared data, database definitions, and historical information. The database and file servers shall automatically ensure that critical information is not lost upon failure of any single disk drive.

Standardisation Schedule:

I. Servers running the operating system native without virtualization or hosting only one guest virtual machine shall have at least two (2) processors, four (4) network adapters, RAID controllers with backup battery configured as at least RAID5 storage, redundant power supplies and an integrated management module offering console redirection.

II. Servers hosting multiple virtual machines shall have at least four (4) processors, four (4) network adapters, RAID controllers with backup battery configured as at least RAID5 storage, redundant power supplies and an integrated management module offering console redirection.

3.2.3 Cyber Security

3.2.3.1 Policies and Standards

Security shall be aligned to the requirements from the North American Electric Reliability Corporation (NERC) on critical infrastructure protection supplemented by ISO/IEC 27002.

The CMS shall comply to the following policies and standards:

- 240-55410927: Cyber Security Standard for Operational Technology
- 32-373: Information Security - IT/OT Remote Access Standard

- System to be fully NERC CIP compliant, including the delivery and implementation of the configuration of parameters throughout the 7 layer OSI model.
- 240-72942279: EMS and DMS Master Station Computer Disaster Recovery Standard
- 240-91479924: Cyber Security Configuration Guidelines of Networking Equipment for Operational Technology
- 240-79669677: Demilitarised Zone (DMZ) Designs for Operational Technology

3.2.3.2 Technologies

Information Schedule:

I. What anti-virus software is preferred on all the components of the CMS.
II. List any intrusion penetration software used in the CMS and where and how it will be used.
III. Provide details on any auditing software configured on the CMS.
IV. Define what end point security is deployed / recommended on the CMS.
V. Are there any hard coded usernames and password used in the CMS solution. If any, how is this managed.
VI. Provide details on how remote access – from the supplier into the CMS - is managed.

3.2.3.3 Methodology

The focus of the security architecture shall be to design and implement the following security guidelines:

- Defence in depth: Layered security (i.e., protection mechanisms at multiple levels).
- Hardened platforms: Secure system installation/build.
- Deny by default: Explicit rules required to allow access.

Network-level security shall govern the types of network access allowed among the various security domains with which the CMS system can potentially communicate. These requirements shall apply to both the physical and the logical configurations of various network segments.

System (host-level) security shall determine the access allowed among hosts, services, applications, and users in the various security domains that potentially communicate with the CMS system. Host and application security measures to achieve the desired results shall be deployed to comply with the cyber security policies and standards.

A migration path shall ensure that the Operating System's kernel, hardware layer, system library, shells and system utilities remain updated and supported.

All workstations connecting from the Eskom corporate network shall conform to the user authentication, authorisation and accounting policy using radius servers for workstations to authenticate engineering and maintenance users and authorise their access to the requested system or service.

Information Schedule:

I. List any concerns and provide actions to mitigate the risk associated with non-compliance with the proposed methodology for cyber security on the CMS.

II. Describe all best practices and standards integrated in the CMS solution for cyber security.

3.3 Functional Requirements

The intent of the CMS system is to perform the following functions:

- Provide a controlled environment\system to manage and store all the secondary plant configuration files:
    - Management of master configuration files.
    - Management of as built configuration files.
    - Version control of all configuration files.
    - Enable secure, controlled, authorised configuring of secondary plant.
    - Govern separation of duties.
    - Provide change management.
    - Reduce offline or untracked configuration files of user laptops.
- Provide a platform for users to create, view, edit, review configuration files without the need to remove the configuration file from the CMS environment, as far as possible.
- Manage incompatibility of configuration software tools against secondary plant devices in an attempt to prevent devices being configured with older or newer software tools which are causing corrupt or false positive configurations leading to maloperation.
- Integrate with a remote engineering platform (EADS) to leverage:
    - Authentication, Authorisation and Accounting (AAA) framework
    - Secure remote proxy infrastructure to allow for users to access end devices with vendor-specific applications.
    - Gathering secondary plant device information (device name, firmware version, hardware version, configuration file, etc.)
- Enable auditing and reporting:
    - Config mismatch - highlight operational devices using a configuration not recorded in the CMFS.
    - Checking for unauthorised software
    - Event logs to record actions taken on the CMS by CMS users
    - Secondary plant device tracking

Merging a CMS system with an AREP can be beneficial as there will be some overlap in functionality. See *Annex A – Engineering And Data concentrator Solution System* for an overview of the EADS Transmission architecture. The list below details the SUBNET software which TX is strongly considering using in the EADS AREP:

AREP component	**Software**
Enterprise engineering server - Centralized Device Management	PowerSYSTEM Center 2023
TX substation - Engineering Workstation Substation Computing Platform	SubSTATION Center v2023

3.3.1 Configuration Management Solution

Standardisation Schedule:

I. The CMS is able to ingest and manage vendor specific configuration files: e.g. SCD, ICD, CID. (see Annex B for a more comprehensive list of configuration files)

II. The CMS is able to ingest and manage PDF Documents related to Training Manuals, configuration guides, commissioning guides and application guides.

III. The CMS shall cater for varying size and type of configurations in its native format.

IV. The CMS configuration files shall have a standard naming convention.

V. Hardware model and firmware version of a device shall be populated or associated with each configuration file.

VI. Configurations checked-out for editing to be checked out only to a single user at any one time.

VII. Configurations checked-out by user details to be captured by the system and clearly displayed.

VIII. Configurations to be checked-in must be verified for a change. Should there be a change in that configuration, the system shall automatically revise that version of the configuration, during the check-in process.

Information Schedule:

I. Indicate whether the CM system has limitations in terms of the file types and/or sizes which can be ingested by the system.

II. Describe how a configuration file can be locked by an administrator or a CMS user which is busy updating the configuration.

III. Indicate whether the CM systems configurations can have meta data associated with the device entry.

IV. Indicate if the CM system can compare a file with the existing file on the system when it is checked back in, and if so, how does the systems compare the two file instances.

V. Indicate whether CM systems typically include a CMFS or if the CMFS is a standalone storage server or both.

VI. Indicate what checked-out by user details can be displayed in the CMS GUI.

VII. Indicate whether a checked-out configuration and still be copied or read by other users.

VIII. Describe how configurations to be checked-in, can be verified for a change against the version which was checked out.

IX. Indicate whether the CMS will ignore an unchanged file being checked in or just override the stored file anyways.

X. Describe how the CMS can compare configuration files to determine if they are different.

XI. Indicate how configuration file integrity can be checked and verified during check-in.

XII. Indicate whether PowerSYSTEM Center and/or SubSTATION Center can seamlessly be integrated to a CMS. If not, then describe how this is accomplished.

XIII. List available meta data fields in a CMS system which can be used to enable easy reference and searching.

XIV. Indicate whether the CMS has a search function which can search based on meta data fields.

XV. Indicate other known Remote Engineering Platform software, like PowerSYSTEM Center and SubSTATION Center, which can facilitate the remote configuration interactions with secondary plant.

XVI. List and describe CMS systems which has the remote engineering/ configuration built in.

XVII. Indicate whether CM systems include functionality to interface to a CTMS. If not, how can this be achieved.

XVIII. Describe the flexibility which the CMS has to present\package configurations in a hierarchical structure, i.e.: Substation > voltage level > bay.

XIX. Describe how the CMS can retrieve configurations on secondary plant. If not, how this can be accomplished.

3.3.2 Configuration Tools Management System

The CTMS shall include the capability to host VMs on which the various configuration tool software is installed.

The CTMS must be able to interact with the CMS to check-out, edit and check-in configurations (role based access dependant).

Standardisation Schedule:

I.	Users on the CTMS shall be able to access configurations on or from the CMS without the configuration leaving the security zone.

Information Schedule:

I.	Indicate whether and off the shelf CTMS is available. If not, how this can be accomplished.
II.	Describe the maximum number of VM instances which the CTMS should be restricted to per server.
III.	Describe how CTMS VM servers should be scaled as users of the CTMS increase.

3.3.3 Substation Devices

Configurable substation devices are listed in **Error! Reference source not found.** in Annex B.

3.3.4 Access Control

Granular access control has largely been standardised on the following roles:

a. **Basic user** - with read only access.

b. **Advanced user** - with read and write access.

c. **Administrator** – with the ability to add / remove user access and manage the system.

Standardisation Schedule:

I.	Role-based access shall be implemented.
II.	The administrator of the system shall have the capability to manage the users role-based access permissions.

Information Schedule:

I.	Indicate whether a Lightweight Directory Access Protocol (LDAP) server can be used for the CMS.
II.	Indicate whether an Active Directory (AD) server can be used for the CMS.
III.	Describe how the same user authentication server can be used for both the CMS and CTMS.
IV.	Indicate whether role based access for user can be defined based on discipline and/or customised groupings/tags.
V.	Describe how the CMS can handle the scenario where a user has checked-out a configuration and an administrator, in an emergency, needs to edit/update the configuration.

3.3.5 Logs and Reports

The CMS shall log events that occur in the system, such as problems, errors or just information on current operations. Logs of all previous transactions should be made available on the system to all users.

Reporting is the process of collecting and organising data into charts and tables that enable the tracking and monitoring of data and performance metrics.

Standardisation Schedule:

I. Periodic or on demand reports can be generated on the status of configurations.

II. Report shall be exportable in Microsoft Excel format and/or PDF format.

III. Reporting shall have the capability to create customisable reports.

IV. Search facilities shall be available within reports.

V. Filter facilities shall be available within reports.

VI. Each report shall have a configurable scheduling capability. i.e. daily, weekly, etc.

VII. Reporting shall have the ability to email reports automatically.

Information Schedule:

I. Describe how notification and alerts can be achieved in the CMS.

II. Indicate whether multiple configuration files can be combined into a single report.

III. List all the report types possible.

IV. Indicate all the exportable types supported within reports.

V. Indicate whether multiple data sources can be combined into a single report.

VI. Indicate all the exportable types supported within reports.

VII. List all the report types possible.

VIII. List information which the CMS can include in the reporting, i.e.: if the configuration is checked-out, duration of check-out, checked-out by user details, checked-in details, etc.

3.3.6 Notifications

Notification and alert mechanisms can be delivered directly through the client tools or via email. Triggers and notification's structure shall be configurable.

Standardisation Schedule:

I. Notification triggers shall be configurable.

II. Notifications shall be delivered via email with the subject- and body- content being customisable.

III. The structure and content within notification messages shall be customisable.

Information Schedule:

I. Describe how notification and alerts can be achieved in the CMS.

3.4 Service Requirements

3.4.1 Configuration Management System

3.4.1.1 Support for the configuration management system

Support for the configuration management system can include, but is not limited to, on-call support, remote-access support, and physical support and maintenance on-site as required.

Standardisation Schedule:

I. The solution shall receive support from the vendor.

II. Support shall be defined within a Service Level Agreement (SLA).

Information Schedule:

I. Describe support services the vendor can offer, the nature of support, and all components of the solution such support can be extended to.

II. Describe the availability of support (if any) for any additional features useful to the CMS system.

3.4.1.2 Operation of the configuration management system

Information Schedule:

I. Describe any services on offer relating to the operations of the configuration management system.

II. Describe any services on offer relating to the maintenance of the configuration management system.

3.5 Project Requirements

3.5.1 Product Roadmap

Information Schedule:

I. Provide the product roadmap/s for the proposed solution, over the next five (5) years.

II. Describe the product development approach, including the involvement of user groups.

3.5.2 Project Programme

Standardisation Schedule:

I. The five (5) phases of the Project Programme shall adhere to the Secondary Plant Technology Development Guideline (474-313).

The five (5) phases of the Project Programme are:

Phase 1 – Functional Design

Scope ratification shall be conducted with the supplier prior to the start of the project and the Works Information shall be agreed upon.

In this phase the supplier shall be required to produce a Functional Design Specification (FDS) and a System Design Report. The Functional Specification details Eskom's functional requirements in the context of the products that were tendered. The System Design Report documents the design that has been developed in order to meet the requirements as specified in the Functional Specification. This design is a high-level view of the system components and shall include the identification of the principal modules of the proposed system.

Functional designs and detailed designs shall be performed during this phase and will be subjected to approval from the relevant Eskom governance committees. Further details will be provided by Eskom when required.

The deliverables for this phase shall be:

- The Functional Design Specification.
- The System Design Report.

All other relevant documentation including manuals, guides and settings templates shall also be produced by the tenderer during this period.

Phase 2 – Detailed Design

During this phase the supplier produces a Detailed Design Specification (DDS) for both hardware and Software components of the system with special reference to cyber security requirements, as well as the Factory Acceptance Testing (FAT) and Site Acceptance Testing (SAT) Procedures. Acceptance Testing Procedures define all tests to be performed, and the expected results, to qualify that the products comply with the requirements, as specified.

These deliverables shall be individually approved by Eskom prior to the commencement of Phase 3.

The deliverables for this phase shall be:

- The Detailed Design Specification for both hardware and software components of the system.
- Process Document
- Factory Acceptance Test Document
- Site Acceptance Test Document

Phase 3 – Development, System Integration and Factory Acceptance Test

Phase 3 shall commence on completion of Phase 2. Once system integration is complete, the pre-Factory Acceptance Test shall be performed by the supplier and verified by Eskom to determine the accuracy of the Factory Acceptance Test documents. If satisfied with the pre-Factory Acceptance Test results, Eskom shall conduct a Factory Acceptance Test at the supplier's premises.

The deliverables for this phase shall be:

- A signed-off Factory Acceptance Test report.

Phase 4 – Delivery, Installation, Testing and Commissioning

Phase 4 shall commence on completion of Phase 3. Proper arrangements shall be made with Eskom prior to any work on site.

The deliverables for this phase shall be:

- the supply,
- installation,
- testing, and
- commissioning of the prototype equipment.

Phase 5 – Site Acceptance Test

This phase shall consist of performing of tests according to the approved SAT procedure. The deliverable shall be the signed off SAT report. After final testing has been accepted, the products and prototypes are to be fully documented in terms of design drawings and reports, as well as maintenance procedures, any special decommissioning requirements and spares recommendations.

The deliverables for this phase shall be:

- A signed-off Site Acceptance Testing report indicating accepted completion of Site Acceptance Testing.
- A handover Certificate
- Source Code for all software delivered

Information Schedule:

I. Provide an indicative timeline for the proposed five (5) phases of the Project Programme inclusive of the specified deliverables.
II. Indicate any concerns with regards to the project phases or deliverables described above.

3.5.3 Training Offered

Information Schedule:

I. Provide details on the envisioned levels of training for various user groups of the CMS.

3.5.4 Indicative Pricing

Provide costing while using the following breakdown as a guide. Clearly indicate any volume discounts and other relevant information. Costs should be provided in ZAR, excluding VAT for the local portion. The foreign portion should be indicated in the foreign currency.

Table 1: Outline of the Indicative Pricing Required

Activity No.	Activity
1.	**Architecture:**
1.1.	Configuration Management Solution disaster recovery
1.2.	CMS without CTMS:
1.2.1.	Internally - fully hosted (virtualised) on Employer premises and managed by Supplier
1.2.2.	On premise - Supplier installation on Employer premises and managed by Supplier
1.2.3.	Software as a Service
1.3.	CMS with CTMS:
1.3.1.	Internally - fully hosted (virtualised) on Employer premises and managed by Supplier
1.3.2.	On premise - Supplier installation on Employer premises and managed by Supplier
1.3.3.	Software as a Service
1.4.	CMS architecture to interface with secondary plant independent of an AREP
2.	**Functional Requirements**
2.1.	Data Engineering:
2.1.1.	Migration of existing Project Wise configuration repository
2.1.2.	Setup and configuration of the CM system hierarchical structure
2.2.	Inclusion of a Configuration Management File Storage system
2.3.	Integration to an Advanced Remote Engineering Platform
2.4.	Dashboard/GUI for visualisation
2.5.	Client tools
2.6.	Notifications
2.7.	Reporting
3.	**Services**
3.1.	Disaster Recovery and Business Continuity Manual
3.2.	Configuration Management Solution:
3.3.	Firmware upgrade and/or patching
3.4.	Support for the CMS:
3.4.1.	Support service for the CM system
3.4.2.	Support service for the Configuration Management File Storage system
3.4.3.	Support service for the Configuration Tool Management System
3.5.	Services related to the support (if any) for any additional features like dashboard development, development of reports, device auditing, etc.
3.6.	Services related to the operations of the CMS
3.7.	Services related to enhancements of the CMS
4.	**Project Programme Engineering**
4.1.	Phase 1 – Functional Design
4.2.	Phase 2 – Detailed Design

Activity No.	Activity
4.3.	Phase 3 – Development, System Integration and Factory Acceptance Test
4.4.	Phase 4 – Delivery, Installation, Testing and Commissioning
4.5.	Phase 5 – Site Acceptance Test
5.	**Training**
5.1.	List training levels for various user groups
6.	**Hardware:**
6.1.	List of Hardware/Equipment for CMS without CTMS (include detailed hardware specifications)
6.2.	List of Hardware/Equipment for CMS with CTMS (include detailed hardware specifications)
7.	**Software Components**
7.1.	Configuration Management system
7.2.	Configuration Management File Storage
7.3.	Configuration Tool Management system
8.	**Cyber security**
8.1.	List of cyber security Hardware/Equipment
8.2.	List of cyber security software
8.3.	Compliance certification
9.	**Licensing**
9.1.	Operating System/s
9.2.	List third party software required for the solution (price individually)
9.3.	List component licensing (i.e.: SQL/ Relational database/ ODBC, Microsoft Client Access Licenses, etc.)
10.	**Maintenance**
10.1.	Maintenance cost of the solution for a period of 5 years:
10.1.1.	Hardware
10.1.2.	Software
10.1.3.	Spares

3.5.5 Additional Information

Information Schedule:

I. Provide information on challenges, additional functionalities, or improvements to the CMS that you have identified as being beneficial or crucial to this project based on your implementation experience. Align additional responses to the section titles above. Note this is not limited to points raised above.

3.5.6 Skills and Support

Information Schedule:

How many employees are employed by the company locally in South Africa: I. Engineering management II. Engineering design III. Technical support IV. Quality V. Production VI. Installation & commissioning VII. Finance

3.5.7 Industry Experience

Information Schedule:

I. Give a brief summary of your present range of equipment and services available. II. Briefly describe the nature of your resources in the Republic of South Africa e.g. workshop; design; equipment development; testing; and production facilities etc. III. Supplier's comparable sized project experience references. a) State the customer names that you have delivered services to during the past five (5) years. b) List and describe the number of projects that are currently in progress and/planned to start through 2024/25. c) Provide customer references indicated in a and b. d) Provide the original and actual delivery dates of the projects listed above. e) Where applicable provide the major reasons for project completion delays, where handover was delayed for more than six (6) months from the original schedule. IV. State your level of adherence to International Engineering Standards.

4. Authorization

This document has been seen and accepted by:

Name and surname	Designation
Judith Malinga	PTM&C – Senior Manager
Mpumelelo Mathe	PTM&C – Control Automation and Technology Support Manager

5. Revisions

Date	Rev.	Compiler	Remarks
December 2023	1	TC Visser	New document is required that details the RFI questions for a CMS.

6. Development team

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

- Mpumelelo Mathe
- Pitso Sekhoto
- Tumiso Ledwaba

7. Acknowledgements

- Ronny Lehutso
- Mary Mammen

Annex A – Engineering And Data Concentrator Solution system

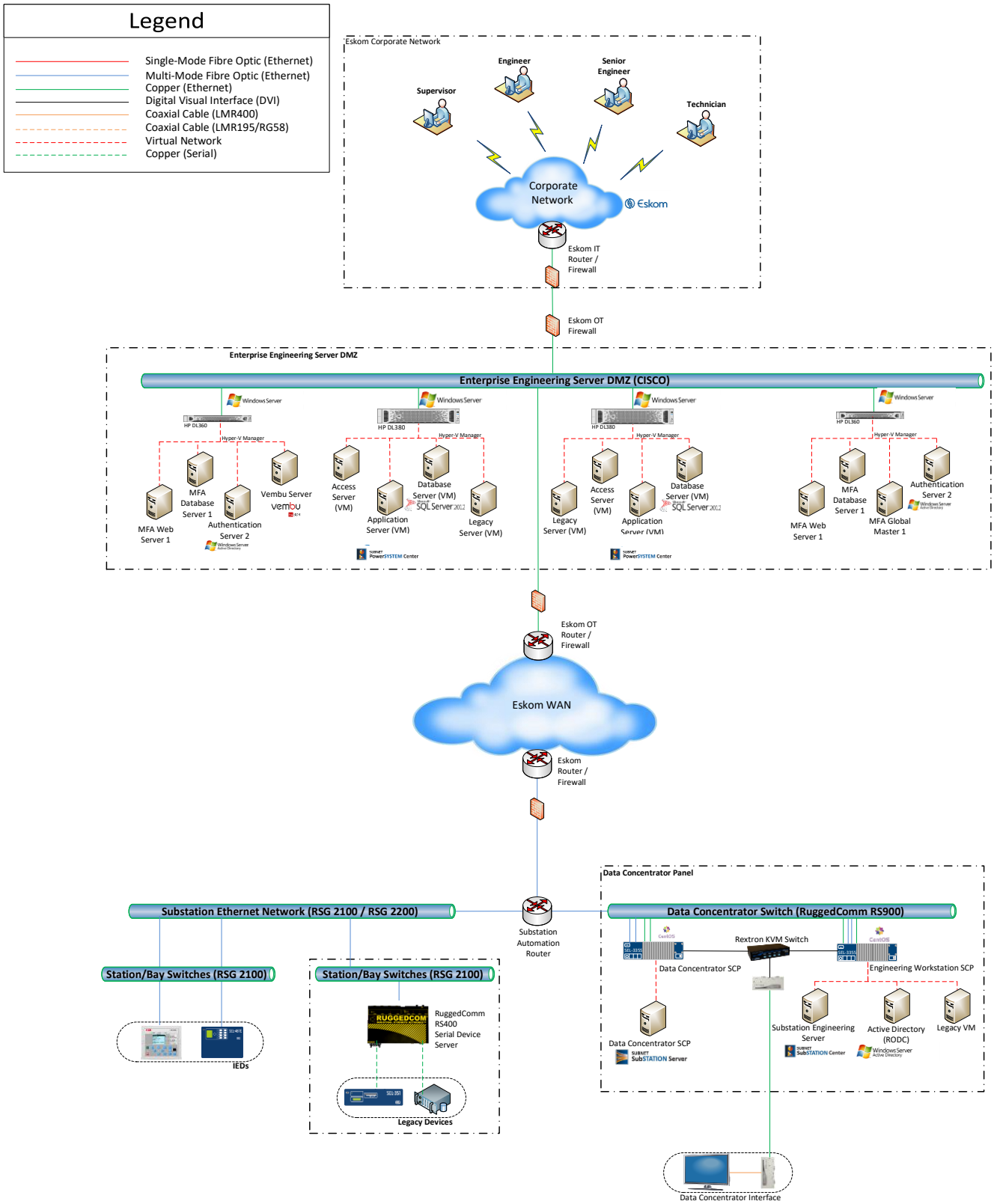

Figure 1: Transmission EADS Architecture

Annex B – Devices and Configuration tool lists

Table 2: Secondary plant devices and their respective configuration tools

Note: The table provides information on devices such as device type, firmware version, configuration tool, configuration tool version, and configuration file type. At the time of the RFI, efforts to conclude the table were still underway. Any missing information can be confirmed if deemed critical.

DC & Auxiliary Supplies					
Devices	**Device type**	**Firmware Version**	**Configuration tool**	**Configuration tool version**	**Configuration file type**
Cordex CXC controller	Cordex controller	N/A	Codex Ver. 2.27		
Cordex CXC controller		N/A	Eskom Language for CXCR Ver		
Cordex CXC controller		N/A	cxcr Configuration file		.cfg
Cordex HP Controller	Cordex chargers	N/A	Codex HP Ver. 7		
Cordex HP Controller	Cordex chargers	N/A	Eskom Language for HP Ver		
Cordex HP Controller			HP Configuration file		.cfg
1 kW Rectifiers	Codex Rectifiers				.ACAN
1.1 kW Rectifiers	Codex Rectifiers				.ACAN
3.3 kW Rectifiers	Codex Rectifiers				.ACAN
4 kW Rectifiers	Codex Rectifiers				.ACAN
4.4 kW Rectifiers	Codex Rectifiers	1.14			.ACAN
Digital UPS					

Digital DC-DC Converter			Codex HP Ver. 7		
Metering					
Devices	**Device Type**	**Firmware version**	**Configuration tool**	**configuration tool version**	**Configuration file type**
ABB	Transducer		Contrans E-SU		SU4
Measurlogic DTS305 Meter	Transducer		DTS Config		DCF
Measurlogic DTS305 Display	Display		DTS Config		DCD
Measurlogic DTS300	Transducer	B14-B40	DTS View	V7.1	DTS
Landis & Gyr ZMD	Meter	H03	MAP 120	V7.1	PRD
Landis & Gyr ZMQ	Meter		MAP120		PRD
Elster	Meter	V340-V370	Power Master Unit	V3.2	MDX/DBF
Schneider ION 8800	Meter	V003.001.000	ION Setup	V3.2	DCF
Schneider PM8000	Transducer	B14-B40	ION Setup	V2.3.2	DCF
Truteq	Modem	1.17	YatPro	1.3	N/A
Enerdis Triad 2	Transducer		Triad Just2		TRD
CTLab Vectograph	Power Quality		PQRM		REV,XML
CTLab Vecto II/III	Power Quality		OspreyLite		CSV, PQDIF, EPQDIF,DB
NMC Telecoms					
Devices	**Device type**	**Firmware Version**	**Configuration tool**	**Configuration tool version**	**Configuration file type**
Huawei Core Switch	CE8861-4C-EI	VRP8	eNSP		topo file
Huawei Distribution Switch	CE6881-48S6CQ	VRP8	eNSP		topo file
Huawei Access Switch	S5735S-S24P4X	VRP8	eNSP		topo file
Huawei Data Center Firewall	USG6630E	VRP8	eNSP		topo file
Huawei DMZ Firewall	USG6610E	VRP8	eNSP		topo file
Sophos Firewall	XGS2100				
OT Telecoms					
Devices	**Device Type**	**Firmware Version**	**Configuration tool**	**Configuration tool version**	**Configuration file type**
Siemens		1.7.0_05			

Alcatel-Lucent		01.10.10			.txt
Alcatel-Lucent		01.10.10	AWY_CT		.txt
Cisco		9.0.2 build 9453	Cisco Jabber		
Schneider Electric		R3.11.0	Tview+ Diagnostics		.cfg
Siemens		5.0.81.0	Hipath 4000 Expert Access		
Ericsson		7.1	LMT		.cfg
Ericsson		OMS 1600_LCT_3_1_6_6	Marconi LCT		
Ericsson		2.18	Mini link Craft		Java Properties File (.properties)
NEC		Rev 4.23.014	PNMT		
Schneider Electric		R3.23.1 (build 16)	Tview+ Management Suite		
Tait Communications		3.28	TB8100 Service Kit		.t8c
Motorola		15.5	STS 15.50		.scf
Cisco		5.3.2.0027	Cisco Packet Tracer		
Ilja Herlein		3.4.4	NetSetMan		
Icom		1.1	CS-F44G(MPT)		
Icom		1	CS-F44G(MPT) ADJ		
Tait Communications		1.3.0.5	TM8200/TM9300/TP9300 Programming Application		
Tait Communications		Rev 3.2	CS-F3020/F5010/F5020 Series		
ATDI		1	ATDI Content Browser		
ATDI		Ver 9.5.7	ICS Telecom		
Siemens			Comwin		

Siemens		v4	Hipath 4000 v4 we interface		
		V3	ACM		.cfg
		V2 R10	TCO		
Alcatel-Lucent			Alcatel Llc manger		
Cisco			Cisco AnyConnect		
VFR Communications ltd			Aprisa		.txt
Barnstone			Accessor		
Barnstone			Consurgo		
Barnstone			Workplace		
			USBLAN		
			PDF Creator		
Siemens			WinZip		
Areva Transducer Software			aviat		.backup
Measurlogic DTS305			DTS Config		
			Clonezilla		
Handheld radios		v6.61	Handheld Software Tool		All HHST files (.dat, .pm, .pmet, .pmon, .hipm, .cdma, .gsm, .cs, .et1, .spg, .rssi, .ss, .evdo)

Protection

Devices	Device Type	Firmware Version	Configuration tool	Configuration tool version	Configuration file type
ABB		Latest	ITT600		
ABB		2.3	PCM600		
ABB		2.5	PCM600		
ABB		7.5	HMI500		
ABB		2.1	Switch2X		
ABB		F.J	Wavewin		
ABB		4.91	WinECP Suite		
Cooper		3.01	Form 4C		

Cooper		4.0.2	Form 5		
Cooper		1.06	Form 5 TCC Editor		
Cooper		4.0.1	Form 6 Pro View		
Tavrida		4.1.2.134	Telarm		
Nulec		4.29	WSOS		
Nulec - Schneider		5.15.24	WSOS		
Eberle		3.5	Winreg		
Eberle		9.9	Winconfig		
Eberle		1.4	DNP Regparm Edit		
Eberle		2.3	GenReg		
Eberle		1.42	Reg Update		
Areva		1.4 B	DIP5000 HMI		
Areva		2.1 A	DIP5000 HMI		
Areva		2.2 D	DIP5000 HMI		
Areva		2.3 B	DIP5000 HMI		
ABB		3.2	HMI 500		
ABB		4.01	HMI 600		
ABB		1.32	HMI 570		
Areva		3.1	RPH2 Config		
Areva		3.41	Micom S1 Studio		
Areva		4.81	Micom S1		
Areva		5.11	Opticom		
Areva		1.00.0009	QDSP		
GE		5.6	Enervista UR		
GE		2.4	MIIPC		
GE		3.11	DFP 200-Link		
Hathaway		3.12	Replay		
Messko		3.9.2.6	EPT202		
Megger		4	AVTS		
Megger			MGC		

Megger		10.3.8	PowerDB10 Advanced		
Omicron		4.3	Test Universe		
Omicron		2.1	CPC		
Omicron		4.21	CT Analyzer		
Omicron		3.00.0214.0	IED Scout		
Omicron			Station Scout		
Omicron			MBX		
SEL		5.12.1.0	AcSELerator quickset		
SEL		2.0.9.2	SEL Compass		
SEL		3.38	SEL 5010 Relay Assistant		
SEL		3.2	SEL 5020		
SEL		2.2.0	SEL 5601 Analytic Assistant		
Siemens		2.1.95.01	DIGSI		
Siemens			OSCOP P		
Siemens		9.4 4.87	DIGSI		
Siemens		4	MJXplorer		
Beckwith Electric		2.01.09	TapTalk		
Strike Technologies		1	RLC		
Strike Technologies		2	RLC		
Strike Technologies		3	RLC		
Strike Technologies		1.1	FP 2000		
Grid Protection Alliance		4.2.12	PMU Connection Tester		
Vamp Technologies		1.29	Vampset		
Vamp Technologies		2.2.41	Vampset		
Vamp Technologies		2.2.84	Vampset		
Schneider		0.1.0.1	WIC 1		
SIEMENS		latest	PSD Control		
Research					

Devices	Device type	Firmware Version	Configuration tool	configuration tool version	Configuration file type
CISCO 6800 X CHASSIS STANDARD TABLES	Switch	Cisco IOS Release 15.5(1)SY	Command Line Interface		Running config; starup-config
CISCO ONENEXUS5672UP 1RU	Switch	NX-OS 7.0(5)N1(1)	Command Line Interface		Running config; starup-config
NEXUS 2000 10GT FEX	Switch	NX-OS 7.3(5)N1(1)	Cisco Prime data Network Manager or Command Line Interface		Running config; starup-config
ASR 903 SERIES ROUTER CHASIS	Agregated Services Router	Cisco IOS® XE S Software	Command Line Interface		Running config; starup-config
CISCO CGR 2010 SECURITY BUNDLE	Connected Grid Router	Cisco IOS Release 15.3 (3) M8	Command Line Interface		Running config; starup-config
829 INDUSTRIAL ISR 4G LTE MULTIMODE GLOBAL	Integrated Service Router	Cisco IOS Release 15.3 (3) M8	Command Line Interface		Running config; starup-config
CISCO CGS 2520	Connected Grid Switch	Cisco IOS Release 15.0(2) EZ	Command Line Interface		Running config; starup-config
CISCO 3945 WSPE150	Integrated Service Router	Cisco IOS Release 15.7(3) M10	Command Line Interface		Running config; starup-config
IE-4010-4S24P	Industrial Ethernet Switch	IOS XE 17.3.2	Cisco Prime Infrastructure		Running config; starup-config
ISA-3000-2C2F-K9	Indstrial Security Appliance	IOS XE 17.3.2	Cisco Prime Infrastructure		Running config; starup-config
ISR4431-V/K9	Router	IOS XE 17.3.3	Cisco Prime Infrastructure		Running config; starup-config
ISR4451-X-V/K9	Router	IOS XE 17.3.4	Cisco Prime Infrastructure		Running config; starup-config
BE7H-M4-K9	Server	BIOS 2.4.0 and CIMC 4.1(4i)	UCS Manager or UCS Central		Service profile tenplate or configuration backup file

L-ISA3000-TA	Firewall	Cisco Nexus 1000V Release 5.2(1)SV3(1.1)	Nexus 1000V Virtual Supevisor Model (VSM)		Running config; starup-config
FS-VMW-2-SW-K9	Management Center	IOS 15.9(3) M3b	CLI		Running config; starup-config
R-CISCO-2-EPNM-K9	Network Manager	EPNM v6.X Software release	GUI		Running config; starup-config
ISA-3000-4C-K9	Firewall	IOS 15.9(3) M3b	Command Line Interface		Running config; starup-config
NU11 Spirent Test Centre	Traffic Generator	STC Frimware 4.66	Spirent Test Centre Application		Project file(.tcc), configurtaion file (.scp) or testcasefile (.tst)
VNX5400 CHASSIS	Storage	OE 7.1.84.1	EMC Unisphere or CLI		Configuration File (.cfg)
FortiGate Firewall 280D-POE	Firewall	FortiIOS Version 6.4.4	FortiManager, FortiCloud, Web UI		Configuration File (.conf)
7705 SAR 8	Router	19.10.R1	CLI		.bin
7750 SR 12	Router	12.0 R4	CLI		.bin
System Operator					
Devices	**Device Type**	**Firmware Version**	**Configuration tool**	**Configuration tool version**	**Configuration file type**
P531	Disturbance Fault Recorder				.OPP
Simeas R	Disturbance Fault Recorder				.SRP
TWS	Distance to Fault Locator				