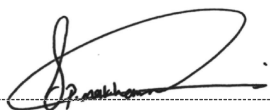


	Standard	National Transmission Company South Africa
---	-----------------	---

Title: CENTRALISED OT CONFIGURATION MANAGEMENT SYSTEM FOR NTCSA	Document Identifier: 240-185000397
	Alternative Reference Number: N/A
	Area of Applicability: National Transmission Company South Africa
	Functional Area: Engineering
	Revision: 1
	Total Pages: 60
	Next Review Date: N/A
	Disclosure Classification: Controlled Disclosure

Compiled by



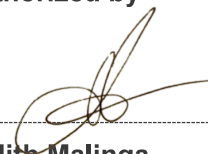
Siphelele Makhanya
PTM&C: Control & Automation Senior Engineer

Approved by



Mpumelelo Mathe
PTM&C: Control & Automation Manager

Authorized by



Judith Malinga
PTM&C: Senior Manager

Date: 19/08/2025

Date: 2025/08/25

Date: 04/09/2025

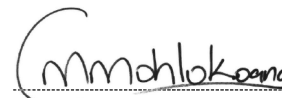
Supported by SCOT/SC



Ernest Mpshe
Systems & Tools SC Chairperson

Date: 02/09/2025

Supported by SCOT/SC



Matankiso Mohlokoana
Protection and Automation SC Chairperson

Date: 27/08/2025

Content

	Page
1. Introduction.....	4
2. Supporting Clauses	4
2.1 Scope.....	4
2.1.1 Purpose.....	4
2.1.2 Applicability	4
2.1.3 Effective date.....	5
2.2 Normative/Informative References	5
Normative	5
Informative	5
2.3 Definitions	6
General	6
Disclosure classification	6
2.4 Abbreviations.	6
2.5 Roles and Responsibilities	7
2.6 Process for Monitoring.....	7
2.7 Related/Supporting Documents.....	7
3. Requirements	7
3.1 System Requirements	7
3.1.1 Configuration Management Overview.....	8
3.1.2 Configuration Management System Overview	12
3.1.3 Scalability & Performance.....	13
3.1.4 Redundancy & Reliability.....	13
3.1.5 Interoperability.....	13
3.1.6 Access Control & User Roles	13
3.2 Functional Requirements.....	14
3.3 Operational & Maintenance Requirements	17
3.4 Compliance, Testing & Deployment Requirements.....	18
4. Acceptance.....	18
5. Revisions	18
6. Development Team	19
7. Acknowledgements	19
Appendix A : OT Device List	20
Appendix B : Schedule of Compliance	39
Appendix C : Extended OT Definition.....	59

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of National Transmission Company South Africa SOC Ltd Reg No 2021/539129/30

Figures

Figure 1: DC & Auxiliary Supplies general configuration method.....	8
Figure 2: Metering general configuration method.	8
Figure 3: Telecoms general configuration method for a new Network Element (NE).	9
Figure 4: Telecoms general configuration method for an existing Network Element (NE).....	9
Figure 5: Protection general configuration method.	10
Figure 6: System Operator (disturbance recorders) general configuration method.	10
Figure 7: Telecontrol general configuration method.	11
Figure 8: Physical Security general configuration method.	11
Figure 9: Configuration Management System Architecture Overview.	12

Tables

Table 1: Device list from all the stakeholders in PTM&C, NMC Telecoms, System Operator: Operations Performance and Research	20
Table 2: Schedule A and B of technical compliance.	39

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of National Transmission Company South Africa SOC Ltd Reg No 2021/539129/30

1. Introduction

A configuration management system is required to manage all operational configurations and tools for various systems and devices for NTCSA. Therefore, this specification document specifies the requirements needed to design, develop, and deploy a configuration management system successfully.

2. Supporting Clauses

2.1 Scope

This specification standard covers the following.

- System requirements
- Functional requirements
- Operational requirements
- Maintenance requirements
- Compliance requirements
- Testing requirements
- Deployment Requirements

The following areas are outside the scope:

- Protection settings are excluded in this configuration management

2.1.1 Purpose

This document specifies the NTCSA's requirements for the successful design, development, and deployment of a configuration management system solution based on the established user requirements. This specification ensures that the required solutions with their features and services are obtained from the market and are in alignment with the respective NTCSA Engineering Technology Roadmaps, where applicable.

2.1.2 Applicability

This specification standard shall apply to the following stakeholders.

- PTM&C
- Telecoms (OPS & NMC)
- Research, Test and Development
- System Operator: Operations Performance
- NTCSA Grids
- Physical security

CONTROLLED DISCLOSURE

2.1.3 Effective date

This specification shall take effect from the authorisation date indicated herein, subject to approval and authorisation by NTCSA stakeholders.

2.2 Normative/Informative References

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

Normative

- [1] ISO 9001 Quality Management Systems

Informative

- [2] 240-170000564: User Requirements Specification for A Configuration Management System In NTCSA.
- [3] 32-85: Information Security Policy
- [4] 240-57855742: Secure Remote Access System Standard Specification for Field IED Access
- [5] 240-77942896: Protection Equipment Configuration File Management Standard
- [6] 240-144560725: Protection Technology Roadmap for National Transmission Company South Africa (NTCSA)
- [7] 342-242: Protection Settings Management Standard
- [8] 240-170000566: Telecontrol Equipment Configuration File Management Standard
- [9] 343-Protection Settings Management Standard
- [10] 240-79034140: Telecontrol Technology Roadmap for Transmission
- [11] 240-55863502: Definition of Operational Technology (OT) and OT/IT collaboration accountabilities
- [12] 32-373: Information Security - IT/OT Remote Access Standard.
- [13] 32-377: Information Security – Firewall Standard.
- [14] 240-185000467 Standard for DC Controllers Software Configuration
- [15] 240-170000292 DC and Power Electronics Systems Setting Standard
- [16] 240-180000006 Transmission Technology Roadmap
- [17] 240-170000096 Physical Security Integration standard
- [18] DEM2412993 & 2425114 LAD PAC for Physical Security Information Management System (PSIM)
- [19] 240-79669677 Demilitarised Zone (DMZ) Designs for Operational Technology

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of National Transmission Company South Africa SOC Ltd Reg No 2021/539129/30

2.3 Definitions

General

Definition	Description
Checksum	Used to verify that the data in the file has not been tampered with or changed.
Configuration	An arrangement of parts, logics or elements in a particular form, figure or combination for a device.
Configuration file	Proprietary software version representing the configuration of a device.
Configuration Management	Its responsibility lies in capturing and preserving engineering data, encompassing functional and physical characteristics, design details, and operational information throughout the entire lifespan of NTCSA's assets.
Implemented (Current)	Refers to the configuration that has been implemented and signed off on-site.
Mission Critical	A system that is critical to the functioning of the organisation and the accomplishment of its mission
Operational Technology	Gartner defines OT as "physical-equipment-oriented technology". In essence, OT is the technology that is used to operate, monitor and control the power system. For a formal definition of OT, refer to Appendix C.
Recovery Time Objective	The maximum acceptable amount of data loss measured in time, in case of a failure or disaster in a system.
Recovery Point Objective	The targeted duration of time within which a system must be restored after an outage to avoid unacceptable consequences.
Repository	A receptacle or place where things are deposited or stored.
Shall	This means that these requirements are non-negotiable and are to be provided.
Supplier/Vendor	A business or a person that makes goods or services available to NTCSA.
The system	Refers to the configuration management system as applicable in this document

Disclosure classification

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

2.4 Abbreviations.

Abbreviation	Explanation
CG	Care Group
DRP	Disaster Recovery Plan
EADS	Engineering and Data Concentrator Solution
IED	Intelligent Electronic Device
ISO	International Organization for Standardization
LAN	Local Area Network
NE	Network Element
NMC	Network Management Centre

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of National Transmission Company South Africa SOC Ltd Reg No 2021/539129/30

Abbreviation	Explanation
NMS	Network Management System
NTCSA	National Transmission Company South Africa
PDF	Portable Document Format
PTM&C	Protection, Telecommunications, Measurements, & Control
RTO	Recovery Time Objective
RPO	Recovery Point Objective
SAI	Substation Automation Integration
SLA	Service Level Agreement
SMTP	Simple Mail Transfer Protocol
OPS	Operations and Field Services
UPS	Uninterruptible Power Supply
WAN	Wide Area Network

2.5 Roles and Responsibilities

The nominated and accepted persons shall use the requirements stipulated below in identifying a system from the market that can manage the associated configurations. Furthermore, future responsibility shall be with NTCSA OT stakeholders.

2.6 Process for Monitoring

The PTM&C Technical Committee will monitor the content and application of this document.

2.7 Related/Supporting Documents

None.

3. Requirements

All technical and non-technical requirements as part of comprehensively specifying what is needed to acquire a configuration management system that shall be used within NTCSA to manage all operational configuration files and tools have been presented below. These requirements shall all be complied with. If any of the requirements have not been satisfied or complied with, this may result in a system that will not fully serve its purpose and the business's needs and compliance.

3.1 System Requirements

The current configuration management method within NTCSA is such that each section has its own method to configure the devices relevant to that specific section. Vendor-specific or, in some cases, internally developed relevant software and tools are used to configure these devices. These methods of executing a configuration on devices as per a specific section(stakeholder) are to be maintained, thus, not to create a new method that may create confusion for the users.

CONTROLLED DISCLOSURE

3.1.1 Configuration Management Overview

The following block diagrams depict the configuration methods for each section. They help to provide context of the existing methods for configuration management within NTCSA, and possible integration points. These existing configuration management methods are to be taken into consideration for the configuration management system, with requirements as specified in the section 3.2.1.

3.1.1.1 DC & Auxiliary Supplies

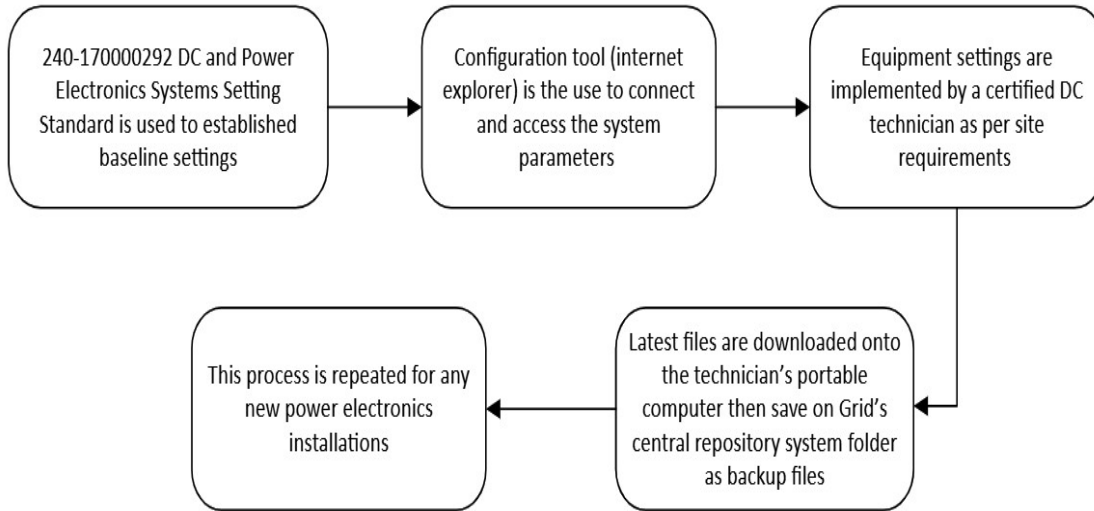


Figure 1: DC & Auxiliary Supplies general configuration method.

3.1.1.2 Metering

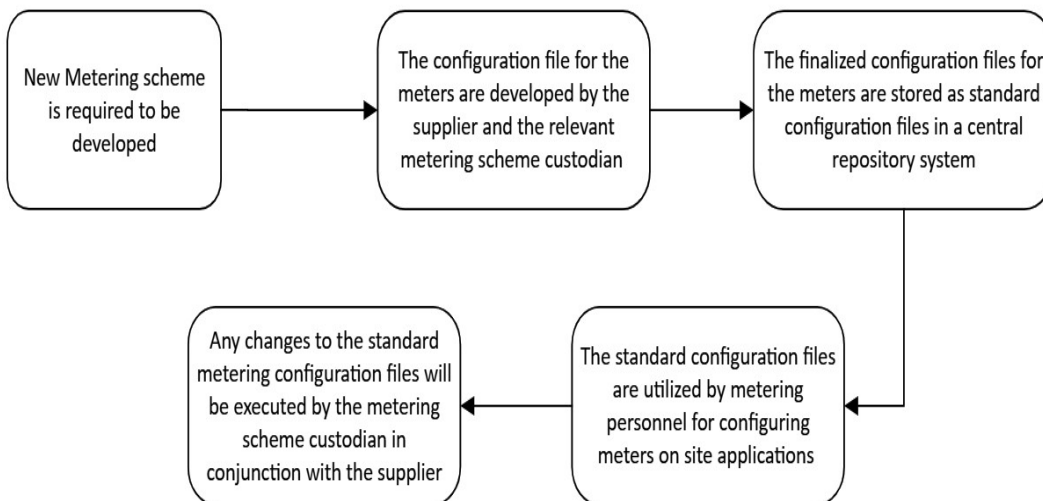


Figure 2: Metering general configuration method.

CONTROLLED DISCLOSURE

3.1.1.3 Telecoms

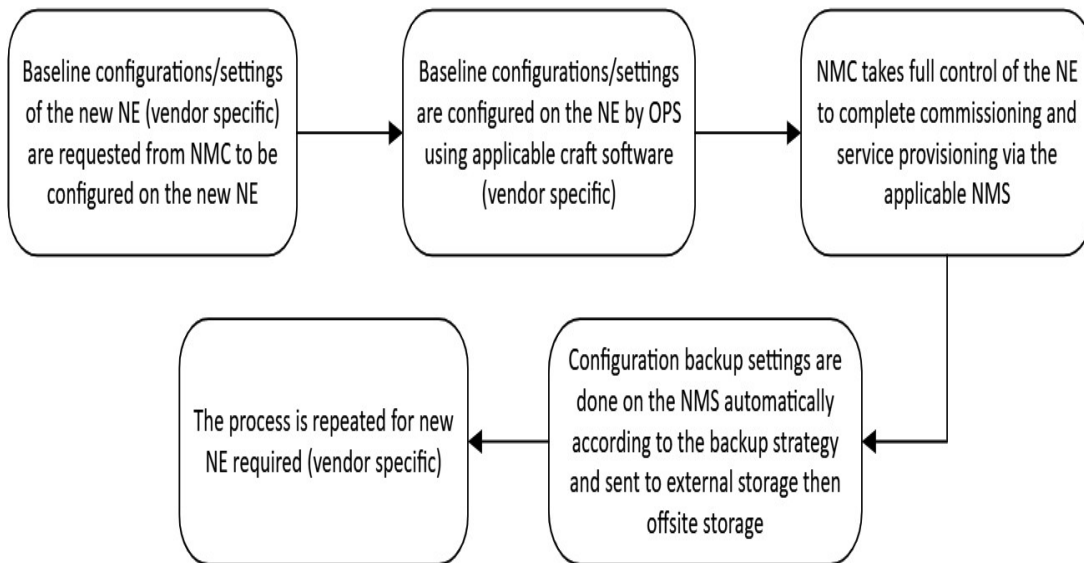


Figure 3: Telecoms general configuration method for a new Network Element (NE).

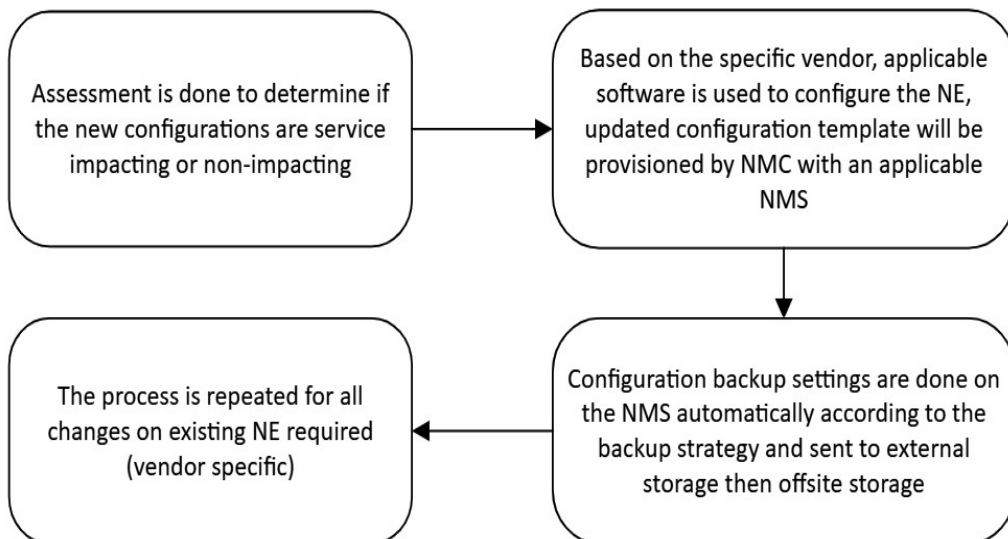


Figure 4: Telecoms general configuration method for an existing Network Element (NE).

CONTROLLED DISCLOSURE

3.1.1.4 Protection

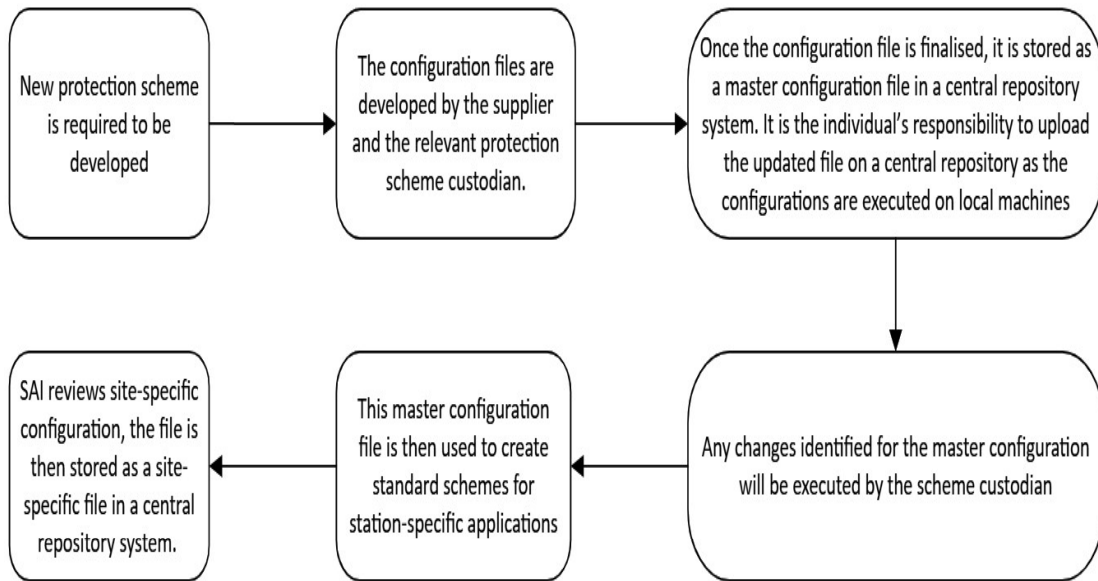


Figure 5: Protection general configuration method.

3.1.1.5 System Operator

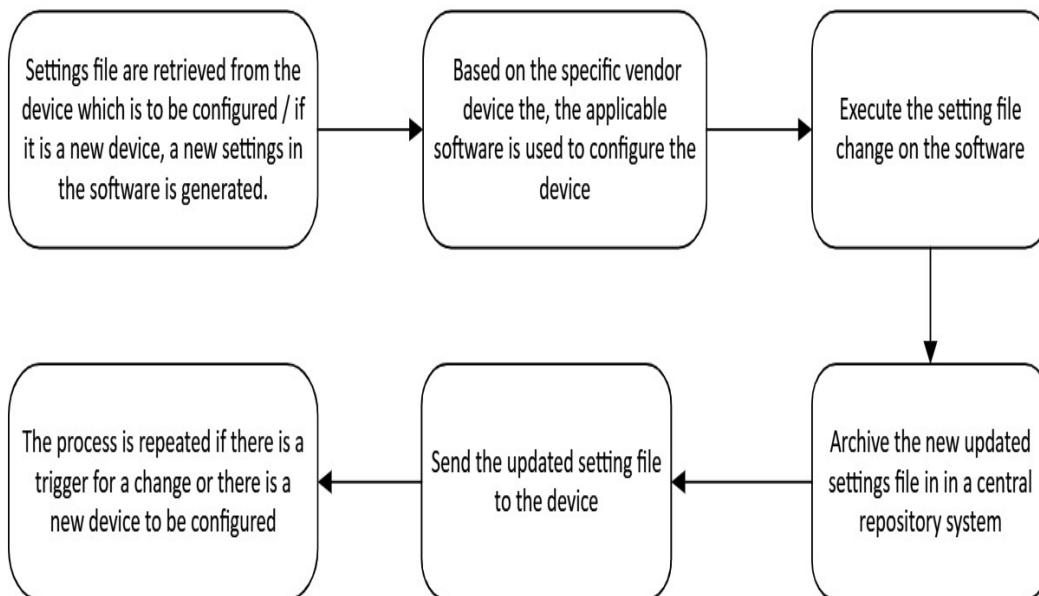


Figure 6: System Operator (disturbance recorders) general configuration method.

CONTROLLED DISCLOSURE

3.1.1.6 Telecontrol

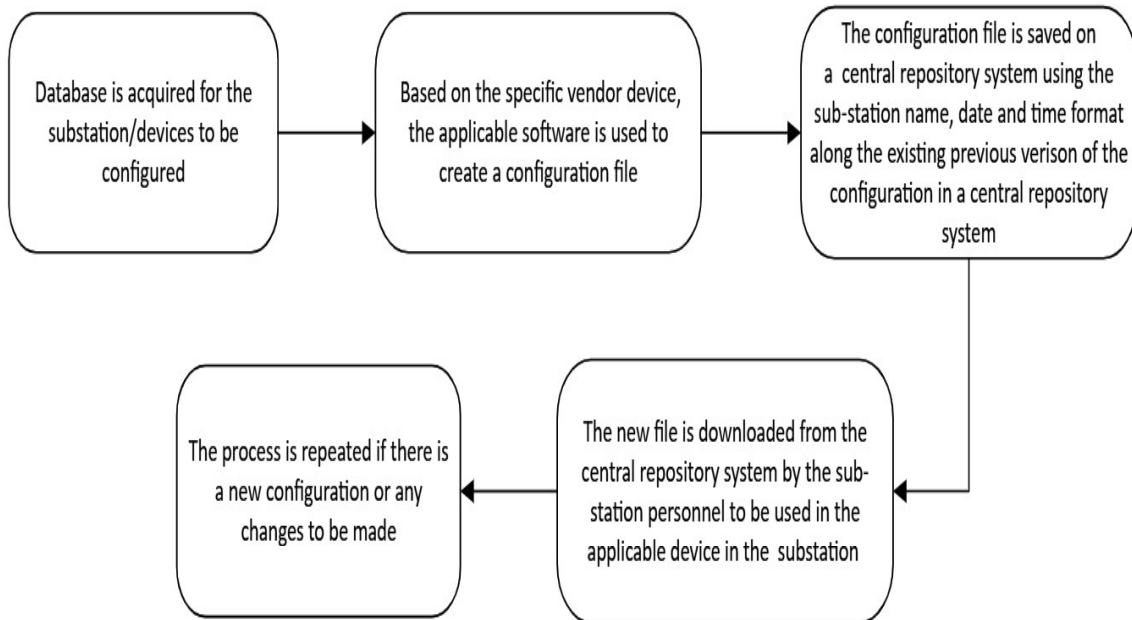


Figure 7: Telecontrol general configuration method.

3.1.1.7 Physical Security

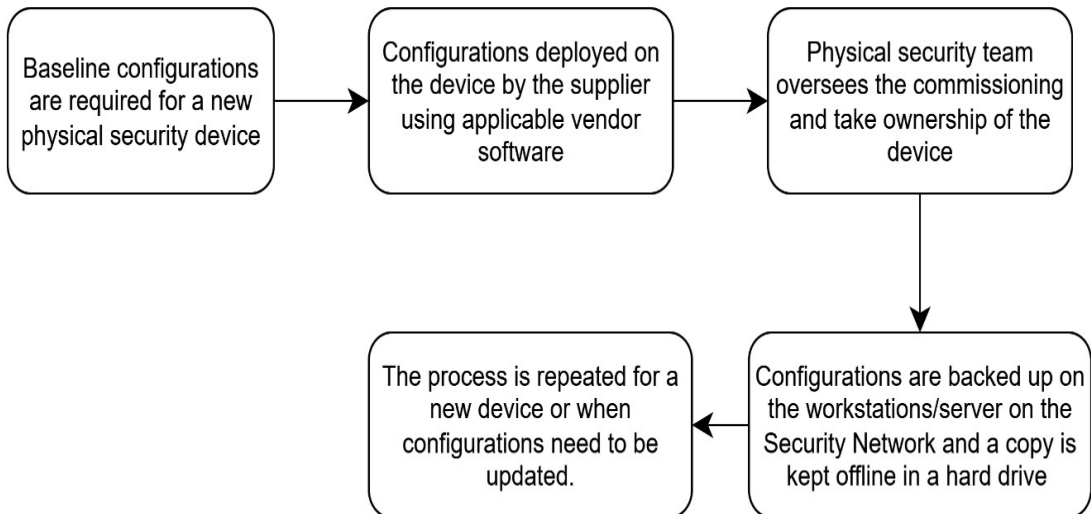


Figure 8: Physical Security general configuration method.

CONTROLLED DISCLOSURE

3.1.2 Configuration Management System Overview

Figure 9 depicts a typical Configuration Management System architecture and how it should be implemented. The Configuration Management System shall be deployed on-premises as per the NTCSA's standards. There shall be the main server running the application and database, and a local HMI for administrative purposes and system configuration purposes. Furthermore, for redundancy, there shall be a secondary server running in active hot-standby and replicating the main server in real-time. The server will be hosting virtualised servers if applicable, which will be replicated on the secondary server. There shall be a firewall as per NTCSA's standards that shall monitor and control incoming and outgoing network traffic between the Configuration Management System and the corporate LAN/WAN.

The system administrators, advanced users and normal users shall access the system through the corporate LAN/WAN. If a user is connected from a network outside of the corporate LAN/WAN, the VPN shall be used in line with NTCSA's standards. The network security and its standard are further discussed in this document.

It is to be noted that there shall be consideration of instances, such as individual deployment to cater for specific sections/user groups with unique deployment requirements for this system.

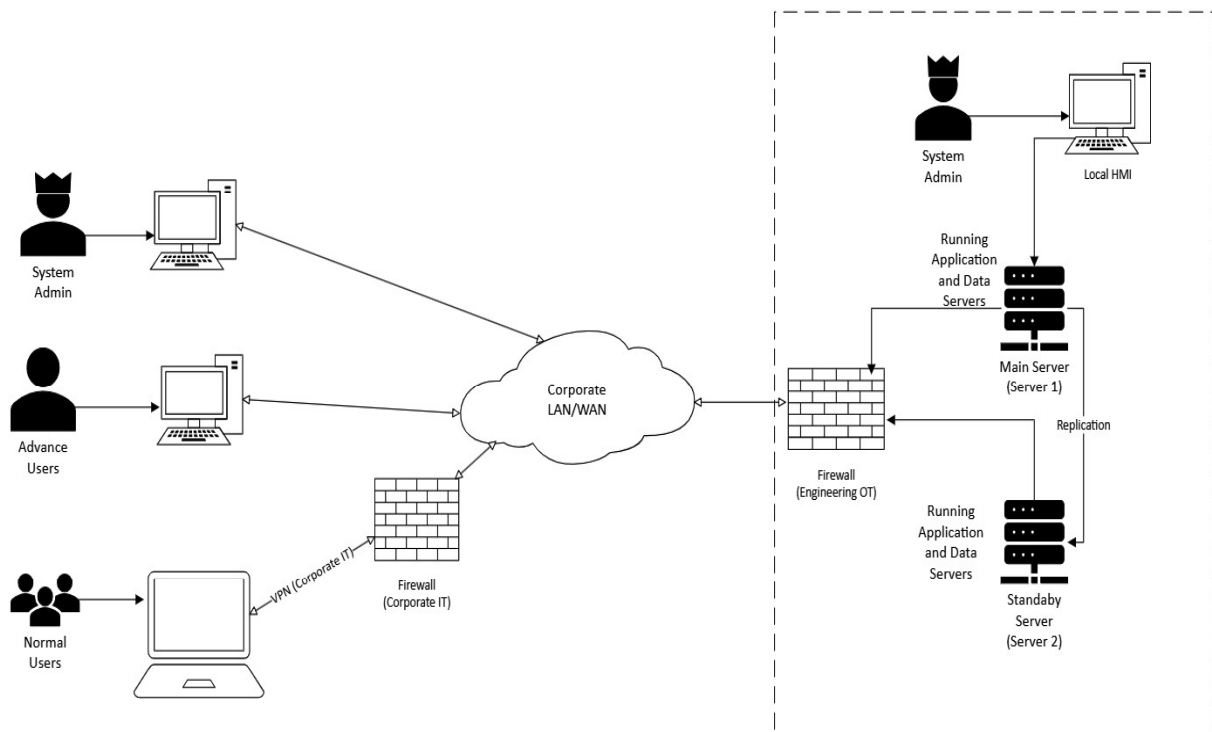


Figure 9: Configuration Management System Architecture Overview.

CONTROLLED DISCLOSURE

3.1.3 Scalability & Performance

- 3.1.3.1 The system shall be scalable, such that it can accommodate and support any device and its configuration, whether currently listed in Appendix A, or introduced in the future by NTCSA as part of their configurable devices.
- 3.1.3.2 The system shall be able to handle increasing workloads, such as an increased number of users, data and any system complexities thereof, without performance degradation.
- 3.1.3.3 The system shall support on-premises deployment.
- 3.1.3.4 The system shall have extendable storage such that the extension process does not affect or compromise the existing data on the system

3.1.4 Redundancy & Reliability

- 3.1.4.1 Considering that this system is a mission-critical system, it shall have a Recovery Time Objective (RTO), meaning acceptable system lost time of 8 – 24 hours, and zero ("0") Recovery Point Objective (RPO), meaning acceptable lost data.
- 3.1.4.2 A redundant failover system shall be in place to switch operations automatically in case of a primary system failure; this shall be in line with the on-premises deployment as specified in 3.1.3.2. The automatic failover shall be applicable for any interruption, including power or network interruptions.
- 3.1.4.3 The system shall have active hot-standby redundancy models that shall be supported for the database, application layers and shall be in line with the RPO and RTO as specified in 3.1.4.1.
- 3.1.4.4 The system shall support real-time database replication to prevent data loss in line with the chosen deployment, as in 3.1.4.2.
- 3.1.4.5 The system shall support at least dual power supplies, such as mains and a backup (e.g. UPS).

3.1.5 Interoperability

- 3.1.5.1 The system shall be able to seamlessly communicate with various devices and third-party software, regardless of manufacturer or protocol differences. This shall be in line with 3.2.1 and take into account Appendix A.
- 3.1.5.2 The system shall provide a unified interface where users can configure various devices regardless of manufacturer or protocol differences.

3.1.6 Access Control & User Roles

- 3.1.6.1 The system shall require users to login using the username and the corresponding strong password/passcode. It shall be possible to integrate with the corporate authentication system.
- 3.1.6.2 As part of added security, the system shall use multi-factor authentication for user login
- 3.1.6.3 The system shall cater for role-based access control as part of the login, where the user roles shall be in line with 3.2.19.

CONTROLLED DISCLOSURE

- 3.1.6.4 The system shall support real-time alerts as part of access control and notify administrators of unauthorised access attempts.
- 3.1.6.5 The system shall support VPN or secure tunnel-encrypted communication for remote logins and shall be in line with 3.2.28.
- 3.1.6.6 Role-based configuration management shall be used to assign specific permissions and responsibilities to users or systems based on the defined roles within the organisation. The system shall support the principle of least privilege, ensuring that each role is granted only the minimum access necessary to perform its tasks. Additionally, segmentation of roles shall be implemented by separating duties among different system users

3.2 Functional Requirements

- 3.2.1 The system shall be able to manage vendor-specific configuration file types, tools, and firmware for various devices as per Appendix A.
- 3.2.2 The system shall be able to store PDF Documents.
- 3.2.3 IED configuration files can vary in size and type, depending on the vendor-specific software used. The system shall be able to cater for this varying size and type of configuration in its native format.
- 3.2.4 The system shall be able to accommodate all various discipline naming convention standards, with at least a minimum of 64 characters.
- 3.2.5 The system shall be able to manage hardware models and firmware versions related to that specific device, which are to be populated as part of the comments field when an initial configuration is checked into the system or if there are any changes to the hardware models or firmware versions.
- 3.2.6 The system shall be able to do a comparison of the configuration on the system with the configuration being uploaded, or interface with the vendor system to do the comparison.
- 3.2.7 The system shall be able to allow the search function to cater for multiple metadata field files.
- 3.2.8 The system shall be able to add metadata fields to files.
- 3.2.9 The system shall have a search function made available to search any of the metadata fields.
- 3.2.10 The configuration management system shall be remotely accessible, preferably through the Engineering and Data Concentrator Solution (EADS) system
- 3.2.11 The system shall be fully available for 24 hours a day, 7 days a week, with a hot standby to ensure high availability, continuous operation, and seamless failover redundancy.
- 3.2.12 The system shall have a disaster recovery mechanism.
- 3.2.13 The system shall have the ability to do off-site back-ups.
- 3.2.14 The system shall be able to capture snapshots from the primary source system.
- 3.2.15 The system shall be able to have a clearly defined workflow configuration mechanism.
- 3.2.16 The system shall be flexible to accommodate device firmware and software upgrades.
- 3.2.17 The system shall be able to do the check-in and check-out of files, and as part of this requirement, it shall further satisfy the following requirements.

CONTROLLED DISCLOSURE

- 3.2.17.1 Configurations/Settings to be checked in shall 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. In a case where there are no changes to the said configuration compared to that on the system, the current version of that configuration must remain unchanged during the check-in process. The system shall check the file integrity by verifying the file checksum during the upload.
- 3.2.17.2 A configuration file shall only be checked out by a single user at a time for editing.
- 3.2.17.3 Configurations “checked-out by user” details to be captured by the system and clearly displayed, where user details shall include name, unique number, contact details and email address.
- 3.2.17.4 Where configurations are checked out, a time limit is to be specified by the Line Manager for the check-in of such configurations. Should this not be adhered to, the associated Line Manager is to be notified/flagged via email/SMTP to action the late check-in.
- 3.2.17.5 Where configurations are checked out by a specific user, the responsibility will lie with the said user to check-in that configuration that they have worked on. The system shall have the capability for the administrator to check-in the file back into the system, which overrides the user.
- 3.2.17.6 System shall ensure that configurations are setting up flags/indications to inform other users that a said file is being worked on by a specific user and shall also provide checked-out indications to other users.
- 3.2.17.7 For any configuration that is checked out by a user, only read access should be possible by other users.
- 3.2.18 The system shall be able to cater for logs and reports, and as part of this requirement, it shall further satisfy the following requirements.
 - 3.2.18.1 Logs of all interactions, including system logins, check-ins and check-outs, shall be recorded and made available on the system for system administrators. All logs shall be time-stamped.
 - 3.2.18.2 Logs of all system-related errors shall be recorded.
 - 3.2.18.3 The system shall be able to generate reports on configurations/settings based on:
 - 3.2.18.3.1 If the configuration is checked out
 - 3.2.18.3.2 Duration of check-out
 - 3.2.18.3.3 Checked out by user details
 - 3.2.18.3.4 Checked-in details, as well as an interlock that requires a pre-defined comment box (a drop-down list) to be selected before the configuration can be checked back into the system.
 - 3.2.18.4 The system shall be able to generate a report providing the following details:
 - 3.2.18.4.1 The complete user details
 - 3.2.18.4.2 Date
 - 3.2.18.4.3 Time
 - 3.2.18.4.4 The actions taken by the user.
- 3.2.19 The system shall be able to cater for access control, and as part of this requirement, it shall further satisfy the following requirements

CONTROLLED DISCLOSURE

- 3.2.19.1 Handle access control with the following roles:
 - 3.2.19.1.1 **Basic user** – with read-only access and download-only capability
 - 3.2.19.1.2 **Advanced user** – with read and write access
 - 3.2.19.1.3 **Administrator** – with the ability to add/remove user access and manage the system.
- 3.2.19.2 The system shall be configurable to categorise the roles of users based on their geographic location and discipline-specific output.
- 3.2.19.3 In an emergency, an administrator shall be able to override the checked-out configuration, necessitate the required changes, ensure that version control is maintained, check in the updated configuration and inform the user that the configuration was changed as per the emergency requirements.
- 3.2.19.4 The administrator of the system shall have the capability to manage the user's role-based access.
- 3.2.20 The system shall be able to cater for device configuration, and as part of this requirement, it shall further satisfy the following requirements.
 - 3.2.20.1 A user shall be able to define Job-Recurrence Definition tasks for devices that specify the frequency at which specific jobs are executed. Jobs that users can control include configuration retrieval. When new configuration files are retrieved, the system can send out email notifications to subscribers. There shall be 3 statuses for job retrieval,
 - 3.2.20.1.1 Complete - this means the job has been executed, and a new file has been retrieved.
 - 3.2.20.1.2 No Change - compares the configuration in the system to the one in the device.
 - 3.2.20.1.3 Failed - indicates that the system was not able to get the file for the device.
 - 3.2.20.2 The system shall have an option to get the configuration; new configuration files are retrieved and compared with old configuration files. If a change is detected, the configuration is updated in the actual configuration library. Users can use the vendor-specific application to do a comparison between files (if supported by the application), to determine what the actual difference is within the working configuration library.
 - 3.2.20.3 The system shall provide a Published Configuration Library once a working library is approved through the configuration workflow by the authorised user. The work library configuration shall be sent to the published configuration library; this allows the user to update the configuration of the device. Alternatively, the user can use the remote engineering access to connect to the system to update the device.
- 3.2.21 The system shall be able to keep a record and track all configurations deployed on site: As-built and Work-in-Progress folder creation.
- 3.2.22 The system shall be able to do version control of the configurations that are to be managed and effectively referenced and stored in the folder/location designated for such. The naming of configurations shall be identified for quick reference by users. The system shall have the ability to manage the different versions of configurations by providing a unique version number when saved back in the system.
- 3.2.23 The version history of all configurations shall be made accessible on the system.

CONTROLLED DISCLOSURE

- 3.2.24 The system shall be able to provide a log of all activities related to check-in and check-out of the configurations, as well as flagging any configurations not checked in within the pre-defined period.
- 3.2.25 In the event of a system abnormality, the latest/running configuration on site shall be the default configuration for use.
- 3.2.26 Only authorised or/and authenticated users shall be able to check out, check in, delete, and edit the configurations.
- 3.2.27 Role-based access control shall be managed: Viewing rights only, read and edit, and override any file that may be checked out by a specific user.
- 3.2.28 The system shall be accessible remotely via VPN and the required system authentication.
- 3.2.29 The system shall be able to cater for back-ups and recovery, and as part of this requirement, it shall further satisfy the following requirements
 - 3.2.29.1 The system shall provide a secured off-site backup of data in the event of system failure
 - 3.2.29.2 Daily back-ups of data shall be enabled to the off-site back-up.
 - 3.2.29.3 The period of record retention for a configuration file shall be in line with the device's life cycle.
 - 3.2.29.4 The data at rest shall be encrypted according to the best-in-practice cryptographic controls.

3.3 Operational & Maintenance Requirements

- 3.3.1 The system shall be available and accessible 24 hours a day, 7 days a week.
- 3.3.2 Users shall be able to update/revise the configuration history in the configuration, where the facility exists.
- 3.3.3 User application access to the system shall be managed in conjunction with the Line Manager of that specific user.
- 3.3.4 The system shall be able to generate logs of events such as failures, unauthorised access attempts, and abnormal system behaviours for the administrator to analyse and maintain the system as required.
- 3.3.5 The system shall generate notifications via email/SMTP to alert the administrator of any failures or abnormalities in the system as part of continued support. Only necessary and critical reporting shall be generated via email so as not to cause a nuisance.
- 3.3.6 To ensure that the users can effectively operate, maintain, and troubleshoot the system. The system vendor/provider shall provide structured training and workshops for administrators, advanced users, and basic users before the system rollout and on an "as and when" required basis. The training shall include a role-based, hands-on workshop and any other relevant and necessary training, such as cybersecurity-related training for the system.
- 3.3.7 The system vendor/provider shall provide all relevant manuals and documentation required by NTCSA as part of system delivery. This includes, but is not limited to, maintenance manuals, training manuals, etc.
- 3.3.8 There shall be contracts in place to define response times and support availability from the vendor. The system vendor/provider shall provide maintenance and support for at least a period of 5 years, including training for at least 2 years, which shall be in line with NTCSA's maintenance and support standards. The support shall include having system administrators acquainted with maintaining the system.

CONTROLLED DISCLOSURE

3.3.9 The system shall cater for software updates & patches to ensure regular updates to maintain system security and functionality.

3.4 Compliance, Testing & Deployment Requirements

- 3.4.1 The system shall comply with all relevant industry standards, acts and protocols in line with configuration management, such as ISO 10007, and the devices to be managed as per Appendix A.
- 3.4.2 The system shall be able to be tested for functionality as per the NTCSA's applicable testing processes and standards. Functions such as role-based access control, multi-protocol support and verification that configurations can be applied, modified, and rolled back without errors, etc, shall be evaluated and verified.
- 3.4.3 It shall be proven and/or demonstrated that the system is secure and not prone to cyber-attacks as per IEC/SANS 62443-3-3
- 3.4.4 As part of testing, the load and stress test simulation for large-scale substation environments shall be assessed to prove the performance of the system under high load. This shall be conducted and/or demonstrated/evidence provided.

4. Acceptance

This document has been seen and accepted by:

Name	Designation
Andre De La Guerre	Middle Manager: PTM&C Protection, Metering and DC Technologies & Support
Atha Scott	Senior Manager: Asset Investment Planning
Comfort Masike	Senior Manager: Grid Modernisation
Cornelius Naidoo	Middle Manager: PTM&C Telecommunications and Security Technologies & Support
Ernest Mpshe	Middle Manager: National Control System Support
Gert Maphutsi	Middle Manager: Central Grid Secondary Plant
Jacob Thakadu	Middle Manager: Grid Modernisation
Judith Malinga	Senior Manager: PTM&C Engineering
Matankiso Mohlokoana	Chief Engineer: PTM&C Protection
Mpumelelo Mathe	Middle Manager: PTM&C Control and Automation Technologies & Support
Neo Mapapanyane	Chief Engineer: System Operator
Pitso Sekhoto	Middle Manager: PTM&C Substation Automation Integration
Tebogo Mokwana	Senior Consultant: Asset Management - Asset Strategy
Nhlanhla Nzuza	Middle Manager: Asset Management – Maintenance Strategy

5. Revisions

Date	Rev.	Compiler	Remarks
June 2025	0.1	Siphelele Makhanya	Initial Specification.

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of National Transmission Company South Africa SOC Ltd Reg No 2021/539129/30

6. Development Team

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

- Siphelele Makhanya
- Mpumelelo Mathe:
- Ronny Lehutso
- Minenhle Mkhize

7. Acknowledgements

- Configuration Management Care Group

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of National Transmission Company South Africa SOC Ltd Reg No 2021/539129/30

Appendix A: OT Device List**Table 1: Device list from all the stakeholders in PTM&C, NMC Telecoms, System Operator: Operations Performance and Research**

1. DC & Auxiliary Supplies						
Devices	Device type	Firmware Version	Configuration tool	Configuration tool version	Configuration file type	Configuration storage system
Cordex CXC+ controller	Cordex controller (chargers)	V2.27/Bootloader V1.02/ EskomLanguage_V2.04	Internet Explorer (Google Chrome)	Latest Internet Explorer	Excel, PDF, .cfg	Individual PCs, Share Drive
Cordex CXCI Controller	Old Version – Replaced by CXCI+ Controller	Firmware V2.21/bootloader V2.05/ EskomLanguage_V2.04	Internet Explorer (Google Chrome)	Latest Internet Explorer	csvl, .cfg, PDF	Individual PCs, Share Drive
Cordex CXC M4	Old Version – Replaced by Cordex HP Controller	Firmware V2.27/Bootloader V2.05/ EskomLanguage_V2.04	Internet Explorer, Google Chrome/ VMs	Latest Internet Explorer	.csv, .cfg, PDF	Individual PCs, Share Drive
Cordex HP Controller	Cordex chargers (Chargers)	Firmware V7.1, Bootloader V6.3 Eskom Language File V13	Google Chrome	Latest Google Chrome version	Bbit, ezip, cgf, csv, cfg, backup, xml, zip	Individual PCs, Share Drive

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of National Transmission Company South Africa SOC Ltd Reg No 2021/539129/30

**CENTRALISED OT CONFIGURATION MANAGEMENT SYSTEM FOR
NTCSA**Unique Identifier: **240-185000397**Revision: **1**Page: **21 of 60**

650 W Rectifiers	Codex Rectifiers	V2.0	Win 1d	Latest win 1d version	.ACAN	Share Drive
1 kW Rectifiers	Codex Rectifiers	V2.0	Win 1d	Latest win 1d version	.ACAN	Share Drive
1.1 kW Rectifiers	Codex Rectifiers	V2.0	Win 1d	Latest win 1d version	.ACAN	Share Drive
3.3 kW Rectifiers	Codex Rectifiers	V2.0	Win 1d	Latest win 1d version	.ACAN	Share Drive
3.6 kW Rectifiers	Codex Rectifiers	V2.0	Win 1d	Latest win 1d version	.ACAN	Share Drive
4 kW Rectifiers	Codex Rectifiers	V2.0	Win 1d	Latest win 1d version	.ACAN	Share Drive
4.4 kW Rectifiers	Codex Rectifiers	V2.0	Win 1d	Latest win 1d version	.ACAN	Share Drive
Digital UPS	Uross UPS	V3.0	Ucom	Latest Ucom version	Not available	Share Drive
Digital UPS	Tower UPS	N/A	Tower	Latest tower SW version	Not available	Share Drive
Digital UPS	Statron UPS	N/A	Modulizer	Latest Modulizer version	Not available	Share Drive
Digital DC-DC Converter	Com10 DC/DC Converter	V7.0	Codex HP	N/A	N/A	Share Drive
Deepsee Diesel Generator Controller	N/A	N/A	DSE Assist	N/A	N/A	Share Drive

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of National Transmission Company South Africa SOC Ltd Reg No 2021/539129/30

**CENTRALISED OT CONFIGURATION MANAGEMENT SYSTEM FOR
NTCSA**

Unique Identifier: **240-185000397**

Revision: **1**

Page: **22 of 60**

Fuguang battery discharge testers	N/A	V1.83	Battery Test Software	N/A	N/A	Share Drive
2. Metering						
Devices	Device type	Firmware Version	Configuration tool	Configuration tool version	Configuration file type	Configuration storage system
ABB	Transducer	As per the installed base.	Contrans E-SU	Microsoft Version.	SU4	PDE Metering Webpage part 17
Measurlogic DTS305 Meter	Transducer	As per the installed base.	DTS Config	V1.42.0.248	DCF	Locally
Measurlogic DTS305 Display	Display	As per the installed base.	DTS Config	V1.42.0.248	DCD	Locally
Measurlogic DTS300	Transducer	As per the installed base.	DTS View	V1.19	DTS	Locally
Landis & Gyr ZMD	Meter	B14-B40	MAP 120	V7.1	PRD	SharePoint Directory
Landis & Gyr ZMQ	Meter	H03	MAP120	V7.1	PRD	SharePoint Directory
Elster	Meter	As per the installed base	Power Master Unit	Not available	MDX/DBF	SharePoint Directory
Schneider ION 8800	Meter	340-V370	ION Setup	V3.2	DCF	SharePoint Directory
Schneider PM8000	Transducer	V003.001.000	ION Setup	V2.3.2	DCF	SharePoint Directory

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of National Transmission Company South Africa SOC Ltd Reg No 2021/539129/30

**CENTRALISED OT CONFIGURATION MANAGEMENT SYSTEM FOR
NTCSA**

Unique Identifier: **240-185000397**

Revision: **1**

Page: **23 of 60**

Truteq	Modem	As per the installed base.	YatPro	V2.3.2.23	N/A	Manually configured as per configuration device settings.
Enerdis Triad 2	Transducer	1.17	Triad Just2	1.3	TRD	SharePoint Directory
CTLab Vectograph	Power Quality	As per the installed base.	PQRM	V5	REV, XML	To be confirmed with BIBM, and with the VM.
CTLab Vecto II/III	Power Quality	As per the installed base.	OspreyLite	V5.7.1.1831	CSV, PQDIF, EPQDIF, DB	To be confirmed with BIBM, and with the VM.

3. NMC Telecoms

Devices	Device type	Firmware Version	Configuration tool	Configuration tool version	Configuration file type	Configuration storage system
Huawei Core Switch	CE8861-4C-EI	eSight 22.0.0	Huawei eSight	eSight 22.0.0	topo file	N/A
Huawei Distribution Switch	CE6881-48S6CQ	eSight 22.0.0	Huawei eSight	eSight 22.0.0	topo file	N/A
Huawei Access Switch	S5735S-S24P4X	eSight 22.0.0	Huawei eSight	eSight 22.0.0	topo file	
Huawei Data Center Firewall	USG6630E	eSight 22.0.0	Huawei eSight	eSight 22.0.0	topo file	N/A
Huawei DMZ Firewall	USG6610E	eSight 22.0.0	Huawei eSight	eSight 22.0.0	topo file	N/A

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of National Transmission Company South Africa SOC Ltd Reg No 2021/539129/30

**CENTRALISED OT CONFIGURATION MANAGEMENT SYSTEM FOR
NTCSA**

Unique Identifier: **240-185000397**

Revision: **1**

Page: **24 of 60**

Sophos Firewall	XGS2100	eSight 22.0.0	Huawei eSight	eSight 22.0.0		N/A
Cisco	ASR903	EPNM 2.1 and NMIS 8.6.0G	EPNM and NMIS	EPNM 2.1 and NMIS 8.6.0G	.cfg	N/A
Cisco	CGR2010	EPNM 2.1 and NMIS 8.6.0G	EPNM and NMIS	EPNM 2.1 and NMIS 8.6.0G	.cfg	N/A
Cisco	IR8340	EPNM 2.1 and NMIS 8.6.0G	EPNM	EPNM 2.1 and NMIS 8.6.0G	.cfg	N/A
Cisco FW 5520	ASA	Cisco ASDM 7.6(2)150	ASDM	Cisco ASDM 7.6(2)150		N/A
Ceragon Server	N/A	N/A	N/A	N/A	N/A	N/A
DMR Server	TB9300	N/A	N/A	N/A	N/A	Under implementation
ABB FOXMAN Server	FOX615	16.2.5-0	Network Package	16.2.5-0	bck	Active Active configuration, stored on the Server
ABB FOXMAN Server	FOX512	16.2.5-0	Network Package	16.2.5-0	bck	Active Active configuration, stored on the Server
Ericsson	IPT	14B SP2 R4E	IP Transport NMS	14B SP2 R4E	cdb	On Standby Server
Ericsson	Element Manager	22.1.1	Element Manager	22.1.1	cdb	On standby Server
OT Voice	Call Manager	14.01.13900-155	Call Manager	Call Manager	cfg	N/A

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of National Transmission Company South Africa SOC Ltd Reg No 2021/539129/30

**CENTRALISED OT CONFIGURATION MANAGEMENT SYSTEM FOR
NTCSA**Unique Identifier: **240-185000397**Revision: **1**Page: **25 of 60**

OT Voice	Voice Gateway	NMIS 8.6.0G	NMIS	NMIS 8.6.0G	N/A	N/A
Trio	EB450E	N/A	N/A	N/A	N/A	Under implementation
Trio	EB450	N/A	N/A	N/A	N/A	Under implementation
Trio	QB450	N/A	N/A	N/A	N/A	Under implementation
BME	3630	N/A	5620	N/A	N/A	N/A
BME	3600		5620	N/A	N/A	N/A
Adroit	Adroit SCADA	10.0.5.4	N/A	N/A	zip	On the Server Main and Backup
Motorola	N/A	N/A	N/A	N/A	N/A	N/A
OTN	N/A	N/A	N/A	N/A	N/A	N/A

4. OT Telecoms

Devices	Device type	Firmware Version	Configuration tool	Configuration tool version	Configuration file type	Configuration storage system
Alcatel-Lucent	Alcatel 9400 AWY	01.10.10	AWY_CT	N/A	.txt	N/A
Schneider Electric	Trio QB450, Trio EB45e, Trio EB450	R3.11.0	Tview+ Diagnostics	N/A	.cfg	N/A
Siemens		5.0.81.0	Hipath 4000 Expert Access	N/A	N/A	N/A

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of National Transmission Company South Africa SOC Ltd Reg No 2021/539129/30

**CENTRALISED OT CONFIGURATION MANAGEMENT SYSTEM FOR
NTCSA**

Unique Identifier: **240-185000397**

Revision: **1**

Page: **26 of 60**

Ericsson	Ericsson LH TN	7.1	LMT	N/A	.cfg	N/A
Ericsson	Ericsson ADM OMS 1600	OMS 1600_LCT_3_1_6_6	Marconi LCT	N/A		N/A
Ericsson	Ericsson Mini link	2.18	Mini link Craft	N/A	Java Properties File (.properties)	N/A
NEC	NEC Pasolink	Rev 4.23.014	PNMT	N/A	NetworkConfig and MibConfig	N/A
Schneider Electric	Trio QB450, Trio EB45e, Trio EB450	R3.23.1 (build 16)	Tview+ Management Suite	N/A	.mdb	N/A
Tait Communications	Tait TB8100 - UHF Repeater Tait TB8100 - VHF Repeater	3.28	TB8100 Service Kit	N/A	.t8c	N/A
Motorola	ACE 3600	15.5	STS 15.50	N/A	.scf	N/A
Tait Communications	TM8200 /TM9300 /TP9300	1.3.0.5	TM8200 /TM9300 /TP9300Programmi ng Application	N/A	N/A	N/A
Siemens	Hicom 300 /3X3 /340 /342 /372382 /392	N/A	Comwin	N/A	N/A	N/A
Siemens	Siemens HI-Path 4000	V4	Hipath 4000 v4 we interface	N/A		N/A
		V3	ACM	N/A	.cfg	N/A

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of National Transmission Company South Africa SOC Ltd Reg No 2021/539129/30

**CENTRALISED OT CONFIGURATION MANAGEMENT SYSTEM FOR
NTCSA**

Unique Identifier: **240-185000397**

Revision: **1**

Page: **27 of 60**

		V2 R10	TCO	N/A		N/A
VFR Communications Ltd	Aprisa XE, Aprisa - UHF 1400MHz Link Aprisa - UHF 450MHz Link	N/A	Aprisa	N/A	.txt	N/A
Areva Transducer Software	Aviat Eclipse	N/A	aviat	N/A	.backup	N/A

5. Protection

Devices	Device type	Firmware Version	Configuration tool	Configuration tool version	Configuration file type	Configuration storage system
ABB	ABB SPACOM Relays	All	CAP 505	2.5.0	N/A	ProjectWise
ABB	ABB 500 series relays	All	CAP 540 (CAP 531 included)	1.3-00 SP05	N/A	ProjectWise
ABB	Configuration Dependant	N/A	PCM600	2.3	N/A	ProjectWise
ABB	Configuration Dependant ABB Relion Relays	N/A	PCM600	2.5	N/A	ProjectWise
ABB	ABB Relion Relays	N/A	PCM600	2.7	N/A	ProjectWise
ABB	ABB Relion Relays	N/A	PCM600	2.9	N/A	ProjectWise

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of National Transmission Company South Africa SOC Ltd Reg No 2021/539129/30

**CENTRALISED OT CONFIGURATION MANAGEMENT SYSTEM FOR
NTCSA**

Unique Identifier: **240-185000397**

Revision: **1**

Page: **28 of 60**

ABB	ABB Relion Relays	N/A	PCM600	2.11	N/A	ProjectWise
ABB	Certain ABB Tele-protections Devices	N/A	HMI 500	3.2	N/A	N/A
ABB	Certain ABB Tele-protections Devices	N/A	HMI500	7.5	N/A	N/A
ABB	Certain ABB Tele-protections Devices		HMI 600	4.01		
ABB	N/A	N/A	HMI 570	1.32	N/A	N/A
ABB	N/A	N/A	Switch2X	2.1	N/A	N/A
ABB	ABB DPU2000R Relay	N/A	WinECP	4.91	N/A	N/A
Tavrida		N/A	Telarm	4.1.2.134	N/A	N/A
Eberle	REG-D Voltage Regulating Relays	N/A	WinReg	4.2.11	N/A	ProjectWise
Eberle	REG-D Voltage Regulating Relays	N/A	Winconfig	13.46	N/A	ProjectWise
Areva	DIP5000 Tele-protection Devices	N/A	DIP5000 HMI	1.4 B	N/A	N/A
Areva	DIP5000 Tele-protection Devices	N/A	DIP5000 HMI	2.1 A	N/A	N/A

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of National Transmission Company South Africa SOC Ltd Reg No 2021/539129/30

**CENTRALISED OT CONFIGURATION MANAGEMENT SYSTEM FOR
NTCSA**

Unique Identifier: **240-185000397**

Revision: **1**

Page: **29 of 60**

Areva	DIP5000 Tele-protection Devices	N/A	DIP5000 HMI	2.2 D	N/A	N/A
Areva	DIP5000 Tele-protection Devices		DIP5000 HMI	2.3 B		
Areva	RPH2 Point on Wave Switching Devices	N/A	RPH2 Config	3.1	N/A	N/A
Areva	Legacy MiCOM IEDs		Micom S1 Studio	4.0.1	N/A	N/A
Areva	MiCom IEDs	4.81	Easergy Studio	9.3.6	N/A	N/A
ACTOM	MiCOM P847 PMU	N/A	MiCOM S1 Agile	2.1.3	N/A	N/A
Areva		N/A	Opticom	5.11	N/A	N/A
Areva		N/A	QDSP	1.00.0009	N/A	N/A
GE		N/A	DFP 200-Link	3.11	N/A	N/A
Hathaway		N/A	Replay	3.12	N/A	N/A
Messko	Transformer Digital Temperature Instrument	N/A	EPT202	3.9.2.6	N/A	N/A
Megger	Megger Test Sets	N/A	AVTS	4	N/A	ProjectWise
Megger	Megger Goose Configurator	N/A	MGC	10.3.8	N/A	

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of National Transmission Company South Africa SOC Ltd Reg No 2021/539129/30

**CENTRALISED OT CONFIGURATION MANAGEMENT SYSTEM FOR
NTCSA**

Unique Identifier: **240-185000397**

Revision: **1**

Page: **30 of 60**

Megger	Megger Devices - Test Data Management Software		PowerDB10 Advanced	10.3.8		
Omicron	Omicron Test Sets	N/A	Test Universe	4.3	N/A	N/A
Omicron	Omicron CPC Test Sets	N/A	CPC	2.1	N/A	N/A
Omicron	Omicron CT Analyser Test Set	N/A	CT Analyzer	4.21	N/A	N/A
Omicron	Omicron Test Sets	N/A	IED Scout	3.00.0214.0	N/A	N/A
Omicron	Omicron Test Sets	N/A	Station Scout		N/A	N/A
Omicron		N/A	MBX		N/A	N/A
SEL	Modern SEL IED's	N/A	AcSELeRator quickset	5.12.1.0	N/A	ProjectWise
SEL287V	Legacy SEL IEDs	N/A	SEL-5010 Relay Assistant	3.3.8	N/A	Not available
SEL	Certain SEL IED's	N/A	SEL Compass	2.0.9.2	N/A	ProjectWise
SEL	Certain SEL IED's	N/A	SEL 5020	3.2	N/A	ProjectWise
SEL	Certain SEL IED's		SEL 5601 Analytic Assistant	2.2.0		ProjectWise
Siemens	SIPROTEC 2	N/A	DIGSI	2.1.95.01	N/A	N/A

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of National Transmission Company South Africa SOC Ltd Reg No 2021/539129/30

**CENTRALISED OT CONFIGURATION MANAGEMENT SYSTEM FOR
NTCSA**

Unique Identifier: **240-185000397**

Revision: **1**

Page: **31 of 60**

Siemens	SIPROTEC 3 or 4	N/A	DIGSI	4.94	N/A	N/A
Siemens	SIPROTEC 5	N/A	DIGSI 5	9.40	N/A	N/A
Siemens		N/A	MJXplorer	4	N/A	N/A
Beckwith Electric		N/A	TapTalk	2.01.09	N/A	N/A
Strike Technologies		N/A	FP 2000	1.1	N/A	N/A
SIEMENS		N/A	PSD Control	Latest	N/A	N/A
Strike Technologies RLC04B	Multifunction Capacitor and Filter Bank Protection Relay	N/A	RLC04 Communication Program	N/A	N/A	Not available
General Electric Multilin C70	Multifunction Capacitor and Filter Bank Protection Relay	5.61 5.90 8.42 8.50	GE Enervista UR Setup	8.42 8.51	.urs	ProjectWise
General Electric Multilin MIB	High Impedance Restricted Earth Fault Protection Relay	3.00	GE Enervista MII Setup	2.70	.ajs	ProjectWise
6. Research						
Devices	Device type	Firmware Version	Configuration tool	Configuration tool version	Configuration file type	Configuration storage system

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of National Transmission Company South Africa SOC Ltd Reg No 2021/539129/30

**CENTRALISED OT CONFIGURATION MANAGEMENT SYSTEM FOR
NTCSA**Unique Identifier: **240-185000397**Revision: **1**Page: **32 of 60**

CISCO 6800 X CHASSIS STANDARD TABLES	Switch	Cisco IOS Release 15.5(1) SY	Command Line Interface	N/A	Running config; startup-config	NVRAM or External Devices such USB Flash drive
CISCO ONENEXUS5672U P 1RU	Switch	NX-OS 7.0(5)N1(1)	Command Line Interface	N/A	Running config; startup-config	NVRAM or External Devices such USB Flash drive
NEXUS 2000 10GT FEX	Switch	NX-OS 7.3(5)N1(1)	Cisco Prime data Network Manager or Command Line Interface	N/A	Running config; startup-config	NVRAM or External Devices such USB Flash drive
ASR 903 SERIES ROUTER CHASIS	Aggregated Services Router	Cisco IOS® XE S Software	Command Line Interface	N/A	Running config; startup-config	NVRAM or External Devices such USB Flash drive
CISCO CGR 2010 SECURITY BUNDLE	Connected Grid Router	Cisco IOS Release 15.3 (3) M8	Command Line Interface	N/A	Running config; startup-config	NVRAM or External Devices such USB Flash drive
829 INDUSTRIAL ISR 4G LTE MULTIMODE GLOBAL	Integrated Service Router	Cisco IOS Release 15.3 (3) M8	Command Line Interface		Running config; startup-config	NVRAM or External Devices such USB Flash drive
CISCO CGS 2520	Connected Grid Switch	Cisco IOS Release 15.0(2) EZ	Command Line Interface	N/A	Running config; startup-config	NVRAM or External Devices such USB Flash drive
CISCO 3945 WSPE150	Integrated Service Router	Cisco IOS Release 15.7(3) M10	Command Line Interface	N/A	Running config; startup-config	NVRAM or External Devices such USB Flash drive

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of National Transmission Company South Africa SOC Ltd Reg No 2021/539129/30

**CENTRALISED OT CONFIGURATION MANAGEMENT SYSTEM FOR
NTCSA**Unique Identifier: **240-185000397**Revision: **1**Page: **33 of 60**

IE-4010-4S24P	Industrial Ethernet Switch	IOS XE 17.3.2	Cisco Prime Infrastructure	N/A	Running config; startup-config	NVRAM or External Devices such USB Flash drive
ISA-3000-2C2F-K9	Industrial Security Appliance	IOS XE 17.3.2	Cisco Prime Infrastructure	N/A	Running config; startup-config	NVRAM or External Devices such USB Flash drive
ISR4431-V/K9	Router	IOS XE 17.3.3	Cisco Prime Infrastructure	N/A	Running config; startup-config	NVRAM or External Devices such USB Flash drive
ISR4451-X-V/K9	Router	IOS XE 17.3.4	Cisco Prime Infrastructure	N/A	Running config; startup-config	NVRAM or External Devices such USB Flash drive
BE7H-M4-K9	Server	BIOS 2.4.0 and CIMC 4.1(4i)	UCS Manager or UCS Central	N/A	Service profile template or configuration backup file	UCS Manager or NAS storage
L-ISA3000-TA	Firewall	Cisco Nexus 1000V Release 5.2(1)SV3(1.1)	Nexus 1000V Virtual Supervisor Model (VSM)	N/A	Running config; startup-config	VSM or External Devices such USB Flash drive
FS-VMW-2-SW-K9	Management Center	IOS 15.9(3) M3b	CLI	N/A	Running config; startup-config	NVRAM or External Devices such USB Flash drive
R-CISCO-2-EPNM-K9	Network Manager	EPNM v6.X Software release	GUI	N/A	Running config; startup-config	NVRAM or External Devices such USB Flash drive
ISA-3000-4C-K9	Firewall	IOS 15.9(3) M3b	Command Line Interface	N/A	Running config; startup-config	NVRAM or External Devices such USB Flash drive

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of National Transmission Company South Africa SOC Ltd Reg No 2021/539129/30

**CENTRALISED OT CONFIGURATION MANAGEMENT SYSTEM FOR
NTCSA**

Unique Identifier: **240-185000397**

Revision: **1**

Page: **34 of 60**

NU11 Spirent Test Centre	Traffic Generator	STC Firmware 4.66	Spirent Test Centre Application	N/A	Project file(.tcc), configuration file (.scp) or testcasefile (.tst)	Application server or external device
VNX5400 CHASSIS	Storage	OE 7.1.84.1	EMC Unisphere or CLI	N/A	Configuration File (.cfg)	System, or external device
FortiGate Firewall 280D-POE	Firewall	FortiOS Version 6.4.4	FortiManager, FortiCloud, Web UI	N/A	Configuration File (.conf)	System, flash drive or external system
7705 SAR 8	Router	19.10.R1	CLI	N/A	.bin	SR OS file System
7750 SR 12	Router	12.0 R4	CLI	N/A	.bin	SR OS file System

7. System Operator

Devices	Device type	Firmware Version	Configuration tool	Configuration tool version	Configuration file type	Configuration storage system
Siemens P531	Disturbance/Digital Fault Recorder	N/A	OSCO P	6.50.19	.OPP	Hyperwave/OpenText
Siemens Simeas-R	Disturbance/Digital Fault Recorder	N/A	OSCO P	6.50.19	.SRP	Hyperwave/OpenText
Qualitrol TWS MK5/MK6	Distance to Fault Locator	N/A	iQ+	4.19.0008.2301	.cfg	N/A
Qualitrol TWS FL8	Distance to Fault Locator	N/A	iQ+	4.19.0008.2301	.cfg	N/A
Qualitrol IDM+	Disturbance/Digital Fault Recorder	4.19_30	iQ+	4.19.0008.2301	.cfg	Hyperwave/OpenText

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of National Transmission Company South Africa SOC Ltd Reg No 2021/539129/30

**CENTRALISED OT CONFIGURATION MANAGEMENT SYSTEM FOR
NTCSA**

Unique Identifier: **240-185000397**

Revision: **1**

Page: **35 of 60**

	& Distance to Fault Locator					
8. Telecontrol						
Devices	Device type	Firmware Version	Configuration tool	Configuratio n tool version	Configuratio n file type	Configuration storage system
D400 - IEC61850/IHMI	Gateway	2.75	IEC 61850 Loader & SG Config HMI Viewer	2.1.4.9344	.zip	ProjectWise
D400 - IEC61850/IHMI	Gateway	5.5	D400 Run Time HMI & DS Agile Studio	5.5 & 2.5 Respectively	.iso	ProjectWise
D400 – ESTEL/IHMI	Gateway	2.75	SG Config HMI Viewer	N/A	.zip	ProjectWise
D400 – ESTEL/IHMI	Gateway	5.5	D400 Run Time HMI	5.5	.zip	ProjectWise
D20 - ESTEL & IEC61850	Station RTU	ISTE000125-164	Config Pro	6	.zip	ProjectWise
D25 - ESTEL & IEC61850	Bay Processor	ISTE000086-164 & ISTE000124	Config Pro	6	.zip	ProjectWise
Talus BP	Bay Processor	501B	Unicon	1.7.24	.fac	ProjectWise
Talus Station RTU	Station RTU	501B	Unicon	1.7.24	.fac	ProjectWise
Talus ERTU	Gateway	501B	Unicon	1.7.24	.fac	ProjectWise
Tekron TCG01-E	GPS	F2.20.2.038	Tekron Clock Configuration Tool	4.1.0.24	.tcg	ProjectWise

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of National Transmission Company South Africa SOC Ltd Reg No 2021/539129/30

**CENTRALISED OT CONFIGURATION MANAGEMENT SYSTEM FOR
NTCSA**

Unique Identifier: **240-185000397**

Revision: **1**

Page: **36 of 60**

Tekron TCG01-G	GPS	F2.21.3.11r2.c1.06.1.0 4b	Tekron Clock Configuration Tool	4.2.1.0	.tcg	ProjectWise
Symmetricom XL750	GPS		xl - 750	2.023	.tcg	ProjectWise
RSG2100, RSG2200, RSG416, RS900 and RSG 2488	Network Switches	4.3.5	Terminal emulator/ Browser	N/A	.csv	ProjectWise
RX1100 and RX1500	Network router	1.16, ROX2.13	Terminal emulator/ Browser	N/A	.cli	ProjectWise
Advantech Siemens	Gateway	8.19	Sicam PAS	8.19	.zip	ProjectWise
RTU 560 - CMU 04	Station RTU	N/A	RTUtil	7.1.1.0 & 7.6.1.0	.gcd/ .iod/ .ptx/.rtu	ProjectWise
RTU 560 - CMU 05	Station RTU	N/A	RTUtil	9.9.2.0	.gcd/ .iod/ .ptx/ .rtu	ProjectWise
RTU560 SLI	Station RTU	N/A	RTUtil	6.3.230.1	.gcd/ .iod/ .ptx/.rtu	ProjectWise
Siemens AdvantechECU- 4784PC	Siemens HMI	WINCC 7.5, SCC 9.08	Sicam PAS	7.1.1.0 & 7.6.1.0	N/A	ProjectWise
P and C SEL (info to be confirmed)	Gateway	N/A	N/A	N/A	N/A	N/A
EADS Subnet	Data Concentrator and Substation Server	N/A	N/A	N/A	N/A	N/A

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of National Transmission Company South Africa SOC Ltd Reg No 2021/539129/30

**CENTRALISED OT CONFIGURATION MANAGEMENT SYSTEM FOR
NTCSA**

Unique Identifier: **240-185000397**

Revision: **1**

Page: **37 of 60**

G500 (info to be confirmed)	TBC	N/A	N/A	N/A	N/A	N/A
9. Physical Security						
Devices	Device type	Firmware Version	Configuration tool	Configuration tool version	Configuration file type	Configuration storage system
Ipixa/Huawei	Switches	N/A	Web Browser	N/A	.cfg	Web Browser
Dell PowerEdge R350	Servers	1.1.303	Windows Server 2022	N/A	N/A	Windows Backup/Restore
UNV 516-128	NVR	N/A	EZ Tools	Ver: 2.0	.xml	Web Browser
Dell XPS 8950	Workstation	1.2.0	Windows 11 Pro	N/A	N/A	Windows Backup/Restore
UNV IPC3234SA-DZK IR Dome	Camera	N/A	EZ Tools	Ver: 2.0	.xml	Web Browser
UNV IPC264EA-HDZK IR Bullet	Camera	N/A	EZ Tools	Ver: 2.0	.xml	Web Browser
UNV TIC2621SR-F3-4F4AC-VD Thermal Bullet	Camera	N/A	EZ Tools	Ver: 2.0	.xml	Web Browser
UNV IPC6852ER-X45-VF PTZ Camera	Camera	N/A	EZ Tools	Ver: 2.0	.xml	Web Browser
TOA A1SC15 E00 POE	Horn Speaker	3.30	Web Browser	N/A	.spconf	Web Browser
Acuvox C313	Intercom Master	213.30.11.202	Web Browser	N/A	.cfg	Web Browser

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of National Transmission Company South Africa SOC Ltd Reg No 2021/539129/30

**CENTRALISED OT CONFIGURATION MANAGEMENT SYSTEM FOR
NTCSA**

Unique Identifier: **240-185000397**

Revision: **1**

Page: **38 of 60**

Acuvox R20A	Intercom Slave	320.87.10.103	Web Browser	N/A	.cfg	Web Browser
Paxton Net2 Plus	Access Controller	N/A	Net2 Configurator	Ver: 6.5	.ndb	Net2 Pro Paxton Software
WI-I Detection Module	PIDS	N/A	Web Browser	N/A	.cfg	Web Browser
TBS	Bio Readers	N/A	Web Browser	N/A	.cfg	Web Browser
Satel Integra 64	Alarm Panel	1.22	DLoadX	1.24	.prg	DLoadX
Cambium Cnpilot E510	PIDS Bridge Access Points	N/A	Web Browser	N/A	.conf	Web Browser
Fortinet FG-40F Series	Firewall	7.4.7	Web browser	7.4.7	.conf	Web Browser

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of National Transmission Company South Africa SOC Ltd Reg No 2021/539129/30

Appendix B: Schedule of Compliance

Table 2: Schedule A and B of technical compliance.

Specification clause number	Description	Schedule A: NTCSA's minimum technical requirements	Schedule B: Supplier's statements of compliance	Supplier's Reference/Comment (Supporting Evidence)
3	Requirements			
3.1	System Requirements			
3.1.3	Scalability & Performance			
3.1.3.1	The system shall be scalable, such that it can accommodate and support any device and its configuration, whether currently listed in Appendix A, or introduced in the future by NTCSA as part of their configurable devices.			
3.1.3.2	The system shall be able to handle increasing workloads, such as an increased number of users, data and any system complexities thereof, without performance degradation			

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of National Transmission Company South Africa SOC Ltd Reg No 2021/539129/30

**CENTRALISED OT CONFIGURATION MANAGEMENT SYSTEM FOR
NTCSA**

Unique Identifier: **240-185000397**

Revision: **1**

Page: **40 of 60**

3.1.3.3	The system shall support on-premises deployment			
3.1.3.4	The system shall have extendable storage such that the extension process does not affect or compromise the existing data on the system			
3.1.4	Redundancy & Reliability			
3.1.4.1	Considering that this system is a mission-critical system, it shall have a Recovery Time Objective (RTO), meaning acceptable system lost time of 8 – 24 hours, and zero ("0") Recovery Point Objective (RPO), meaning acceptable lost data.			
3.1.4.2	A redundant failover system shall be in place to switch operations automatically in case of a primary system failure; this shall be in line with the on-premises deployment as specified in 3.1.3.2. The automatic failover shall be applicable for any interruption, including power or network interruptions			

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of National Transmission Company South Africa SOC Ltd Reg No 2021/539129/30

**CENTRALISED OT CONFIGURATION MANAGEMENT SYSTEM FOR
NTCSA**

Unique Identifier: **240-185000397**

Revision: **1**

Page: **41 of 60**

3.1.4.3	The system shall have active hot-standby redundancy models that shall be supported for the database, application layers and shall be in line with the RPO and RTO as specified in 3.1.4.1.			
3.1.4.4	The system shall support real-time database replication to prevent data loss in line with the chosen deployment, as in 3.1.4.2.			
3.1.4.5	The system shall support at least dual power supplies, such as mains and a backup (e.g. UPS)			
3.1.5	Interoperability			
3.1.5.1	The system shall be able to seamlessly communicate with various devices and third-party software, regardless of manufacturer or protocol differences. This shall be in line with 3.2.1 and take into account Appendix A.			
3.1.5.2	The system shall provide a unified interface where users can configure various devices regardless of manufacturer or protocol differences.			

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of National Transmission Company South Africa SOC Ltd Reg No 2021/539129/30

**CENTRALISED OT CONFIGURATION MANAGEMENT SYSTEM FOR
NTCSA**

Unique Identifier: **240-185000397**

Revision: **1**

Page: **42 of 60**

3.1.6	Access Control & User Roles			
3.1.6.1	The system shall require users to login using the username and the corresponding strong password/passcode. It shall be possible to integrate with the corporate authentication system.			
3.1.6.2	As part of added security, the system shall use multi-factor authentication for user login			
3.1.6.3	The system shall cater for role-based access control as part of the login, where the user roles shall be in line with 3.2.19.			
3.1.6.4	The system shall support real-time alerts as part of access control and notify administrators of unauthorised access attempts			
3.1.6.5	The system shall support VPN or secure tunnel-encrypted communication for remote logins and shall be in line with 3.2.28			

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of National Transmission Company South Africa SOC Ltd Reg No 2021/539129/30

**CENTRALISED OT CONFIGURATION MANAGEMENT SYSTEM FOR
NTCSA**

Unique Identifier: **240-185000397**

Revision: **1**

Page: **43 of 60**

3.1.6.6	Role-based configuration management shall be used to assign specific permissions and responsibilities to users or systems based on the defined roles within the organisation. The system shall support the principle of least privilege, ensuring that each role is granted only the minimum access necessary to perform its tasks. Additionally, segmentation of roles shall be implemented by separating duties among different system users			
3.2	Functional Requirements			
3.2.1	The system shall be able to manage vendor-specific configuration file types, tools, and firmware for various devices as per Appendix A.			
3.2.2	The system shall be able to store PDF Documents			
3.2.3	IED configuration files can vary in size and type, depending on the vendor-specific software used. The system shall be able to cater for this varying size and type of configuration in its native format.			

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of National Transmission Company South Africa SOC Ltd Reg No 2021/539129/30

**CENTRALISED OT CONFIGURATION MANAGEMENT SYSTEM FOR
NTCSA**

Unique Identifier: **240-185000397**

Revision: **1**

Page: **44 of 60**

3.2.4	The system shall be able to accommodate all various discipline naming convention standards			
3.2.5	The system shall be able to manage hardware models and firmware versions related to that specific device, which are to be populated as part of the comments field when an initial configuration is checked into the system or if there are any changes to the hardware models or firmware versions.			
3.2.6	The system shall be able to do a comparison of the configuration on the system with the configuration being uploaded			
3.2.7	The system shall be able to allow the search function to cater for multiple metadata field files.			
3.2.8	The system shall be able to add metadata fields to files			
3.2.9	The system shall have a search function made available to search any of the metadata fields			

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of National Transmission Company South Africa SOC Ltd Reg No 2021/539129/30

**CENTRALISED OT CONFIGURATION MANAGEMENT SYSTEM FOR
NTCSA**

Unique Identifier: **240-185000397**

Revision: **1**

Page: **45 of 60**

3.2.10	The configuration management system shall be remotely accessible, preferably through the Engineering and Data Concentrator Solution (EADS) system			
3.2.11	The system shall be fully available for 24 hours a day, 7 days a week, with a hot standby to ensure high availability, continuous operation, and seamless failover redundancy			
3.2.12	The system shall have a disaster recovery mechanism			
3.2.13	The system shall have the ability to do off-site back-ups.			
3.2.14	The system shall be able to capture snapshots from the primary source system.			
3.2.15	The system shall be able to have a clearly defined workflow configuration mechanism			
3.2.16	The system shall be flexible to accommodate device firmware and software upgrades			

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of National Transmission Company South Africa SOC Ltd Reg No 2021/539129/30

**CENTRALISED OT CONFIGURATION MANAGEMENT SYSTEM FOR
NTCSA**

Unique Identifier: **240-185000397**

Revision: **1**

Page: **46 of 60**

3.2.17	The system shall be able to do the check-in and check-out of files, and as part of this requirement, it shall further satisfy the following requirements			
3.2.17.1	Configurations/Settings to be checked in shall 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. In a case where there are no changes to the said configuration compared to that on the system, the current version of that configuration must remain unchanged during the check-in process. The system shall check the file integrity by verifying the file checksum during the upload.			
3.2.17.2	A configuration file shall only be checked out by a single user at a time for editing.			
3.2.17.3	Configurations "checked-out by user" details to be captured by the system and clearly displayed, where user details shall include name, unique number, contact details and email address.			

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of National Transmission Company South Africa SOC Ltd Reg No 2021/539129/30

**CENTRALISED OT CONFIGURATION MANAGEMENT SYSTEM FOR
NTCSA**

Unique Identifier: **240-185000397**

Revision: **1**

Page: **47 of 60**

3.2.17.4	Where configurations are checked out, a time limit is to be specified by the Line Manager for the check-in of such configurations. Should this not be adhered to, the associated Line Manager is to be notified/flagged via email/SMTP to action the late check-in.			
3.2.17.5	Where configurations are checked out by a specific user, the responsibility will lie with the said user to check-in that configuration that they have worked on. The system shall have the capability for the administrator to check-in the file back into the system, which overrides the user			
3.2.17.6	System shall ensure that configurations are setting up flags/indications to inform other users that a said file is being worked on by a specific user and shall also provide checked-out indications to other users.			
3.2.17.7	For any configuration that is checked out by a user, only read access should be possible by other users.			

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of National Transmission Company South Africa SOC Ltd Reg No 2021/539129/30

**CENTRALISED OT CONFIGURATION MANAGEMENT SYSTEM FOR
NTCSA**

Unique Identifier: **240-185000397**

Revision: **1**

Page: **48 of 60**

3.2.18	The system shall be able to cater for logs and reports, and as part of this requirement, it shall further satisfy the following requirements.			
3.2.18.1	Logs of all interactions, including system logins, check-ins and check-outs, shall be recorded and made available on the system for system administrators. All logs shall be time-stamped.			
3.2.18.2	Logs of all system-related errors shall be recorded.			
3.2.18.3	The system shall be able to generate reports on configurations/settings based on:			
3.2.18.3.1	If the configuration is checked out			
3.2.18.3.2	Duration of check-out			
3.2.18.3.3	Checked out by user details			
3.2.18.3.4	Checked-in details, as well as an interlock that requires a pre-defined comment box (a drop-down list) to be selected before the configuration can be checked back into the system			

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of National Transmission Company South Africa SOC Ltd Reg No 2021/539129/30

**CENTRALISED OT CONFIGURATION MANAGEMENT SYSTEM FOR
NTCSA**

Unique Identifier: **240-185000397**

Revision: **1**

Page: **49 of 60**

3.2.18.4	The system shall be able to generate a report providing the following details:			
3.2.18.4.1	The complete user details			
3.2.18.4.2	Date			
3.2.18.4.3	Time			
3.2.18.4.4	The actions taken by the user.			
3.2.19	The system shall be able to cater for access control, and as part of this requirement, it shall further satisfy the following requirements			
3.2.19.1	Handle access control with the following roles:			
3.2.19.1.1	Basic user – with read-only access and download-only			
3.2.19.1.2	Advanced user – with read and write access			
3.2.19.1.3	Administrator – with the ability to add/remove user access and manage the system.			

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of National Transmission Company South Africa SOC Ltd Reg No 2021/539129/30

**CENTRALISED OT CONFIGURATION MANAGEMENT SYSTEM FOR
NTCSA**

Unique Identifier: **240-185000397**

Revision: **1**

Page: **50 of 60**

3.2.19.2	The system shall be configurable to categorise the roles of users based on their geographic location and discipline-specific output			
3.2.19.3	In an emergency, an administrator shall be able to override the checked-out configuration, necessitate the required changes, ensure that version control is maintained, check in the updated configuration and inform the user that the configuration was changed as per the emergency requirements.			
3.2.19.4	The administrator of the system shall have the capability to manage the user's role-based access			
3.2.20	The system shall be able to cater for device configuration, and as part of this requirement, it shall further satisfy the following requirements			

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of National Transmission Company South Africa SOC Ltd Reg No 2021/539129/30

**CENTRALISED OT CONFIGURATION MANAGEMENT SYSTEM FOR
NTCSA**

Unique Identifier: **240-185000397**

Revision: **1**

Page: **51 of 60**

3.2.20.1	A user shall be able to define Job-Recurrence Definition tasks for devices that specify the frequency at which specific jobs are executed. Jobs that users can control include configuration retrieval. When new configuration files are retrieved, the system can send out email notifications to subscribers. There shall be 3 statuses for job retrieval,			
3.2.20.1.1	Complete - this means the job has been executed, and a new file has been retrieved.			
3.2.20.1.2	No Change - compares the configuration in the system to the one in the device.			
3.2.20.1.3	Failed - indicates that the system was not able to get the file for the device.			

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of National Transmission Company South Africa SOC Ltd Reg No 2021/539129/30

**CENTRALISED OT CONFIGURATION MANAGEMENT SYSTEM FOR
NTCSA**

Unique Identifier: **240-185000397**

Revision: **1**

Page: **52 of 60**

3.2.20.2	The system shall have an option to get the configuration; new configuration files are retrieved and compared with old configuration files. If a change is detected, the configuration is updated in the actual configuration library. Users can use the vendor-specific application to do a comparison between files (if supported by the application), to determine what the actual difference is within the working configuration library.			
3.2.20.3	The system shall provide a Published Configuration Library once a working library is approved through the configuration workflow by the authorised user. The work library configuration shall be sent to the published configuration library; this allows the user to update the configuration of the device. Alternatively, the user can use the remote engineering access to connect to the system to update the device.			

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of National Transmission Company South Africa SOC Ltd Reg No 2021/539129/30

**CENTRALISED OT CONFIGURATION MANAGEMENT SYSTEM FOR
NTCSA**

Unique Identifier: **240-185000397**

Revision: **1**

Page: **53 of 60**

3.2.21	The system shall be able to keep a record and track all configurations deployed on site: As-built and Work-in-Progress folder creation.			
3.2.22	The system shall be able to do version control of the configurations that are to be managed and effectively referenced and stored in the folder/location designated for such. The naming of configurations shall be identified for quick reference by users. The system shall have the ability to manage the different versions of configurations by providing a unique version number when saved back in the system			
3.2.23	The version history of all configurations shall be made accessible on the system.			
3.2.24	The system shall be able to provide a log of all activities related to check-in and check-out of the configurations, as well as flagging any configurations not checked in within the pre-defined period.			

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of National Transmission Company South Africa SOC Ltd Reg No 2021/539129/30

**CENTRALISED OT CONFIGURATION MANAGEMENT SYSTEM FOR
NTCSA**

Unique Identifier: **240-185000397**

Revision: **1**

Page: **54 of 60**

3.2.25	In the event of a system abnormality, the latest/running configuration on site shall be the default configuration for use			
3.2.26	Only authorised or/and authenticated users shall be able to check out, check in, delete, and edit the configurations.			
3.2.27	Role-based access control shall be managed: Viewing rights only, read and edit, and override any file that may be checked out by a specific user.			
3.2.28	The system shall be accessible remotely via VPN and the required system authentication.			
3.2.29	The system shall be able to cater for back-ups and recovery, and as part of this requirement, it shall further satisfy the following requirements			
3.2.29.1	The system shall provide a secured off-site backup of data in the event of system failure			
3.2.29.2	Daily back-ups of data shall be enabled to the off-site back-up			

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of National Transmission Company South Africa SOC Ltd Reg No 2021/539129/30

**CENTRALISED OT CONFIGURATION MANAGEMENT SYSTEM FOR
NTCSA**

Unique Identifier: **240-185000397**

Revision: **1**

Page: **55 of 60**

3.2.29.3	The period of record retention for a configuration file shall be in line with the device's life cycle			
3.2.29.4	The data at rest shall be encrypted according to the best-in-practice cryptographic controls.			
3.3	Operational & Maintenance Requirements			
3.3.1	The system shall be available and accessible 24 hours a day, 7 days a week.			
3.3.2	Users shall be able to update/revise the configuration history in the configuration, where the facility exists			
3.3.3	User application access to the system shall be managed in conjunction with the Line Manager of that specific user			
3.3.4	The system shall be able to generate logs of events such as failures, unauthorised access attempts, and abnormal system behaviours for the administrator to analyse and maintain the system as required.			

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of National Transmission Company South Africa SOC Ltd Reg No 2021/539129/30

**CENTRALISED OT CONFIGURATION MANAGEMENT SYSTEM FOR
NTCSA**

Unique Identifier: **240-185000397**

Revision: **1**

Page: **56 of 60**

3.3.5	The system shall generate notifications via email/SMTP to alert the administrator of any failures or abnormalities in the system as part of continued support. Only necessary and critical reporting shall be generated via email so as not to cause a nuisance.			
3.3.6	To ensure that the users can effectively operate, maintain, and troubleshoot the system. The system vendor/provider shall provide structured training and workshops for administrators, advanced users, and basic users before the system rollout and on an "as and when" required basis. The training shall include a role-based, hands-on workshop and any other relevant and necessary training, such as cybersecurity-related training for the system.			
3.3.7	The system vendor/provider shall provide all relevant manuals and documentation required by NTCSA as part of system delivery. This includes, but is not limited to, maintenance manuals, training manuals, etc.			

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of National Transmission Company South Africa SOC Ltd Reg No 2021/539129/30

**CENTRALISED OT CONFIGURATION MANAGEMENT SYSTEM FOR
NTCSA**

Unique Identifier: **240-185000397**

Revision: **1**

Page: **57 of 60**

3.3.8	There shall be contracts in place to define response times and support availability from the vendor. The system vendor/provider shall provide maintenance and support for at least a period of 5 years, including training for at least 2 years, which shall be in line with NTCSA's maintenance and support standards. The support shall include having system administrators acquainted with maintaining the system.			
3.3.9	The system shall cater for software updates & patches to ensure regular updates to maintain system security and functionality.			
3.4	Compliance, Testing & Deployment Requirements			
3.4.1	The system shall comply with all relevant industry standards, acts and protocols in line with configuration management, such as ISO 10007, and the devices to be managed as per Appendix A.			

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of National Transmission Company South Africa SOC Ltd Reg No 2021/539129/30

**CENTRALISED OT CONFIGURATION MANAGEMENT SYSTEM FOR
NTCSA**

Unique Identifier: **240-185000397**

Revision: **1**

Page: **58 of 60**

3.4.2	The system shall be able to be tested for functionality as per the NTCSA's applicable testing processes and standards. Functions such as role-based access control, multi-protocol support and verification that configurations can be applied, modified, and rolled back without errors, etc, shall be evaluated and verified.			
3.4.3	It shall be proven and/or demonstrated that the system is secure and not prone to cyber-attacks as per IEC/SANS 62443-3-3			
3.4.4	As part of testing, the load and stress test simulation for large-scale substation environments shall be assessed to prove the performance of the system under high load. This shall be conducted and/or demonstrated/evidence provided.			

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of National Transmission Company South Africa SOC Ltd Reg No 2021/539129/30

Appendix C: Extended OT Definition

C.1 OT Definition

In the Eskom context Operational Technology (OT) is defined as:

Operational systems which form **part of** Eskom's **plant / network assets**, and which could by virtue of design, maintenance or operation **directly** result in the failure of these assets to meet their **purpose and performance criteria**, where:

- **Operational systems:** are all systems (including electronic, telecommunications and computer systems and components) which process, store or communicate operational data or information.
- **Part of:** means contribute to the asset meeting its purpose and performance criteria.
- **Plant / network assets:** are any part of the "built environment" utilized by Eskom to run its production, delivery and logistics processes, including generation, transmission and distribution of electricity, etc.
- **Directly:** means in real time or near real time. E.g. would include supervisory control systems, but would exclude spares ordering applications (even though these could eventually result in the failure of the asset).
- **Purpose and performance criteria:** The "design to", "maintain to" and "operate to" criteria that are generally specified formally.

Systems, sensors, transducers and Programmable Local Controller equipment, which extract signals and measurements from the plant / network asset or its control environment, or facilitate control over the these assets generally meet the above criteria and qualify as OT, since their failure could directly result in the failure of the plant / network asset or its ability to meet its purpose and performance criteria.

In some cases, obvious failures of **operational systems** may not directly result in the failure of purpose or performance of the **plant / network asset**, but because of the way it is designed, normal operations or maintenance of the operational system could result in a risk to the plant / network asset. An example is:

- Voltage spike induced in a control circuit due to a lightning strike on the power supply of an IT server not fitted with the same spec of surge protection as used on the control circuit, and inadequate voltage supply decoupling (e.g. optical decoupling).

Such equipment generally meets the above criteria and qualifies as OT, since their design, operation or maintenance could directly result in the failure or impact of the plant / network asset or its ability to meet its purpose and performance criteria.

CONTROLLED DISCLOSURE

C.2 Typical characteristics of OT, IT and joint OT/IT systems

	Operational Technology (OT) OT is about running the electrical network	Information Technology (IT) IT is about enabling the business	Joint OT/IT End to end business optimisation
Purpose / Role	Manage / monitor / control physical assets, plant and network equipment.	Process business transactions, provides communication, information, supports people, decision making and data.	End to end solutions => Convergence.
Architecture	Embedded hardware/software – application specific, purpose built substation Local Area Networks (LANs) and Wide Area Networks (WANs) for grid operations and engineering purposes.	Generic enterprise Local Area Networks, on site Network Edge IP Routing and Data Centre infrastructure and applications, MPLS, ISP.	Common Information Model (CIM) IP/MPLS.
Security	NERC-CIP (Critical Infrastructure Protection) compliant. OT Security that is utility best practice.	Generic Enterprise Cyber Security – ISO27001/2. Overall enterprise cyber security risk.	Integrated Cyber Security.
Interfaces	Electromechanical, coded displays/customised Graphic User Interfaces (GUIs), computer based Human Machine Interface (HMI).	Windows-based GUI, terminal and keyboard (desktop / laptop).	Converged connectivity.
Connectivity	Mostly hardwired control networks, serial / non-IP protocols, may use Internet Protocol (IP) as part of protocol stack. This includes telecommunication infrastructure.	Typically IP-based connectivity with significantly lower performance requirement except between data centres, voice and video applications.	Converged connectivity.
Operating Systems	Application dependent deterministic or non-deterministic multitasking, embedded.	Non-deterministic multitasking, e.g. Windows.	Mixed and / or converged / shared.
Environment	Typically deployed in harsh environments.	Typically deployed in office environments	Mixed and / or shared.
Type of Data	Real time / Near-real time data.	Non-real time, batch orientated data for Enterprise systems, real-time for IP-based voice, video, inter-data centre, mobile data terminals..	Various as required by end to end solutions.
Ownership	Technology Group and Operating Unit managers.	Group IT.	Group owned, jointly governed or as per business model.
Usage	24/7 availability required.	Mainly business window but can also be 24/7.	Various as required by end to end solutions.
Service Provisioning	Services usually cannot be outsourced due to the critical infrastructure needs.	Some Services are outsourced but all under control of Group IT.	Core not usually outsourced.
Consequence of Failure	Risk of electricity network downtime, potentially catastrophic, security risk, loss of life.	Less likelihood of impact on network operations. Transaction delays and unproductivity and impact on business operations. Can include loss of life.	Combination of both.
Business continuity	Keeping the lights burning. Core product mission critical systems and services including its facilities and support systems.	Business processes critical support systems including its facilities and support systems.	End to end optimised operations.
Typical present examples	EMS, SCADA, Substation Automation (SA), Distribution Automation (DA). Protection Schemes, Meters, Telecommunications infrastructure, etc.	Solutions and systems for SAP, Outlook, Maximo, SAP, SPF, OVS, CC&B, Smallworld, etc.	DMS, AMI, MDMS, MV90, Visualisation, etc.

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of National Transmission Company South Africa SOC Ltd Reg No 2021/539129/30