Eskom	Standard	Technology

Title: **REMOTE DEVICE COMMUNICATION STANDARD FOR DATA RETRIEVAL AND REMOTE ACCESS**

Unique Identifier:	**240-64038621**
Alternative Reference Number:	**<n/a>**
Area of Applicability:	**Engineering**
Documentation Type:	**Standard**
Revision:	**3**
Total Pages:	**21**
Next Review Date:	**January 2027**
Disclosure Classification:	**Controlled Disclosure**

Compiled by	Approved by	Authorized by
Jason Hector	Rishi Hariram	Naresh Hari
Chief Engineer – Control and Automation	Control and Automation Manager	General Manager Transmission Engineering
Date: 22/12/2021	Date: 23/12/2021	Date: 2022-01-04

Supported by SCOT/SC

Nelson Luthuli

PTM&C TC Chairperson

Date: 04 January 2022

PCM Reference: **240-44509543 – PCM Design Systems**

SCOT Study Committee Number/Name: **Telecontrol Study Committee**

Content

1. Introduction

Visibility of the Eskom power network is one of the key criteria required to achieve operational success. Consequently, the communication requirements of remote devices have traditionally been specified to meet the operational needs of Supervisory Control and Data Acquisition (SCADA) control centres. Visibility of network key performance indicators has since transcended and now also includes non-operational activities.

The need for Eskom's engineering departments to provide oversight into network operations, management and monitoring of its plant is now fundamental to the business operations. This can only be achieved through the availability of both operational and non-operational data.

Traditionally the retrieval of non-operational data has been a manual process, requiring an individual to travel to site to upload files (i.e. event or disturbance files) from a device. The benefits of automating the data retrieval and consequently the integration of all data sources into one repository have been identified as a key requirement to further the business into a high-performance utility. An important step required to achieving this data integration, is to ensure that the communication profile of remote devices (also referred to as remote sensors) aligns to a fundamental set of requirements as defined in this document. These requirements will ensure that (a) the future integration of remote devices' data into the corporate data repositories is allowed for, and (b) the devices can be remotely engineered.

2. Supporting clauses

2.1 Scope

2.1.1 Purpose

This standard outlines the requirements for the communication protocol and physical port(s) of any remote device installed within Eskom's Distribution and Transmission network in order to ensure that consistency is maintained with respect to the specification, design and implementation of remote devices.

Eskom specifications for remote devices (Intelligent Electronic Devices (IEDs), remote sensors, Current and Voltage Monitors (CVMs), Fault Path Indicators (FPIs), Dissolved Gas Analysis (DGA) devices, Power Quality (PQ) devices, Travelling Wave Fault Locators (TWS), Reclosers, rural voltage regulators, Telemetered Ring Main Units (RMUs), capacitor banks, etc.) shall, through references to this document, ensure their compliance with the communication standards detailed within.

2.1.2 Applicability

This standard shall apply to Eskom's Distribution and Transmission divisions.

2.2 Normative/informative references

Parties using this document shall apply the most recent edition of the following documents:

[1] IEC 61850, Communication networks and systems in substations

[2] IEC61850-3, (General requirements including EMI type tests)

[3] IEC61850-7-4, Basic communication structure for substation and feeder equipment – compatible logical node classes and data classes

[4] IEEE1815-2012 (DNP3), IEEE Standard for Electric Power Systems Communications – Distributed Network Protocol (DNP3)

[5] IEC 60870-5-101, Transmission protocols, companion standards especially for basic Telecontrol tasks

[6] Modbus Messaging on TCP/IP Implementation Guide

[7] IEEE-1588-2008, Standard for a precision clock synchronization protocol for networked measurement and control systems (version 2)

[8] IEEE C37.238-2011, Standard profile for use of IEEE 1588 precision time protocol in power system applications

[9] 240-53902530, Substation automation – data concentrator specification for data retrieval and remote access

[10] 240-55410927, Cyber Security standard for operational technology

[11] 240-61268959:, Substation Automation Network Architecture Standard for Transmission Substations

[12] 240-81321219, Substation Automation Network Architecture Standard for Distribution Substations

[13] 240-61478967, Eskom slave IEC60870-5-101 implementation standard

[14] 240-42066934, IEC 61850 Protocol Implementation document for the purpose of substation automaton

[15] 240-68107841, Eskom IEC 61850 standard requirements for PICS, PIXIT and TICS

[16] 240-6825024, Eskom IEC 61850 station bus interoperability test standard

[17] 240-59089329, Eskom's DNP3 Implementation Standard

2.2.1 Informative

None

2.3 Definitions

2.3.1 General

Definition	Description
Data Concentrator	A device, located typically within a substation or remote location, which extracts data from several other devices/remote sensors utilizing various protocols and communicates this data back to a centralized point. A data concentrator also facilitates secure remote access sessions to devices and includes logical functions that can facilitate substation automation.
Data Retrieval	Refers to the retrieval of both Engineering Data and Operational Data.
Device/Remote Device	These devices, which are installed either inside or outside the perimeter of a substation, monitor the condition and operation of plant equipment and environmental conditions and, in some cases, can exhibit control on the power system through protection elements. Note that Intelligent Electronic Devices (IEDs) such as installed within a substation are included in this scope.
Engineering Data	This includes all data available from control plant, monitoring and auxiliary systems, and could include operational data. Its use within the power system network reaches beyond the controlling aspect thereof and rather relates to the fundamental base upon which technicians, engineers, managers and other parties of interest use the data to expand and optimize the power system.
Enterprise Historian	Historians are used as the repository of near real-time and real-time process information. These systems allow process information to be viewed and manipulated by all of the corporate users of such information. A historian also interfaces data to and from other condition monitoring and decision-based systems that use or generate process-type data.
Field Controllable Device	Field controllable devices are multifunctional Intelligent Electronic Devices (IEDs) that are used for the protection, monitoring and control of power systems lines, as well as other field installations. These are devices that are typically installed on the line i.e. Pole Mounted Recloser, Voltage Regulator, etc.

Definition	Description
Integrated Device	An Integrated Device is a device or remote devices where the intelligent hardware, software (the IED part) and remote communications (such as cellular modems) are integrated as part of the end equipment and cannot be separated or operate independently from the end equipment. Examples include self-regulating transformers with integrated power electronics and a distribution Current Voltage Monitor (CVM), where the communications and intelligent electronic hardware form part of the unit itself.
Low-Power Device	A class of devices, typically full integrated, that has a very conservative internal energy storage capacity and by virtue of this only reports data upon an event or scheduled basis. These devices cannot be interactively polled for data or remotely engineered unless they are interrogated within a predetermined 'awake' time period, i.e. Fault Path indicator.
Operational Data	This is data that is crucial to the monitoring and operation of the power system network and is applicable to Supervisory, Control and Data Acquisition (SCADA) systems. It includes real-time analogue network loading data such as voltages, currents, power flows, and also the status of primary plant equipment such as breakers and isolators. It is the fundamental information required to monitor and control the network.
Serial Device Server	A network device containing RS232 and RS485 ports with the ability to encapsulate serial data into an Ethernet connection. Each serial port typically has a single Internet Protocol (IP) socket mapped to a serial port.
Substation-based Device	A class of multifunctional Intelligent Electronic Devices (IEDs) that are used for switching, protection, monitoring and control of primary and secondary plant equipment installed in a substation.

2.3.2 Disclosure classification

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

2.4 Abbreviations

Abbreviation	Description
ASCII	American Standard Code for Information Interchange
CPU	Central Processing Unit
CVM	Current and Voltage Monitor
DGA	Dissolved Gas Analysis
DNP3	Distributed Network Protocol v.3
EDNS	Electricity Delivery Network Services
FC	Functional Code
FPI	Fault Path Indicator
FTP	File Transfer Protocol
GOOSE	General Object Orientated Substation/System Event
GPRS	General Packet Radio Service
GPS	Global Positioning System

Abbreviation	Description
GSE	Generic Substation Event
HSDPA	High-speed Downlink Packet Access
HTTP	Hypertext Transfer Protocol
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
IEEE	Institute of Electrical and Electronics Engineers
IMEI	International Mobile Equipment Identity
Ind	Index
IP	Internet Protocol
MIB	Management Information Base
MICS	Model Implementation Conformance Statement
MMS	Manufacturer Messaging Specification
n/a	not applicable
NTP	Network Time Protocol
OT	Operational Technologies
PC	Personal Computer
PDU	Protocol Data Unit
PID	Protocol Implementation Document
PIN	Personal Identification Number
PQ	Power Quality
PTM&C	Protection, Telecommunications, Metering and Control
PUK	Personal Unlocking Key
QC	Qualifier Code
Qty	Quantity
RF	Radio Frequency
RTU	Remote Terminal Unit
SC	Study Committee
SCADA	Supervisory Control and Data Acquisition
SIM	Subscriber Identity Module
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
TCP	Transfer Control Protocol
TICS	Technical Issues Implementations Conformance Statement
Tissues	Technical Issues
TWS	Travelling Wave Fault Locator

Abbreviation	Description
UDP	User Datagram Protocol
UML	Unified Modelling Language
UTC	Coordinated Universal Time
VLAN	Virtual Local Area Network
WAN	Wide Area Network
WiMAX	Worldwide Interoperability for Microwave Access

2.5 Roles and responsibilities

Not applicable.

2.6 Process for monitoring

Not applicable.

2.7 Related/supporting documents

Not applicable.

3. Requirements

3.1 General

3.1.1 Landscape and services overview

Eskom's Enterprise Historian roll-out plan entails a collection of historians distributed throughout all of Eskom's entities. This farm of historians operates in a meshed landscape to create a flexible structure within which data and information are acquired, shared and visualised.

Note: That due to the flexible nature by which the historians can be deployed, the architectures discussed in this document are not exhaustive and are only used to illustrate data acquisition principles.

1 gives a high-level overview of the communication requirements for remote devices. The communication between the enterprise systems and remote device(s) is represented by the bold lines.

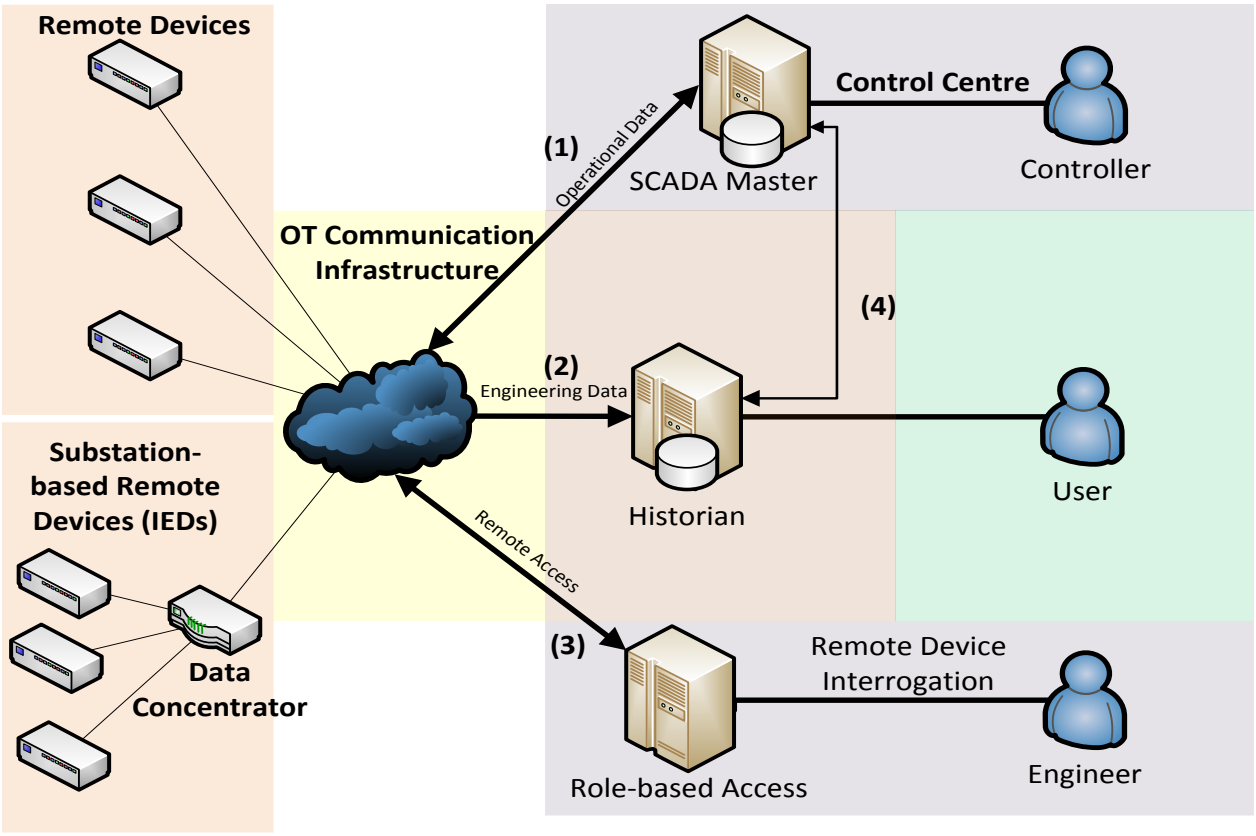

Figure 1: Regional landscape overview

As depicted in 1, Remote devices shall be capable of interfacing to the SCADA Master, Enterprise Historian and role-based access system. Through these interfaces the remote device shall be able to facilitate the retrieval of operation data, engineering data and remote access (remote interrogation, configuration and file retrieval)

Support for interfacing of operational data to control centres shall always be supported and aligned with the requirements of the respective device specification within Eskom.

1 details the type of data that shall be supported by each communication link on the device. The physical requirements of the communication interface are defined in 3.2.

Table 1: Remote device interfaces

Communication link	Data type	User	Supported Protocols
Remote device to SCADA master **(1)**	This link shall cater for all operational interfaces required for the remote device. The specific use case for each sensor shall identify whether this interface is required.	Control Centre	Transmission: IEC 60870-5-101 Distribution: DNP3
Remote device to Historian **(2)**	This link shall cater for all engineering data provided by a remote device. If required by the business, the data included in this link might include operational data.	Engineers	Transmission: DNP3 Distribution: DNP3
Remote device to role-based access **(3)**	This link shall cater for the remote interrogation and configuration of the remote device.	Engineers, technicians and field staff	Not Applicable

Communication link	Data type	User	Supported Protocols
SCADA master to dedicated/provincial historian **(4)**	This link forms part of the internal landscape and is not considered a function of the remote device. It is included for reference purposes.	All	Not Applicable

3.2 Device Classes

a) Intelligent Electronic Devices (IEDs) are engineered to solve a variety of utility-specific needs. They are deployed within substation control rooms, substation yards, HV and MV lines, LV reticulation networks, etc. Depending on the design-criteria of each device type, a suitable communication solution is engineered to support SCADA, remote engineering and data retrieval within the constraints of such device. Eskom recognises the differences in devices used within the electricity transmission and distribution industry, and differentiate between these devices based on the device classes tabulated in Annex A.

b) In addition to defining these classes, each class is also mapped to various requirements that shall be supported as indicated for such class. The following notation is used:

1) Mandatory = $\mathbf{M_{DIV}}$ (requirement shall be met by the device, subscript 'DIV' is used to indicate requirements applicable only to a specific division)

2) Preferred = **P** (requirement that is highly preferred by Eskom and as such measured for compliance)

3) Optional = **O** (requirement that is preferred by Eskom, yet not functionally measured for compliance)

c) Refer to Annex A for the mappings between device types and requirements.

3.3 Solution architecture

a) Communication solutions for remote devices can vary depending on their original design criteria. Some solutions cater for decoupled systems and use internationally standardized protocols to communicate operational and engineering data. Other solutions use proprietary protocols and middleware through which users interface to the device to obtain data. These tightly coupled solutions where the link between the higher-end acquisition systems and end device is proprietary are strongly discouraged, as they inhibit the integration of their data into Eskom's data repositories. It is also noted that in some cases, proprietary middleware can be used to expose internationally standardized protocols through which other systems collect data. However, this practice is discouraged due to the additional maintenance overhead of the middleware and the additional point of failure within the data flow.

b) In order to ensure future standardization, decoupled systems and interoperability, remote devices shall implement and expose on the communication ports, an internationally recognized open protocol for the communication of all operational and engineering data, regardless of whether or not their native solution uses middleware.

c) Remote devices shall also support the remote engineering and configuration of the device. Users should be able to configure the device from a remote location through an Eskom-approved role-based access system.

d) The device's native interrogation and configuration software shall support virtual serial port drivers and/or Transfer Control Protocol (TCP) proxy connections as redirect portals into the device. These virtual proxies (or remote connectors) are created on-demand within the user's Personal Computer (PC) through which the native application is connected to the remote sensor. This requirement is explicitly added to ensure that the use of looped serial ports (whereby two physical ports are connected together to realise a hardware port) on a user's PC is prevented, as is required by some legacy software configuration tools.

e) In order to ensure interoperability with Eskom's approved role-based access system, any replies to TCP/Internet Protocol (IP) traffic into devices shall only be to the source port of the originating system's transport session. The opening of new ports from the device to the role-based access system shall not be allowed.

f) In the sections to follow, Eskom provides the requirements to enable the decoupling of devices from proprietary systems.

g) Protocols implemented by a device shall strictly comply with the definition of that protocol. Any deviations shall be clearly stated, even though these are not encouraged.

3.4 Physical Communication Interfaces

a) Substation Devices:

1) Refer to [11] and [12] for physical Ethernet ports required by substation-based device.

2) When physical redundancy is required at the port level, additional switched Ethernet ports shall be required and specified accordingly by a device's Eskom specification. **Note that the Eskom specification (compiled by the custodian of a device or scheme) for a device may require other additional Ethernet ports be provided.**

b) Field controllable (Non-Substation) Devices:

1) Devices (excluding Integrated Devices) shall, as a minimum, have one 100Base-Tx Ethernet port with full support for data retrieval and remote access.

2) Low powered devices utilising short/medium/long-range radio to a close-coupled micro-RTU shall comply with requirement b)1) above.

3) For Integrated Devices (that utilizes an internal cellular modem for all data communication data retrieval and remote access), it shall be highly preferable to support such functionality over a 100Base-Tx port. If a 100Base-Tx port is not supported, it shall be mandatory to support data retrieval and remote access over a RS232 port, in addition to the integrated cellular modem.

3.5 Data retrieval and remote access protocol support

3.5.1 Data retrieval

a) Substation devices

The following list of standardized protocols is required, in order of preference, for any substation-based device that is a source of operational or engineering data. These protocols align with Eskom's requirements for IED communications to a Data Concentrator and Historians. Note that at least one protocol shall be implemented by any device for data retrieval. Support for more than one listed protocol from a device shall be highly preferable.

1) IEC 61850-8-1 Manufacturer Messaging Specification (MMS) Server [1].

2) IEC 60870-5-101 [5] is mandatory for devices that will be deployed within Transmission.

3) Distributed Network Protocol v.3 (DNP3) as specified in the IEEE1815-2012 standard [4], is mandatory for devices that will be deployed within Distribution.

4) ModbusTCP [6]. Although included, this protocol shall only be considered for legacy and small embedded data sources that either natively implemented this protocol or cannot support any of the other listed protocols due to hardware limitations. This protocol will not be considered for new devices.

b) Field controllable (Non-Substation) devices shall implement:

1) Distributed Network Protocol v.3 (DNP3) as specified in the IEEE1815-2012 standard [4], is mandatory for devices that will be deployed within Distribution.

2) IEC 60870-5-101 [5] is mandatory for devices that will be deployed within Transmission.

3) In addition, preferably also include an IEC 61850-8-1 MMS Server.

c) All protocols implemented shall support the ability to address at least two independent masters on each instance of the protocol, with unique data sets for each configured instance of the protocol.

d) Devices with sleep functionality that disables communication interfaces shall utilise UDP when reporting to a master. TCP shall be implemented as an additional (selectable) option.

e) Devices should preferably implement SNMPv2c (preferably also SNMP v3) or utilise its data retrieval protocol for the communication of vital statistics pertaining to the status of their Ethernet port(s), including:

1) Current operational state of each interface (separate values).

2) Uptime.

3) Number of packets in and out (separate values).

4) Number of octets in and out (separate values).

5) Number of errors in and out (separate values).

6) Number of discards in and out (separate values).

7) Number of failed, established and current UDP and TCP connections.

8) Self-diagnostic data including Central Processing Unit (CPU) utilization; use of volatile and non-volatile memory; and any other data deemed necessary for the remote status diagnosis of the device.

3.5.2 Remote access protocol support

a) Remote access into devices:

1) Shall enable the configuration of the device;

2) Shall allow the applying of settings in the device ;

3) Shall enable firmware updates in the device;

4) Shall enable password changes;

5) Shall allow the viewing of access and statistical logs;

6) Shall enable the extract the sequence of events, disturbance records, log files etc., and

7) Shall allow the viewing of instantaneous values of all data points (i.e. digital input, analogue input, etc.)

b) Protocols used to achieve remote access to devices shall, in order of preference, include one or more of the following:

1) IEC61850-8-1 (MMS Server).

2) Hypertext Transport Protocol (HTTP) or Hypertext Transport Protocol Secure (HTTPS).

3) Secure Shell File Transfer Protocol (SFTP) or FTP (passive) with a configurable fixed range of data ports.

4) A stateless ASCII-based protocol delivered over a SSH or Telnet session.

c) In the event that IEC61850 is not supported as the remote access protocol, the supported protocol shall be defined as required by the Proprietary Protocols (section 3.7).

3.5.3 Files

a) The exchange of any files from a remote device shall be decoupled from its native configuration tool(s) and support such exchanges over an internationally recognized open protocol. In order to achieve the decoupling of any files contained within remote devices, the services provided to transact these files shall include one or more of the protocols as defined further below. Note that the following protocols required to transact files are applicable to both substation-based devices and field controllable devices.

b) Devices that contain waveform, event, sequence of event, configuration and/or any other files of interest shall support, in-order of preference, one or more of the protocols listed below to exchange these files:

1) Secure Shell File Transfer Protocol (SFTP) or FTP (passive) with a configurable fixed range of data ports.

2) Hypertext Transport Protocol (HTTP) or Hypertext Transport Protocol Secure (HTTPS).

c) Support for IEC 61850-8-1 MMS Files Services shall be highly preferable in addition to the preceding list of requirements.

d) Regardless of the method of file exchange, the supplier shall unambiguously state the location of each type of file within its file structure. Such detail shall include any additional detail required to automatically retrieve these files from a third-party system.

e) The device shall have the ability to directly push (as opposed to being pulled/polled) files onto an FTP file server.

f) Low-powered devices shall support FTP for the purposes of retrieving configuration updates. A relative folder location, FTP login credentials and update schedule shall be configurable by the user.

g) The file types supported shall be;

1) Well-defined, structured, parse-able files such as XML, CSV, JSDON, YAML for configuration files

2) Flat files or preferably IEEE C37.239-2010 (COMFEDE) for Sequence of events (SOE) files

3) COMTRADE for waveforms and event data

h) Devices pushing files to a centralised FTP server shall not send scripts or executable file types.

3.5.4 Protocol certification

a) IEC 61850 devices shall comply with the [14] IEC 61850 Protocol Implementation document for the purpose of substation automaton, [15] Eskom IEC 61850 standard requirements for PICS, PIXIT and TICS, and [16] Eskom IEC 61850 station bus interoperability test standard.

b) Conformance requirements in 3.5.4.a are required to provide KEMA certifications against the conformance requirements.

c) For devices implementing DNP3, the device's slave implementation shall:

1) Be certified by an internationally accredited test facility or as a minimum requirement (where allowed by Eskom) provide Eskom with self-test results against Eskom test procedures stipulating the level of conformance testing that has been performed on the device.

2) Support, as a minimum, an application-specific profile as deduced from Annex B.

3) Support unsolicited report-by-exception.

4) Support solicited report-by-exception.

d) Devices implementing [5] IEC 60870-5-101 shall comply with the latest version of [13] 240-61478967.

3.5.5 Data modelling support

a) IEC 61850 enabled devices shall:

1) Implement the full mapping of all internal data to the latest Eskom prescribed Model Implementation Conformance Statement (MICS).

2) Where Eskom's mapping is not sufficient for an application, use the latest edition of IEC 61850-7 data models.

3) Only use GGIO logical nodes for data that cannot be attributed to any logical nodes and data classes prescribed by Eskom or those listed in the latest edition of [3] IEC61850-7-4, and for which an extension to the standardized logical nodes cannot logically be made.

b) Devices implementing DNP3 shall both include a complete DNP V3.00 Device Profile Document as described in the 'DNP V3.00 Subset Definitions' as well as a soft copy of the DNP3 XML Device Profile.

3.6 Security

Support for authentication before access, shall be required as follows:

a) All substation-based and field controllable devices shall:

1) Support authentication by means of a username and associated password.

2) Preferably support three levels of access and include a read-only user; a superuser with write access to the device's configuration and outputs; and an administrator that can change user credentials.

b) The following requirements should preferably apply to all field controllable devices

1) Support encryption algorithms that can be used to secure the link to the device.

2) Such encryption shall be scalable for multiple local and remote connections.

3) Encryption algorithms shall support a key that is 128 bits or larger.

4) Should certificates be required as part of the encryption technique used by a device, the device shall support the import of a self-signed, password-protected certificate (including the private key where applicable) generated by Eskom. Any certificate imported into a device shall be securely stored and only available by using special elevated credentials.

5) Low powered devices with an integrated modem that support Short Message Service (SMS) as an option for sending settings shall only accept messages from pre-configured Mobile Station International Subscriber Directory Numbers (MSISDNs).

c) It shall be highly preferable for substation-based devices to support unique Virtual Local Area Network (VLAN) tagging of each service provided by the device. Such a mechanism shall enable each service exposed by the device to be virtually segregated within a network. If implemented, the use thereof shall be user-configurable within the device, including the option to switch it off.

3.7 Proprietary protocols

a) Devices that do not support IEC61850 as its remote access protocol shall make available to Eskom the complete definition of its proprietary protocol(s) (as listed in 3.5.2).

b) The protocol definition shall include, where applicable, the detail of all:

1) Logical ports used (such as in the case of TCP and User Datagram Protocol (UDP) ports).

2) Sequence of exchanges (preferably in a Unified Modelling Language (UML)) to perform any action via the remote access protocol.

c) Upon Eskom's request, the manufacturer shall supply all functions and required subroutines in Pseudocode to retrieve and change (where applicable) the following data within the device. The Pseudocode shall be detailed enough to enable the translation thereof into any programming language:

1) Files such as event, configuration and waveform files.

2) Configurations.

3) Usernames and passwords.

4) Automated login and logout of the device.

5) Automated configuration retrieval into a device-specific file format.

6) Firmware and software revision.

3.8 Timing requirements

a) Cross-referencing and correlating of wide area disturbances require accurate event timestamps between devices. Depending on the device's location (substation-based or not), the requirements on the accuracy of its timing class will differ. Substation-based devices will require both accurately referenced time to the Coordinated Universal Time (UTC) as well as a higher internal time resolution and corresponding event timestamps. Devices that are not substation-based are typically time synchronized over Wide Area Network (WAN) based protocols for which these requirements are relaxed.

b) All substation-based devices shall:

1) As a minimum, support the synchronization of their internal clocks through the Simple Network Time Protocol version 3 (SNTP v3) protocol.

2) Preferably provide support for [8] IEEE C37.238-2011 through the use of [7] IEEE-1588-2008.

3) As a minimum, support T1 internal clock accuracy. The resolution of the internal clock shall therefore be at least 1ms. All timestamps of data shall consequently also have a resolution of 1 ms or better.

c) Field controllable devices shall:

1) Support a mechanism by which their internal clocks can be synchronized.

2) Support SNTP v3 if they natively include an IP stack.

3) As a minimum, support T0 internal clock accuracy. The resolution of the internal clock shall therefore be at least 10 ms. All timestamps of data shall consequently also have a resolution of 10 ms or better.

d) Any device that includes a Global Positioning System (GPS) receiver (typically used for location-based services) shall optionally use such receiver as a selectable source for its internal time synchronization.

3.9 Communication latency and bandwidth management requirements

a) All communication protocols supported by a device shall tolerate latencies up to at least 5 000 ms in each direction. This timeout setting shall be configurable in steps of at least 100 ms.

b) During periods of high latency, low throughput due to limited bandwidth and/or complete communication outages, the device shall buffer any exception-class data to be reported to the master station. The buffering capabilities of the device shall be made available to Eskom.

c) Should the device implement a connectionless transport protocol (such as UDP), it shall include some feedback mechanism (application layer acknowledgement) that can detect and compensate for any intermittent loss of communication due to an unreliable communication medium.

d) Regardless of the communication protocol used, the device shall, where supported by the layer of protocol, support a configurable PDU to better utilize the available bandwidth.

4. Authorization

This document has been seen and accepted by:

Name and surname	Designation
J Mathebula	Smart Grid Study Committee Chairperson
Ian Naicker	Chief Engineer: PTM&C - Control and Automation
Kenneth Brown	Chief Engineer: Distribution
Kgomotso Manyapetsa	Senior Engineer: PTM&C – Control and Automation
Simphiwe Mbanga	Standards and Implementation - ECOU
Thendo Ramulondi	Standards and Implementation - LOU
Colin Charles	Standards and Implementation - WCOU
Tjaart van der Walt	Standards and Implementation - NCOU
Johann Pretorius	Standards and Implementation - MOU
Riaz Asmal	Standards and Implementation - KZNOU
George Daniel	Standards and Implementation - GOU
Comfort Masike	System Operator Senior Manager
Danie Du Plessis	Senior Manager Grids
Busi Green	Gx Representative
Mervin Mottian	Dx SCADA Representative

5. Revisions

Date	Rev	Compiler	Remarks
Jan 2022	3	J. Hector	Removed section: Network Interface Management. Modification on assessed compliances.
Sept 2016	2	E. Luwaca	Section 3.2 introduces device classes, and all the requirements are categorised into whether the device is a substation or field device. Section 3.5.2 and Section 3.5.3, the remote access protocol and file transfer methods have been revised. File Types that should be supported for configuration, event and SOE files are specified.
July 2013	1	T J Hyman	First issue.

6. Development team

Tertius Hyman	WCOU Network Engineering and design
Juan Atkins	WCOU Network Engineering and design
Kgomotso Manyapetsa	PTM&C Control and Automation
Elekanyani Mugivhi	PTM&C Control and Automation

7. Acknowledgements

Not applicable.

Annex A – Device Classes

Device Class	3.3	a)	b)	c)	d)	e)	f)	g)	3.4	a)1)	a)2)	b)1)	b)2)	b)3)	3.5	3.5.1	a)1)	a)2)	a)3)	a)4)	b)1)	b)2)	b)3)	c)	d)
Substation-based		M								M	M						M							M	
Field Controllable		M										M		P							$M_{(DX)}$	$M_{(TX)}$	P	M	
Low powered		M										P	M	P							$M_{(DX)}$	$M_{(TX)}$	P	M	M

Device Class	e)1)	e)2)	e)3)	e) 4)	e) 5)	e) 6)	e)7)	e) 8)	3.5.2	a)1)	a)2)	a)3)	a)4)	a)5)	a)6)	a)7)	b)	c)	3.5.3	a)	b)	c)	d)	e)	f)	g)
Substation-based	P									M							M	M		M	M	P	M	P		M
Field Controllable	P									M							M	M		M	M	P	M	P		M
Low powered										P							M	M		M	M	P	M	M	M	M

Device Class	h)	3.5.4	a)	a)	c)	d)	3.5.5	a)1)	a)2)	a)3)	b)	3.6	a)1)	a)2)	b)1)	b)2)	b)3)	b)4)	b)5)	c)	3.7	a)	b)	c)
Substation-based	M		M	M	M	M		M			M		M	P						P		M	M	M
Field Controllable	M		M	M	M	M		M			M		M	P	M	M	M	M				M	M	M
Low powered	M		M	M	M	M		M			M				M	M	M	M	M			M	M	M

Device Class	3.8	a)	b)1)	b)2)	b)3)	c)1)	c)2)	c)3)	d)	3.9	a)	b)	c)	d)
Substation-based		M	M	P	M				M		M	M	M	M
Field Controllable		M				M	M	M	M		M	M	M	M
Low powered		M				M	P	M	M		M	M	M	M

Notes:

- A blank box implies that the requirement is Not Applicable to the device class
- $M_{(DX)}$ – Mandatory for Devices used with Eskom Distribution only
- $M_{(TX)}$ – Mandatory for Devices used with Eskom Transmission only

Annex B – DNP3 minimum compliance level

(Normative)

B.1 Introduction

B.1.1 DNP3 is currently the de facto protocol used in Eskom Distribution for SCADA remote communication from devices within and outside of the substation. The purpose of this annex is to standardize on the minimum level of compliance required from any (non-Remote Terminal Unit (RTU)) device that either claims support or is required to support DNP3.

B.1.2 In addition to the minimum DNP3 services and data mapping requirements detailed further below, it shall be highly preferable for devices supporting DNP3 to meet or exceed the implementation of IEEE 1815, Level 3 [4].

B.1.3 The implementation shall preferably also comply with the latest DNP3 IED Certification Procedure for Subset Level 2.

B.2 Definitions

B.2.1 In B.1, the object heading contains DNP3 types and a flag as described below:

Table B.1: DNP3 object types

Abbreviation	Description	Eskom use
S	Static	Static objects are set (write) and retrieved (read), solicited as required. These points can, however, also belong to an equivalent event object that enables unsolicited reporting of the point.
E	Event	Event-based objects are reported unsolicited upon a change of the data. Note that dead bands or delta windows are a function of the device and shall be supported separately.
C	Command	Command objects are used to perform control on output objects typically related to direct operations on the power network. This object includes function codes that enable Select-before-Operate functions. For all other output operations, static output objects should be used.
I	Info	Info objects are related to the internal operations of the device.
Flag		A flag is an octet (byte) of data included in a response that indicates the state of the objects being read. This octet usually contains the health of that object (e.g. Online, Restart, Comm_Lost, Rollover, Over_Range.)

B.3 DNP3 Requirements

B.3.1 The data provided by a device shall be mapped to the approved DNP3 objects as defined below.

B.3.2 All data deemed part of the general sequence of events (during power network fault and disturbances) shall always be mapped to event-based objects.

B.3.3 If event-based objects are supported by the device's DNP3 implementation, the assignment of such events to class data (object 60) shall be supported as **configurable within the device**.

B.3.4 Event-based data shall preferably also have the ability to be assigned to grouped class data **by the master**.

B.3.5 When responding with binary event data and more than one event has occurred for a data point, a device shall include all events.

B.3.6 The Functional Codes (FCs) and Qualifier Codes (QCs) listed in B.2 shall be the minimum supported (able to parsed) by a device claiming support for that particular object and variation.

B.3.7 An '**M**' prefix before any Object and Variation ID in B.2 shall indicate that its support is mandatory and shall be implemented by any device claiming DNP3 compliance with this standard.

B.4 Compliance table

Table B.2: DNP3 approved objects

Object and variation ID	Typical device function	Object				Description	Request (device to parse)		Equivalent subset compliance level
		Group	Variation	Type	Flag incl.		FC (decimal)	QC (hex.)	
1	Binary input, functional status information	1	1	S		Binary Input	1	00,01,06	3
2		1	2	S	x	Binary Input	1	00,01,06	3
3	Binary input events, alarms, sequence of events (with time).	2	1	E	x	Binary Input Event without time	1	06	2
4		2	2	E	x	Binary Input Event with absolute time	1	06	2
5	Binary input with Double-bit representation.	3	1	S		Double-bit Binary Input	1	00,01,06	4
6		3	2	S	x	Double-bit Binary Input	1	00,01,06	4
7	Double-bit binary input events, alarms, sequence of events (with time).	4	1	E	x	Double-bit Binary Input Event without time	1	06	4
8		4	2	E	x	Double-bit Binary Input Event with absolute time	1	06	4
10	Binary output	10	2	S	x	Binary Output status (for reporting only)	1	00,01,06	3
11	Binary outputs, typically used for control operations Supported codes are: 3 – Select, 4 – Operate, 5 – Direct Operate, 6 – Direct Operate without acknowledgement.	12	1	C		Binary Output – Control relay output block	3,4,5, 6	17,28	1
12	General-purpose counters that can be polled	20	1	S	x	32-bit Counter	1	00,01,06	3
13		20	2	S	x	16-bit Counter	1	00,01,06	3
14		20	5	S		32-bit Counter	1	00,01,06	3
15		20	6	S		16-bit Counter	1	00,01,06	3
16	Counters that can be frozen at an instance (during a Master's immediate request or at a certain defined time) and their frozen values read back afterwards	21	1	S	x	32-bit Frozen Counter	1	00,01,06	3
17		21	2	S	x	16-bit Frozen Counter	1	00,01,06	3
18		21	5	S	x	32-bit Frozen Counter with time	1	00,01,06	4
19		21	6	S	x	16-bit Frozen Counter with time	1	00,01,06	4
20		22	1	E	x	32-bit Counter	1	06	3
21		22	2	E	x	16-bit Counter	1	06	3

22	Counter events, reporting of change of counter	22	5	E	x	32-bit Counter with time	1	06	3
23		22	6	E	x	16-bit Counter with time	1	06	3
24	Analogue input, polled	30	1	S	x	32-bit Analogue	1	00,01,06	3
25		30	2	S	x	16-bit Analogue	1	00,01,06	3
26		30	3	S		32-bit Analogue	1	00,01,06	3
27		30	4	S		16-bit Analogue	1	00,01,06	3
28	Analogue input, event based	32	1	E	x	32-bit Analogue without time	1	06	3
29		32	2	E	x	16-bit Analogue without time	1	06	3
30		32	3	E	x	32-bit Analogue with time	1	06	4
31		32	4	E	x	16-bit Analogue with time	1	06	4
M32	Time synchronization from a master utilizing a fine time delay measure to compensate for communication time propagation	50	1	I		Date and Time	1	07 (Qty=1)	3
M33		52	2	I		Fine Time Delay			1
34	Grouping of static and event data into classes, thereby enabling grouped polls and events to occur	60	1	I		Class 0 data objects	1	06	1
35		60	2	I		Class 1 data objects	1 20,21	06 06	1 3
36		60	3	I		Class 2 data objects	1 20,21	06 06	1 3
37		60	4	I		Class 3 data objects	1 20,21	06 06	1 3
M38	Internal Indication – Support shall be mandatory	80	1	S		Internal Indication	1 2	00,01 00(Ind=7)	3 1