

 Eskom	Standard	Technology
--	-----------------	-------------------

Title: **DNP3 IMPLEMENTATION
STANDARD**

Unique Identifier: **240-59089329**

Alternative Reference Number: **<n/a>**

Area of Applicability: **Engineering**

Documentation Type: **Standard**

Revision: **2**

Total Pages: **56**

Next Review Date: **May 2024**

Disclosure Classification: **Controlled
Disclosure**

Compiled by



Simphiwe Mbanga
SI Telecontrol Senior
Engineer SI Telecontrol

Date: 11/04/2019

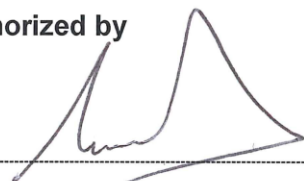
Approved by



Steven Papadopoulos
Control and Automation
Manager

Date: 20/5/2019

Authorized by



Richard McCurrach
PTM&C Senior Manager

Date: 20/5/2019

Supported by SCOT/SC



Marlini Sukhnandan
Telecontrol SC Chairperson

Date: 17/05/2019

Content

	Page
1. Introduction	4
2. Supporting clauses	4
2.1 Scope	4
2.1.1 Purpose	4
2.1.2 Applicability	4
2.2 Normative/informative references	4
2.2.1 Normative	4
2.2.2 Informative	4
2.3 Definitions	5
2.3.1 General	5
2.3.2 Disclosure classification	5
2.4 Abbreviations	5
2.5 Roles and responsibilities	6
2.6 Process for monitoring	6
2.7 Related/supporting documents	6
3. DNP3 implementation requirements	6
3.1 Background	6
3.2 Binary Outputs	6
3.3 Binary inputs	7
3.4 Analogue Outputs	8
3.5 Analogue Inputs	8
3.6 Counters	9
3.7 Assign class function	10
3.8 Unsolicited retry messages	10
3.9 Time synchronization	10
3.10 XML file support (level 4)	11
3.11 Secure authentication	11
3.12 DNP/IP implementation requirements	12
3.12.1 DNP/IP Structure	12
3.12.2 Advantages of the IP Suite	13
3.12.3 Comparison of the Master and Slave configuration Requirements	13
3.12.5 Use of Intrusion Detection Systems (IDS)	14
3.12.6 Use of Autonomic Network Detection System	14
3.13 Eskom minimum DNP3 device profile requirements	15
3.14 Capabilities and current settings for database (outstation only)	17
3.15 Binary outputs	20
4. Authorization	25
5. Revisions	25
6. Development team	26
7. Acknowledgements	26
Annex A – Impact assessment	27
Annex B – Device implementation tables for levels 1 to 4	30

Figures

Figure 1: ISO Structure of DNP/IP13

Tables

Table 1: Master VS SLAVE DNP/IP configuration requirements13
Table 2: Anomaly vs detection14

1. Introduction

This document is necessary to define the various needs of the different levels of DNP3 implementation that are used in the Eskom business. This document set out the standards of DNP implementation. It endeavours to eliminate misinterpretation of DNP user group standards of implementation. With the advent of IP and rollout of fibre the need for migration to DNP/IP has been established. The document will state the conditions required to meet the strategic move.

2. Supporting clauses

2.1 Scope

The standard covers the DNP3 functionality that is required to be implemented from the small Remote Terminal Units (RTUs) (Fault Path Indicators (FPIs)), Auto Reclosers and substations bay processors to gateway level. The document is structured such that it starts with the minimum requirements and builds up to the full set of requirements for the gateway. The levels required for lower levels are automatically required to be met at higher levels, unless otherwise stated.

2.1.1 Purpose

The purpose of the document is to ensure that the suppliers are aware of the expectations that Eskom has regarding DNP3 implementation. It is also to enable the business to have a point of reference when evaluating DNP3 Protocol on equipment supplied to Eskom.

2.1.2 Applicability

This document shall apply throughout Eskom Holdings Limited Divisions.

2.2 Normative/informative references

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

2.2.1 Normative

- [1] ISO 9001, Quality Management Systems.
- [2] IEEE 1815-2012, IEEE Standard for Electric Power Communications – Distributed Network Protocol
- [3] (DNP3)
- [4] DNP3 IED Certification Procedure Subset Level 2 Rev 2.5
- [5] IEC 62351-2, Description: Data Communication Security – Part 2: Glossary
- [6] 240-61224078, Telecontrol DNP3 parameter setting guide
- [7] 240-71086056, Telecontrol DNP3 class allocation standard:
- [8] 240-55410927: Cyber Security Standard for Operational Technology.
- [9] 240-102343347, DNP IP SCADA Standard

2.2.2 Informative

- [10] Bai, J. et Al., 2014: A Network Protection Framework for DNP3 over TCP/IP Protocol. IEEE Journal: 1-27.
- [11] Mander, T. et Al., 2007: Data Object Based Security for DNP3 Over TCP/IP for Increased Utility Commercial Aspects Security. IEEE Journal

- [12] Ortega, A. et AL., 2016: Simulation of the DNP3 Protocol Over TCP/IP on a Network IEEE 802.11g Ad-hoc With Smart Meter

2.3 Definitions

2.3.1 General

Definition	Description
Data Communication Equipment (DCE)	Devices that provide the functions required to establish, maintain and terminate a data transmission connection (radio, modem, etc.).
Data Terminal Equipment (DTE)	Devices acting as a data source, or data sink, or both.
Identical Unsolicited DNP3 Retry	An identical retry of an unsolicited response is a repeat, octet-for-octet of the previously transmitted unsolicited response. The IIN octets shall be the same. The sequence number appearing in the application control octet of an identical retry and the previous unsolicited messages are the same. (2)
Regenerated Unsolicited DNP3 Retry	The octets of a regenerated retry unsolicited response may contain some or all of the data from the previous unsolicited response, and may also include updated data, new data and changed IIN octets. The sequence number in the application control octet is incremented from the previously transmitted unsolicited response. Regeneration is permitted when the outstation does not receive confirmation to an unsolicited response. (2)
Supervisory	Remote control and indications of a DNP3 device by means of a Remote Terminal Unit (RTU) and a telecommunications link.

2.3.2 Disclosure classification

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

2.4 Abbreviations

Abbreviation	Description
AC	Alternating Current
CAP	Committee for Accepted Products
CROB	Control Relay Output Block
DC	Direct Current
DCE	Data Communication Equipment
DTE	Data Terminal Equipment
FPI	Fault Path Indicator
HTML	Hypertext Markup Language
IED	Intelligent Electronic Device
IP	Internet Protocol
IPSec	Internet Protocol Security
ISO	International Standards Organisation
LAN	Local Area Network

Abbreviation	Description
LAP	List of Accepted Products
n/a	not applicable
PTM&C	Protection, Telecoms, Metering and Control
RTU	Remote Terminal Unit
SC	Study Committee
SCADA	Supervisory Control And Data Acquisition
SI	Standards Implementation
SOE	Sequence of Events
TLS	Transport Layer Security
VPN	Virtual Private Network
XML	eXtensible Markup Language
XSLT	Extensible Stylesheet Language Transformations

2.5 Roles and responsibilities

Engineering to ensure that the equipment purchased meets the document requirements.

2.6 Process for monitoring

This standard shall be reviewed every 5 years or earlier, where changes will affect the contents.

2.7 Related/supporting documents

3. DNP3 implementation requirements

3.1 Background

Due to the large scope of the protocol implementation and the availability of documentation that clearly states the different levels of implementation, this document will only highlight the requirements that have been observed to be the minimum requirements to be met for our equipment. This does not in any way exempt the suppliers from meeting some of the requirements that are part of the level specified in the specification for the type of RTU.

When DNP 3 was developed in the early 1990s, there were minimal requirements that had to be met. Since then, the protocol has evolved from level 1 to level 4, with most of the additions being in line with the technological developments that have taken place over the years. Some of the main contributors to this evolution are the high developmental curve in the speed of microprocessors, readily availability of memory and the improvement in communication systems to provide more bandwidth.

With all the issues mentioned above, the key function in DNP 3 is the Interoperability.

3.2 Binary Outputs

3.2.1 Eskom's preferred implementation is in line with the DNP3 User Group Technical Bulletin TB2000-006, as well as with most RTU/Intelligent Electronic Device (IED) Suppliers' implementations. The purpose of this document is to avoid confusion of Control Relay Output Block (CROB) implementations by equipment manufacturers. Technical Bulletin TB2000-006 states: 'More than one of these codes may be accepted on a given index. However, each of the permitted codes shall perform the same function on that index.'

ESKOM COPYRIGHT PROTECTED

3.2.2 Each individual IED Control index should support at least the Preferred Command pair:

Required action	Preferred DNP command	Alternative DNP command	Index No.
Control to specific circuit-breaker to Index X			
Close (Breaker)	Pulse On/Close (0x41)	Latch On/Null (0x03)	X
Trip (Breaker)	Pulse On/Trip (0x81)	Latch Off/Null (0x04)	X
Control to specific transformer tap to Index Y			
Raise (Tfr Tap)	Pulse On/Close (0x41)	Latch On/Null (0x03)	Y
Lower (Tfr Tap)	Pulse On/Trip (0x81)	Latch Off/Null (0x04)	Y
Control to specific ARC/SEF to Index Z			
On (ARC/SEF)	Pulse On/Close (0x41)	Latch On/Null (0x03)	Z
Off (ARC/SEF)	Pulse On/Trip (0x81)	Latch Off/Null (0x04)	Z

3.2.3 Both Pulse and Latch commands may be accepted on any given index. The same functions shall be performed by either control type on that given index.

3.2.4 For any single function indices, the outstation shall accept at least one of the preferred Commands, i.e. Pulse On/Trip or Pulse On/Close. The commands will primarily make use of Function Code 5 (Direct Operate).

3.2.5 As an alternative, Function Codes 3 and 4 (Select before Operate) should also be supported to all indices, with the same function performed as with Function Code 5.

3.2.6 When using select before operate for the control, there shall be a select before operate timeout parameter that is configurable.

3.2.7 If the operate is sent after the timeout has elapsed, the operation shall not be processed.

3.2.8 Pulse On (Trip) and Latch OFF should perform the same function, i.e. in the case of a breaker operation, they should result in a trip action. The same applies to Pulse On (Close) and Latch ON, regarding performing the breaker close operation.

3.2.9 It shall be possible to report the status of the control relay output block, and this functionality shall be configurable to on/off.

3.2.10 In cases where the unit has master functionality, such as the gateway, it shall be configurable to issue both the select before operate and the direct operate commands.

3.2.11 The unit shall also have a configurable pulse width from the 100 ms with steps and the maximum being specified by the supplier.

3.2.12 The unit shall also be able to support the full complement of the control variations provided, either by passing the control message from the Supervisory Control And Data Acquisition (SCADA) master, or/and by independent configuration on the gateway

3.3 Binary inputs

3.3.1 Binary inputs are responsible for the transmission of status indication, alarms and events that occur at the point that is being monitored.

3.3.2 The alarms are not time-stamped; they indicate the change that has taken place on a monitored point such as DC or AC charger failure.

3.3.3 The events, which are stored as Sequence of Events (SOEs), carry critical data that is linked to breaker or switch operations such as breaker Trip/Close, and these are time-stamped as they assist in the second line fault analysis that is conducted by protection engineers. This fault analysis is done to link the events that took place, and also to compare the data with the relay data that is normally archived on site.

3.3.4 As mentioned above, the digitals are status indications that are returned during an integrity poll, and events that are returned during a Class 1,2,3 data poll or as unsolicited messages in report by exception configurations.

3.3.5 For binary input status, the unit shall be able to parse messages from the Master requesting Class 0,1,2,3 messages (normally referred to as the integrity Poll) Group 60 v2,v3,v4 &v1 with qualifier 6 and respond with either Object 1 variation 1 (Single bit) or Object 1 variation 2 (Single bit with status) and Object 2 variation 2. The variation 2 carries the 8-bit status flag octet:

BSTR8: Flag Octet

- Bit 0: ONLINE
- Bit 1: RESTART
- Bit 2: COMM_LOST
- Bit 3: REMOTE_FORCED
- Bit 4: LOCAL_FORCED
- Bit 5: CHATTER_FILTER
- Bit 6: Reserved, always 0
- Bit 7: STATE - has a value of 0 or 1, representing the state of the physical or logical input.

3.3.6 With Eskom's standardization on the use of double bit indications for monitoring of the breaker and isolator status, the units shall also support the newly introduced Object 3 with the same variations as Object 1.

3.3.7 It shall be possible to set the double bit as either a pair of single bits using Object 1, or to be reported as Object 3. Object 3 and Object 4 functionality are DNP 3 Level 4 requirements.

3.4 Analogue Outputs

3.4.1 For setpoint values there must be support for analogue outputs Object 41 variation 2 for 16 bit values. All other supported objects and variations relating to analogue outputs shall be clearly stated.

3.4.2 Analogue outputs are used to set protection groups, speed control, temperature control values etc.

3.5 Analogue Inputs

3.5.1 Analogue data is used to indicate the mainly the values of the Voltage (kV), current (A), Power (kW, kVar and MVA). There are some new applications where room temperature, transformer temperature, oil dam level, etc. analogues are also being sent back to SCADA.

3.5.2 The operation of analogues is centred on the issue of accuracy and resolution:

- a) Accuracy is linked to the reliability of the measurement that is being measured, i.e. the consistency in measuring the same value all the time when it remains the same. This is linked to the stability of the transducer drifting due to temperature, or any other factors that can affect the measurement and can result in inaccuracies of the measurement.
- b) Resolution is a function of how finely we can measure an entity value. This originates from the transducer as well, but can be further influenced by the dead-band value that is set for the point. The settings for dead-band values are not an exact science, as the loading and the fluctuations of the analogues differ from feeder to feeder, depending on the nature of the load. There is also another parameter that has been made available for settings for a hysteresis effect where the Low and High alarms are set.

3.5.3 The dead-band value is a parameter that stipulates that the analogue transgression has been more than the value set. The dead-band shall always be a reference of the last reported value, irrespective of whether the value was reported as an event or as a response to and integrity poll. There are a few variants on the operation of the dead-band, the main difference being whether it is on absolute change or integrated:

- a) For absolute changes, the change is compared to the last reported point, e.g. if the dead-band is X and the last reported value is 100, then the next change will be a transgression of either $100 \pm X$. There are implementations where the reporting is done at exactly $100 \pm X$ and others where the next reported value is an integer greater than the set dead-band. Clarity is required on the exact operation, either $>$ or $\geq$ as the trigger.
- b) The integrated approach is based on the accumulated change being equal to X after the last value either $>$ or $<$ the last reported value. With integrated set-up, there is a possibility of having the same last reported value being reported, e.g. if the dead-band is set as 10, say the last value that is reported is 100, if there is a change from 100 to 105, 105 will not be reported; If the value changes back to 100, then accumulatively there has been a change of 10, resulting in 100 being reported again. Suppliers shall clearly state the expected operation on the reporting of analogues when the dead-band value is set to 0 if it is possible to set it to 0.

3.5.4 For analogues, it is required that the suppliers have configurability for the following parameters:

- a) Individual dead-band per point.
- b) Individual hysteresis per point.
- c) Individual configuration of absolute or integrated.
- d) Cyclic reporting of analogues that has a time interval with possibility to switch off and on.
- e) Analogues shall be selected to be configured as 16- or 32-bit.
- f) Analogues shall be selectable to be sent with/without flags and with/without time.

3.5.5 For analogue input status, the unit shall be able to parse messages from the Master requesting Class 0,1,2,3 messages Group 60 v2,v3,v4 & v1 with qualifier 6 and respond with either Object 32 variation 2 (16-bit analogue input without time) or Object 30 variation 2 (16-bit analogue input with flag) or the floating points Object 32 variation 7 (Analog Input – Single-precision floating-point without time) or Object 30 variation 4 (Analog Input – Single-precision floating-point with flag). The floating points shall clearly denote the notation used in terms of decimal points available. As a minimum FLT32 format shall be met. The variation 2 carries the 8-bit flag octet:

BSTR8: Flag Octet

- Bit 0: ONLINE
- Bit 1: RESTART
- Bit 2: COMM_LOST
- Bit 3: REMOTE_FORCED
- Bit 4: LOCAL_FORCED
- Bit 5: OVER_RANGE
- Bit 6: REFERENCE_ERR

3.5.6 Bit 7: STATE – Reserved, always 0.

3.6 Counters

With the advent of IPP and other business interface equipment the suppliers need to have support for counters. Both normal and frozen counters need to be supported in 16 bit format. It shall also be possible for the device to parse the reset counters message from the master.

ESKOM COPYRIGHT PROTECTED

3.7 Assign class function

- 3.7.1 Outstation devices that are able to store the most recent class assignments from a master in non-volatile memory may use those assignments after a device restart; otherwise, devices shall revert to their default class assignments.
- 3.7.2 Assign class is function code 22 and all devices shall be able to parse assign class messages from the master station.
- 3.7.3 Assign class shall be supported for Class 0,1,2,3 for both the digitals and the analogues.
- 3.7.4 The unit shall support the different variations, assignment of a single point, assignment of a group of points that are sequential and assignment of a group of points that are at different positions on the database.
- 3.7.5 For all the points that have been assigned as Class 0 via the protocol, only the current status shall be reported upon integrity data polls (Class 0 Poll) from the Master, and no events shall be generated for those points.
- 3.7.6 For points that have been assigned to Class 1, 2 or 3, it is expected that they will conform to the globally set parameters for that class regarding the number of messages to be generated and the time delay before the message is sent to SCADA as per (6).
- 3.7.7 Suppliers shall clearly state the implementation regarding what happens to the settings that are set via the protocol on start-up of the unit.

3.8 Unsolicited retry messages

- 3.8.1 There are two variations available in DNP3 regarding the retry messages: identical unsolicited retry and regenerated retry.
- 3.8.2 These variations should be available for configuration by the user and the reporting shall be as per the following description.
 - a) Identical unsolicited DNP3 retry: An identical retry of an unsolicited response is a repeat, octet-for-octet of the previously transmitted unsolicited response. The IIN octets shall be the same. The sequence number appearing in the application control octet of an identical retry and the previous unsolicited messages are the same.
 - b) Regenerated unsolicited DNP3 retry: The octets of a regenerated retry unsolicited response may contain some or all of the data from the previous unsolicited response, and may also include updated data, new data and changed IIN octets. The sequence number in the application control octet is incremented from the previously transmitted unsolicited response. Regeneration is permitted when the outstation does not receive confirmation to an unsolicited response.
- 3.8.3 There should be a configurable number of retry messages, after which a longer back-off regenerated timeout can be used. It would be preferable to have the back-off regenerated parameter configurable in terms of time and as soon as a new event happens.

3.9 Time synchronization

- 3.9.1 The units that are used in substations are used together with protection equipment that also has time-stamped events.
- 3.9.2 When there is a fault at a substation, the RTU events are compared with the protection relay events and it is very critical that the time that is reported with the events is as accurate as possible.
- 3.9.3 The RTU shall have a parameter that is configurable with the period, after which it will send an IIN4 [need time] if it has not received time from SCADA for the configured period.
- 3.9.4 The master clears this bit by issuing a write request to Object Group 50v1, which shall be parsed by the unit by resetting the IIN4 bit.

- 3.9.5** The unit shall not generate the need time message on its own; it shall only be part of a response message or an unsolicited message that occurs after the period has elapsed.
- 3.9.6** The outstation may not clear the bit until the master issues a time synchronization message, write date and time to the RTU.
- 3.9.7** The unit shall be able to parse the following time setting messages from SCADA:
- a) Delay measurement: Function code 23. Delay Measurement Function Code: The Outstation shall report the time it takes to process and initiate the transmission of its response. This allows the master to compute the propagation delay in the communications channel. Used for non-Local Area Network (LAN) time synchronization. The unit shall return a Fine Time Delay DNP3 object, Object Group 52v2.
 - b) Record_current_time: Function code 24. Record Current Time Function Code: The Outstation shall save the time when the last octet of this message is received. Used for LAN time synchronization.

3.10 XML file support (level 4)

- 3.10.1** The eXtensible Markup Language (XML) specification defines a language that can be used to transfer information electronically in a platform and application independent fashion.
- 3.10.2** XML defines the syntax for the language, but not a valid vocabulary for a specific application. The XML Schema specification provides a mechanism for describing a vocabulary to be used in a specific application.
- 3.10.3** The DNP Users Group provides an XSLT template that can be used to translate a DNP3 Device Profile XML instance file to an HTML file with contents formatted similar to the device profile document.
- 3.10.4** The techniques and information required to generate an XML document that describes the capabilities and current/default configuration of an Outstation shall be clearly stated.
- 3.10.5** The XML and XML Schemas provide a widely used, robust and powerful mechanism for exchanging information between applications.
- 3.10.6** XML and XML Schema support is available on most platforms and in most development/runtime environments.
- 3.10.7** The XML files can be read or written to the units. The tag named standard is used via the file transfer capabilities of DNP3. To read the file enables the user to view the complete set of DNP 3 parameters that are on the unit. When writing to the unit, settings that are on the unit are altered to the new desired settings.
- 3.10.8** Suppliers are required to demonstrate how they have implemented the XML and the XML Schema functionality as the specification for Level 4 devices.

3.11 Secure authentication

- 3.11.1** Authentication messages are formatted as additional DNP3 function codes and object variations within the application layer. The physical layer for transmission can either be serial or IP.
- 3.11.2** The purpose of the specification of secure authentication is to define a protocol mechanism that:
- a) A DNP3 outstation can use to unambiguously determine it is communicating with a user who is authorized to access the services of the outstation.
 - b) A DNP3 master can use to unambiguously determine that it is communicating with the correct outstation.

- 3.11.3** The secure authentication specification addresses only the following security threats, as defined in (4) Part 2: Spoofing; Modification; Replay; Eavesdropping - on exchanges of cryptographic keys only, not on other data; and Non-repudiation – to the extent of identifying individual users of the system (4). The authentication messages are formatted as additional DNP function codes and object variations.
- 3.11.4** According to (2), Implementers are requested to note that logging and auditing of security events such as authentication failures is a critical part of information security. It is recommended that all implementations at a minimum log all successful and unsuccessful authentications and key changes, including the time, the DNP addresses and the affected user.
- 3.11.5** Suppliers should clearly state and demonstrate how they have implemented the handling of the following Secure authentication functionality:
- a) Initiation and response to initiation messages.
 - b) Generation and exchange of keys.
 - c) Implementation of the aggressive mode.
 - d) Authentication failures.

3.12 DNP/IP implementation requirements

A communication network involving critical applications, as in the case of electric power transmission and distribution must be highly reliable, extremely safe and resilient to failures. This trend in utilizing the Internet brought in enhancements to the quality of services provided to the SCADA system. Nevertheless, it also introduced new vulnerabilities to the SCADA system [11]. SCADA protocols' payloads are coded at the application level, this differentiates them from other protocols. This makes legacy firewalls fail in detecting attacks targeting SCADA systems [9].

The main advantage of DNP/IP is the seamless integration of the SCADA LAN and WAN. There is leverage on existing equipment and standards. The internet protocol suite is platform independent. [2] Cybersecurity is critical in the rollout of DNP/IP. The cyber-security is used to detect and block data transmissions that do not conform to the allowed DNP3 function code and object header usage for a device on a connection basis with multiple masters or outstations [10]. The cyber-security therefore must ensure that only valid function codes are used with a device. Currently, DNP3 security requires the use of the Transport Layer Security (TLS) or Internet Protocol Security (IPsec) when used over TCP/IP, which may also be in addition to commercial firewall appliances. The TLS, IPsec, and commercial firewalls provide security for DNP3 over TCP/IP, such as confidentiality and authentication, but since they are designed for general commercial application they do not provide security designed specifically for DNP3, limiting their effectiveness for DNP3 [10] & [9].

A commercial-off-the shelf firewall appliance would not be capable of examining a received data-link link frame to detect and prevent an outstation from receiving a stop application command. In addition, TLS authentication would not be capable of preventing an outstation from receiving illegitimate control commands from a compromised master since the data would have been properly authenticated by the master. VPN and Secure Internet Protocols (IPSec) are recommended to provide site-to-site security, in accordance with the company policies.

3.12.1 DNP/IP Structure

This section will look at the required ISO layers for compliance with DNP/IP. DNP/IP is not the same as DNP over IP as there is differentiation in the ISO layers for the two setups [8]. For DNP over IP a complete DNP message is transported over an IP network through a serial to IP server, whereas for DNP/IP the IP layers and Ethernet communication requirements are embedded on the message structure. Figure 1: ISO Structure of DNP/IP below shows the structure of DNP/IP.

DNP Application Layer
DNP Transport Layer
DNP Data Link layer
Connection Management
TCP/UDP Transport layer
Network layer, IPV4,ICMP
Physical layer – Device driver

Figure 1: ISO Structure of DNP/IP

3.12.2 Advantages of the IP Suite

3.12.2.1 It leverages on existing equipment and standards (The protocol stack is the same as the serial)

3.12.2.2 The internet Protocol stack is platform independent

3.12.2.3 There is seamless integration of the SCADA LAN to the WAN

3.12.3 Comparison of the Master and Slave configuration Requirements

To resolve a case of simultaneous initiation of connections by both the master and slave, the master's connection takes precedence.

Table 1: Master VS SLAVE DNP/IP configuration requirements

Master	Outstation/Slave
Support for multiple end points to support multiple outstations	Support for multiple endpoints to support multiple masters
Port number 20000 support	Port number 20000 support
TCP is recommended – Due to TCP being connection oriented it provides seamless integration with serial	TCP recommended
IP Address must be supported	IP Address must be supported
The following end point setups need to be supported: TCP initiating end Point Datagram end Point TCP Dual end point	The following end point setups need to be supported: TCP listening end Point Datagram end Point TCP Dual end point

On top of the basic configuration requirements, some rudimentary security features for IP apply to both the slave and the Master and they depend on the following:

- IP Address
- IP Range
- Validation features provided by higher level application security layers.

3.12.4 The future of DNP/IP Security

3.12.5 Use of Intrusion Detection Systems (IDS)

There are mainly two types of intrusion based systems that are currently used, Knowledge-based and Behaviour-based Intrusion detection systems [9].

3.12.5.1 Knowledge-based Intrusion detection system

Knowledge-based Intrusion Detection searches for runtime features that match a unique pattern to identify an intrusion. Knowledge-based Intrusion Detection suffers from the lack of capabilities to detect novel or modified attacks; nevertheless, it is very efficient in detecting previously seen attacks with known signatures.

3.12.5.2 Behaviour-based Intrusion detection

Behaviour-based Intrusion Detection matches runtime features to previous knowledge of the normal values of those features, if it detects a deviation, then it consider that to be anomalous, which is an indication of an intrusion. Most Behaviour-based Intrusion Detection suffers from high false positive rate due to the incomplete knowledge of the normal operations region of the monitored environment. However, Behaviour-based detection is able to detect novel never seen attacks as well as morphed versions of previously seen attacks.

3.12.6 Use of Autonomic Network Detection System

The autonomic Network detection system is based on the concept of monitoring and control. This framework not only detects headers of TCP and IP layers, but also analyses and parses the DNP3 payloads. Anomaly detection techniques are widely used in various domains of science. In network area, the terminology anomaly detection usually refers to figuring out the unexpected behaviour patterns that tamper the normal behaviours in network traffic [9]. Table 4-2 shows the detection features for various types of anomalies encountered. This is a branch of machine learning, based on unsupervised learning theory.

Table 2: Anomaly vs detection

Anomaly	Feature detection
Length field Attack	Follow any rule in the rule set that deletes the conditions of length field in the initial normal rule set.
Control field of Data Link Layer Attack	Follow any rule in the rule set that deletes the conditions of control field in Data Link Layer in the initial normal rule set.
Destination Address field Attack	Follow any rule in the rule set that deletes the conditions of Destination Address field in the initial normal rule set.
FIR and FIN Attack	Follow any rule in the rule set that deletes the conditions of FIR and FIN in the initial normal rule set.
Control Function field of Application Layer Attack	Follow any rule in the rule set that deletes the conditions of Control Function field in Application Lay in the initial normal rule set.
Flooding reset Attack	The reset packets rate

3.13 Eskom minimum DNP3 device profile requirements

Eskom's minimum DNP3 device profile requirements are given in the following tables:

Link layer	Capabilities
Data Link Address: Indicates if the link address is configurable over the entire valid range of 0 to 65,519. Data link addresses 0xFFFF0 through 0xFFFFF are reserved for broadcast or other special purposes.	☐ Fixed at _____ X Configurable, range __0__ to __65519__ ☐ Configurable, selectable from ____, ____, ____ ☐ Configurable, other, describe _____
DNP3 Source Address Validation: Indicates whether the device will filter out messages not from a specific source address.	☐ Never X Always, one address allowed (shown in 1.4.3) ☐ Always, any one of multiple addresses allowed (each selectable as shown in 1.4.3) ☐ Sometimes, explain _____
Sends Confirmed User Data Frames: A list of conditions under which the device transmits confirmed link layer services (TEST_LINK_STATES, RESET_LINK_STATES, CONFIRMED_USER_DATA).	☐ Always X Sometimes, explain _____ ☐ Never
Data Link Layer Confirmation Timeout: This timeout applies to any secondary data link message that requires a confirm or response (link reset, link status, user data, etc.).	☐ None ☐ Fixed at _____ ms X Configurable, range __0__ to __60000__ ms ☐ Configurable, selectable from ____, ____, ____ ms ☐ Configurable, other, describe _____ ☐ Variable, explain _____
Maximum Data Link Retries: The number of times the device will retransmit a frame that requests Link Layer confirmation.	☐ Never Retries ☐ Fixed at _____ X Configurable, range __0__ to __255__ ☐ Configurable, selectable from ____, ____, ____ ☐ Configurable, other, describe _____
Maximum number of octets Transmitted in a Data Link Frame: This number includes the CRCs. With a length field of 255, the maximum size would be 292.	☐ Fixed at __292__ ☐ Configurable, range _____ to _____ ☐ Configurable, selectable from ____, ____, ____ ☐ Configurable, other, describe _____
Maximum number of octets that can be Received in a Data Link Frame: This number includes the CRCs. With a length field of 255, the maximum size would be 292. The device shall be able to receive 292 octets to be compliant.	☐ Fixed at __292__ ☐ Configurable, range _____ to _____ ☐ Configurable, selectable from ____, ____, ____ ☐ Configurable, other, describe _____
Application layer	Capabilities

Link layer	Capabilities
Maximum number of octets that can be Received in an Application Layer Fragment: This size does not include any transport or frame octets. Masters shall provide a setting greater than or equal to 2048. Outstations shall provide a setting greater than or equal to 249.	☐ Fixed at _____ ☐ Configurable, range _____ to _____ ☐ Configurable, selectable from ____, ____, ____ X Configurable, other, describe __greater than 249
Timeout waiting for Complete Application Layer Fragment: Timeout if all frames of a message fragment are not received in the specified time. Measured from time first frame of a fragment is received until the last frame is received.	☐ None ☐ Fixed at _____ ms ☐ Configurable, range 1000 to 255000 ms ☐ Configurable, selectable from ____, ____, ____ ms ☐ Configurable, other, describe _____ ☐ Variable, explain _____
Maximum number of objects allowed in a single control request for CROB (group 12):	X Fixed at _1____(enter 0 if controls are not supported) ☐ Configurable, range _____ to _____ ☐ Configurable, selectable from ____, ____, ____ ☐ Configurable, other, describe _____ ☐ Variable, explain _____
Fill out the following items for masters only	Capabilities
Timeout waiting for Complete Application Layer Response(ms): Timeout on Master if all fragments of a response message are not received in the specified time.	☐ None ☐ Fixed at _____ ms X Configurable, range _5000_____ to _60000_____ms ☐ Configurable, selectable from ____, ____, ____ ms ☐ Configurable, other, describe _____ ☐ Variable, explain _____
Maximum Application Layer Retries for Request Messages: The number of times a Master will retransmit an application layer request message if a response is not received. This parameter shall never cause a Master to retransmit control or time sync messages. Outstations should never transmit retries.	☐ None (required) ☐ Fixed at _____ X Configurable, range _0_____ to _255_____ ☐ Configurable, selectable from ____, ____, ____ ☐ Configurable, other, describe _____ ☐ Variable, explain _____
Outstation unsolicited response support	Capabilities

Link layer	Capabilities
Supports Unsolicited Reporting: When the unsolicited response mode is configured 'off', the device is to behave exactly like an equivalent device that has no support for unsolicited responses. If set to On, the Outstation will send a null Unsolicited Response after it restarts, then wait for an Enable Unsolicited Response command from the master before sending additional Unsolicited Responses containing event data.	☐ Not Supported X Configurable, selectable from On and Off
Master Data Link Address: The destination address of the master device where the unsolicited responses will be sent.	☐ Fixed at _____ X Configurable, range __0__ to __65535__ ☐ Configurable, selectable from ____, ____, ____ ☐ Configurable, other, describe _____
Unsolicited Response Confirmation Timeout: This is the amount of time that the outstation will wait for an Application Layer confirmation back from the master indicating that the master received the unsolicited response message. As a minimum, the range of configurable values shall include times from one second to one minute. This parameter may be the same one that is used for normal, solicited, application confirmation timeouts, or it may be a separate parameter.	☐ Fixed at _____ ms ☐ Configurable, range __5000__ to __60000__ ms ☐ Configurable, selectable from ____, ____, ____ ms ☐ Configurable, other, describe _____ ☐ Variable, explain _____

3.14 Capabilities and current settings for database (outstation only)

The following tables identify the capabilities and current settings for each DNP3 data type. Each data type also provides a table defining the data points available in the device or a description of how this information can be obtained if the database is configurable. Tables for data types not supported may be deleted. Additional columns may be added to the point list table if necessary

Single-bit binary inputs Static (steady-state) Group Number: 1 Event Group Number: 2	Capabilities
Static Variation reported when variation 0 requested:	☐ Variation 1 – Single-bit Packed format x Variation 2 – Single-bit with flag ☐ Based on point Index (add column to table below)
Event Variation reported when variation 0 requested:	☐ Variation 1 – without time x Variation 2 – with absolute time ☐ Variation 3 – with relative time ☐ Based on point Index (add column to table below)
Event reporting mode: When responding with event data and more than one event has occurred for a data point, an Outstation may include all events or only the most recent event. All events are typically reported for Binary Inputs.	☐ Only most recent x All events

Single-bit binary inputs Static (steady-state) Group Number: 1 Event Group Number: 2	Capabilities
Binary Inputs included in Class 0 response: If Binary Inputs are not included in the Class 0 response, Binary Input Events (group 2) may not be reported.	☒ Always ☐ Never ☐ Only if point is assigned to Class 1, 2, or 3 ☐ Based on point Index (add column to table below)
Definition of Binary Input Point List: List all addressable points. Points that do not exist (for example, because an option is not installed) shall be omitted from the table.	☐ Fixed, list shown in table below ☐ Configurable (current list may be shown in table below) ☐ Other, explain _____

Point index	Name	Default class assigned to events (1, 2, 3 or none)	Name for state when value is 0 (intermediate)	Name for state when value is 1 (Off)	Name for state when value is 2 (On)	Name for State when value is 3 (indeterminate)	Description
0							
1							
2							
:	Add more rows as necessary						

Double-bit input points Static (steady-state) Group Number: 3 Event Group Number: 4	Capabilities
Static Variation reported when variation 0 requested:	☐ Variation 1 – Double-bit Packed format ☒ Variation 2 – Double-bit with flag ☐ Based on point Index (add column to table below)
Event Variation reported when variation 0 requested:	☐ Variation 1 – without time ☒ Variation 2 – with absolute time ☐ Variation 3 – with relative time ☐ Based on point Index (add column to table below)
Event reporting mode: When responding with event data and more than one event has occurred for a data point, an Outstation may include all events or only the most recent event. All events are typically reported for Double-bit Inputs.	☐ Only most recent ☒ All events

Double-bit input points Static (steady-state) Group Number: 3 Event Group Number: 4	Capabilities
Double-bit Inputs included in Class 0 response: If Double-bit Inputs are not included in the Class 0 response, Double-bit Input Events (group 4) may not be reported.	☒ Always ☐ Never ☐ Only if point is assigned to Class 1, 2, or 3 ☐ Based on point Index (add column to table below)
Definition of Double-bit Input Point List: List all addressable points. Points that do not exist (for example, because an option is not installed) shall be omitted from the table.	☐ Fixed, list shown in table below ☐ Configurable(current list may be shown in table below) ☐ Other, explain _____
Command Event reporting mode: When responding with event data and more than one event has occurred for a data point, an Outstation may include all events or only the most recent event.	☐ Only most recent ☒ All events
Maximum Time between Select and Operate:	☐ Not Applicable ☐ Fixed at _____ seconds ☐ Configurable, range _10_____ to _60000_____ ms (in 1 ms steps) ☐ _____ Configurable, _____ selectable from _____, _____, _____ seconds ☐ _____ Configurable, _____ other, describe _____ ☐ Variable, explain _____ ☐ Based on point Index (add column to table below)
Definition of Binary Output Status/Control relay output block (CROB) Point List: List all addressable points. Points that do not exist (for example, because an option is not installed) shall be omitted from the table.	☐ Fixed, list shown in table below ☐ Configurable(current list may be shown in table below) ☐ Other, explain _____

Point index	Name	Default class assigned to events (1, 2, 3 or none)	Name for state when value is 0 (intermediate)	Name for state when value is 1 (Off)	Name for state when value is 2 (On)	Name for state when value is 3 (indeterminate)	Description
0							
1							
2							

Point index	Name	Default class assigned to events (1, 2, 3 or none)	Name for state when value is 0 (inter-mediate)	Name for state when value is 1 (Off)	Name for state when value is 2 (On)	Name for state when value is 3 (indeterminate)	Description
...	Add more rows as necessary						

3.15 Binary outputs

Point index	Name	Supported control operations											Name for state when value is 0	Name for state when value is 1	Default Class Assigned to Events (1, 2, 3 or none)		Description
		Select/Operate	Direct Operate	Direct Operate – No Ack	Pulse On	Pulse Off	Latch On	Latch Off	Trip	Close	Count > 1	Cancel Currently Running Operation			Change	Command	
0																	
1																	
2																	
...	Add more rows as necessary																

Binary output status and control relay output block Binary Output Status Group Number: 10 Binary Output Event Group Number: 11 CROB Group Number: 12 Binary Output Command Event Object Num: 13	Capabilities
Minimum pulse time allowed with Trip, Close, and Pulse On commands:	x Fixed at <u> 10 </u> ms (hardware may limit this further) ☐ Based on point Index (add column to table below)
Maximum pulse time allowed with Trip, Close, and Pulse On commands:	x Fixed at <u> 65535 </u> ms (hardware may limit this further) ☐ Based on point Index (add column to table below)

Binary output status and control relay output block Binary Output Status Group Number: 10 Binary Output Event Group Number: 11 CROB Group Number: 12 Binary Output Command Event Object Num: 13	Capabilities
Binary Output Status included in Class 0 response: If Binary Output Status points are not included in the Class 0 response, Binary Output Status Events (group 11) may not be reported.	☐ Always ☐ Never ☐ Only if point is assigned to Class 1, 2, or 3 ☐ Based on point Index (add column to table below) X Configurable on the device to Never or Always
Reports Output Command Event Objects:	☐ Never ☐ Only upon a successful Control x Upon all control attempts
Event Variation reported when variation 0 requested:	☐ Variation 1 – without time x Variation 2 – with absolute time ☐ Based on point Index (add column to table below)
Command Event Variation reported when variation 0 requested:	☐ Variation 1 – without time x Variation 2 – with absolute time ☐ Based on point Index (add column to table below)
Event reporting mode: When responding with event data and more than one event has occurred for a data point, an Outstation may include all events or only the most recent event.	☐ Only most recent x All events

Counters/Frozen Counters Static Counter Group Number: 20 Static Frozen Counter Group Number: 21 Counter Event Group Number: 22 Frozen Counter Event Group Number: 23	Capabilities
Static Counter Variation reported when variation 0 requested:	x Variation 1 – 32-bit with flag ☐ Variation 2 – 16-bit with flag ☐ Variation 5 – 32-bit without flag ☐ Variation 6 – 16-bit without flag ☐ Based on point Index (add column to table below)
Counter Event Variation reported when variation 0 requested:	☐ Variation 1 – 32-bit with flag ☐ Variation 2 – 16-bit with flag x Variation 5 – 32-bit with flag and time ☐ Variation 6 – 16-bit with flag and time ☐ Based on point Index (add column to table below)

Counters/Frozen Counters Static Counter Group Number: 20 Static Frozen Counter Group Number: 21 Counter Event Group Number: 22 Frozen Counter Event Group Number: 23	Capabilities
Counters included in Class 0 response: If Counters are not included in the Class 0 response, Counter Events (group 22) may not be reported.	☒ Always ☐ Never ☐ Only if point is assigned to Class 1, 2, or 3 ☐ Based on point Index (add column to table below)
Counter Event reporting mode: When responding with event data and more than one event has occurred for a data point, an Outstation may include all events or only the most recent event. All events are typically reported for Counters.	☒ Only most recent ☐ All events
Static Frozen Counter Variation reported when variation 0 requested:	☐ Variation 1 – 32-bit with flag ☐ Variation 2 – 16-bit with flag ☒ Variation 5 – 32-bit with flag and time ☐ Variation 6 – 16-bit with flag and time ☐ Variation 9 – 32-bit without flag ☐ Variation 10 – 16-bit without flag ☐ Based on point Index (add column to table below)
Frozen Counter Event Variation reported when variation 0 requested:	☐ Variation 1 – 32-bit with flag ☐ Variation 2 – 16-bit with flag ☒ Variation 5 – 32-bit with flag and time ☐ Variation 6 – 16-bit with flag and time ☐ Based on point Index (add column to table below)
Frozen Counters included in Class 0 response: If Frozen Counters are not included in the Class 0 response, Frozen Counter Events (group 23) may not be reported.	☒ Always ☐ Never ☐ Only if point is assigned to Class 1, 2, or 3 ☐ Based on point Index (add column to table below)
Frozen Counter Event reporting mode: When responding with event data and more than one event has occurred for a data point, an Outstation may include all events or only the most recent event. All events are typically reported for Frozen Counters.	☐ Only most recent ☒ All events

Counters/Frozen Counters Static Counter Group Number: 20 Static Frozen Counter Group Number: 21 Counter Event Group Number: 22 Frozen Counter Event Group Number: 23	Capabilities
Counters Roll Over at:	☐ 16 Bits (65,535) ☒ 32 Bits (4,294,967,295) ☐ Other Fixed Value _____ ☐ Configurable; range _____ to _____ ☐ Configurable, selectable from ____, ____, ____ ☐ Configurable, other, describe _____ ☐ Based on point Index (add column to table below)
Counters frozen by means of:	☐ Master Request ☒ Freezes itself without concern for time of day ☐ Freezes itself and requires time of day ☐ Other, explain _____
Definition of Counter/Frozen Counter Point List: List all addressable points. Points that do not exist (for example, because an option is not installed) shall be omitted from the table.	☐ Fixed, list shown in table below ☐ Configurable (current list may be shown in table below) ☐ Other, explain _____
Static Counter Variation reported when variation 0 requested:	☒ Variation 1 – 32-bit with flag ☐ Variation 2 – 16-bit with flag ☐ Variation 5 – 32-bit without flag ☐ Variation 6 – 16-bit without flag ☐ Based on point Index (add column to table below)
Counter Event Variation reported when variation 0 requested:	☐ Variation 1 – 32-bit with flag ☐ Variation 2 – 16-bit with flag ☒ Variation 5 – 32-bit with flag and time ☐ Variation 6 – 16-bit with flag and time ☐ Based on point Index (add column to table below)
Counters included in Class 0 response: If Counters are not included in the Class 0 response, Counter Events (group 22) may not be reported.	☒ Always ☐ Never ☐ Only if point is assigned to Class 1, 2, or 3 ☐ Based on point Index (add column to table below)
Counter Event reporting mode: When responding with event data and more than one event has occurred for a data point, an Outstation may include all events or only the most recent event. All events are typically reported for Counters.	☒ Only most recent ☐ All events

Counters/Frozen Counters Static Counter Group Number: 20 Static Frozen Counter Group Number: 21 Counter Event Group Number: 22 Frozen Counter Event Group Number: 23	Capabilities
Static Frozen Counter Variation reported when variation 0 requested:	☐ Variation 1 – 32-bit with flag ☐ Variation 2 – 16-bit with flag ☒ Variation 5 – 32-bit with flag and time ☐ Variation 6 – 16-bit with flag and time ☐ Variation 9 – 32-bit without flag ☐ Variation 10 – 16-bit without flag ☐ Based on point Index (add column to table below)
Frozen Counter Event Variation reported when variation 0 requested:	☐ Variation 1 – 32-bit with flag ☐ Variation 2 – 16-bit with flag ☒ Variation 5 – 32-bit with flag and time ☐ Variation 6 – 16-bit with flag and time ☐ Based on point Index (add column to table below)
Frozen Counters included in Class 0 response: If Frozen Counters are not included in the Class 0 response, Frozen Counter Events (group 23) may not be reported.	☒ Always ☐ Never ☐ Only if point is assigned to Class 1, 2, or 3 ☐ Based on point Index (add column to table below)
Frozen Counter Event reporting mode: When responding with event data and more than one event has occurred for a data point, an Outstation may include all events or only the most recent event. All events are typically reported for Frozen Counters.	☐ Only most recent ☒ All events
Counters Roll Over at:	☐ 16 Bits (65,535) ☒ 32 Bits (4,294,967,295) ☐ Other Fixed Value _____ ☐ Configurable; range _____ to _____ ☐ Configurable, selectable from ____, ____, ____ ☐ Configurable, other, describe _____ ☐ Based on point Index (add column to table below)
Counters frozen by means of:	☐ Master Request ☒ Freezes itself without concern for time of day ☐ Freezes itself and requires time of day ☐ Other, explain _____
Definition of Counter/Frozen Counter Point List: List all addressable points. Points that do not exist (for example, because an option is not installed) shall be omitted from the table.	☐ Fixed, list shown in table below ☐ Configurable (current list may be shown in table below) ☐ Other, explain _____

Point Index	Name	Default Class Assigned to Counter Events (1, 2, 3 or none)	Frozen Counter Exists (Yes or No)	Default Class Assigned to Frozen Counter Events (1, 2, 3 or none)	Description
0					
1					
2					
:	Add more rows as necessary				

4. Authorization

This document has been seen and accepted by:

Name and surname	Designation
Sham Dhrampal	Group IT: Corporate Specialist
Prince Moyo	General Manager: Power Delivery Engineering
Mervin Mottian	Dx SCADA Managers Forum Convenor
Prudence Madiba	Senior Manager Generation
Joe Manyisa	Senior Manager Telecoms
Comfort Masike	Senior Manager System Operator
Danie Conradie	Senior Manager Distribution
Danie Du Plessis	Senior Manager Transmission
Sham Dhrampal	Group IT: Corporate Specialist
Prince Moyo	General Manager: Power Delivery Engineering
Mervin Mottian	Dx SCADA Managers Forum Convenor

5. Revisions

Date	Rev	Compiler	Remarks
May 2019	2	S Mbanga	Edited the document Added Counters Added Analogue Outputs Added support for floating points under analogue inputs Added the DNP/IP section
Jan 2014	1	S Mbanga	First draft

6. Development team

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

- Insert Simphiwe Mbanga SI Eastern Cape Operating Unit
- Niel Myburgh SI Free State Operating Unit
- Thendo Ramulondi SI Limpopo Operating Unit
- Marlini Sukhnandan PTM&C: Control and Automation

7. Acknowledgements

- Tertius Hyman
- Ayanda Ndlebe
- Kenneth Brown
- George Daniel
- Colin Charles

Annex A – Impact assessment

(Normative – for Eskom internal use only)

1) Guidelines

- All comments shall be completed.
- Motivate why items are not applicable (n/a).
- Indicate actions to be taken, persons or organizations responsible for actions and deadline for action.
- Change control committees to discuss the impact assessment and, if necessary, give feedback to the compiler regarding any omissions or errors.

2) Critical points

2.1 Importance of this document, e.g. is implementation required due to safety deficiencies, statutory requirements, technology changes, document revisions, improved service quality, improved service performance, optimized costs.

Comment: The document addresses the issues that have been identified as gaps in the DNP 3 implementation by the suppliers.

2.2 If the document to be released impacts on statutory or legal compliance, this needs to be very clearly stated and so highlighted.

Comment: Not applicable, the document does not impact on statutory or legal compliance.

2.3 Impact on stock holding and depletion of existing stock prior to switch over.

Comment: No.

2.4 When will new stock be available?

Comment: This will apply to new DNP 3 RTU equipment.

2.5 Has the interchangeability of the product or item been verified, i.e. when it fails, is a straight swap possible with a competitor's product?

Comment: The interoperability of the protocol allows for multiple vendor equipment to communicate.

2.6 Identify and provide details of other critical (items required for the successful implementation of this document) points to be considered in the implementation of this document.

Comment: n/a

2.7 Provide details of any comments made by the Regions regarding the implementation of this document.

Comment: (n/a during commenting phase).

3) Implementation time frame

3.1 Time period for implementation of requirements.

Comment: At the time of going for tender for the Substation RTU evaluation.

3.2 Deadline for changeover to new item and personnel to be informed of DX wide changeover.

Comment: n/a

4) Buyer's guide and power office

4.1 Does the Buyer's Guide or Buyer's List need updating?

Comment: No.

4.2 What Buyer's Guides or items have been created?

Comment: None.

4.3 List all assembly drawing changes that have been revised in conjunction with this document.

Comment: None.

4.4 If the implementation of this document requires assessment by CAP, provide details under 5).

4.5 Which Power Office packages have been created, modified or removed?

Comment: None.

5) CAP/LAP pre-qualification process-related impacts

5.1 Is an ad hoc re-evaluation of all currently accepted suppliers required as a result of implementation of this document?

Comment: No.

5.2 If NO, provide motivation for issuing this specification before Acceptance Cycle Expiry date.

Comment: The document is a DNP3 standard implementation document not a specification.

5.3 Are ALL suppliers (currently accepted per LAP) aware of the nature of changes contained in this document?

Comment: No, it is not necessary as they met the minimum requirements stipulated on the equipment specification they went on tender.

5.4 Is implementation of the provisions of this document required during the current supplier qualification period?

Comment: No, It will only be applicable when we go on the next tender evaluation.

5.5 If Yes to 0, what date has been set for all currently accepted suppliers to comply fully?

Comment: n/a

5.6 If Yes to 0, have all currently accepted suppliers been sent a prior formal notification informing them of Eskom's expectations, including the implementation date deadline?

Comment: n/a

5.7 Can the changes made, potentially impact upon the purchase price of the material/equipment?

Comment: n/a

5.8 Material group(s) affected by specification (refer to Pre-qualification invitation schedule for list of material groups).

Comment: RTUs.

6) Training or communication

6.1 Is training required?

Comment: No.

6.2 State the level of training required to implement this document (e.g. awareness training, practical/on job, module).

Comment: n/a

6.3 State designations of personnel that will require training.

Comment: n/a

6.4 Is the training material available? Identify person responsible for the development of training material.

Comment: n/a

6.5 If applicable, provide details of training that will take place (e.g. sponsor, costs, trainer, schedule of training, course material availability, training in erection/use of new equipment, maintenance training).

Comment: n/a

6.6 Was Technical Training Section consulted regarding module development process?

Comment: n/a

6.7 State communications channels to be used to inform target audience.

Comment: Hyperwave, email, SCOT Study Committees.

7) Special tools, equipment, software

7.1 What special tools, equipment, software, etc. will need to be purchased by the Region to effectively implement?

Comment: None.

7.2 Are stock numbers available for the new equipment?

Comment: Not applicable, as this is about the implementation standard, and not equipment.

7.3 What will be the cost of these special tools, equipment, software?

Comment: No cost.

8) Finances

8.1 What total costs would the Regions be required to incur in implementing this document? Identify all cost activities associated with implementation, e.g. labour, training, tooling, stock, obsolescence.

Comment: No costs will be incurred.

Impact assessment completed by:

Name: Simphiwe Mbanga

Designation: Senior Telecontrol Engineer

Annex B – Device implementation tables for levels 1 to 4

The Device profiles shown in this annex are as per the IEEE 1815-2012, Interoperability section.

Level 1 device Implementation table

DNP3 OBJECT GROUP & VARIATION			REQUEST Master may issue Outstation shall parse		RESPONSE Master shall parse Outstation may issue	
Group num	Var num	Description	Function codes (dec)	Qualifier codes (hex)	Function codes (dec)	Qualifier codes (hex)
1	1	Binary Input— Packed format			129 (response)	00, 01 (start-stop)
1	2	Binary Input— With flags			129 (response)	00, 01 (start-stop)
2	1	Binary Input Event— Without time			129 (response) 130 (unsol. resp)	17, 28 (index)
2	2	Binary Input Event— With absolute time			129 (response) 130 (unsol. resp)	17, 28 (index)
2	3	Binary Input Event— With relative time			129 (response) 130 (unsol. resp)	17, 28 (index)
10	0	Binary Output— Any Variation	1 (read)	06 (no range, or all)		
10	2	Binary Output— Output status with flags			129 (response)	00, 01 (start-stop)
12	1	Binary Command— Control relay output block (CROB)	3 (select) 4 (operate) 5 (direct op)	17, 28 (index)	129 (response)	echo of request
			6 (dir op, no ack)	17, 28 (index)		
20	1	Counter— 32-bit with flag			129 (response)	00, 01 (start-stop)
20	2	Counter— 16-bit with flag			129 (response)	00, 01 (start-stop)
20	5	Counter— 32-bit without flag			129 (response)	00, 01 (start-stop)
20	6	Counter— 16-bit without flag			129 (response)	00, 01 (start-stop)
22	1	Counter Event— 32-bit with flag			129 (response) 130 (unsol. resp)	17, 28 (index)
22	2	Counter Event— 16-bit with flag			129 (response) 130 (unsol. resp)	17, 28 (index)

ESKOM COPYRIGHT PROTECTED

Level 1 device Implementation table - continued

DNP3 OBJECT GROUP & VARIATION			REQUEST Master may issue Outstation shall parse		RESPONSE Master shall parse Outstation may issue	
Group num	Var num	Description	Function codes (dec)	Qualifier codes (hex)	Function codes (dec)	Qualifier codes (hex)
30	1	Analog Input— 32-bit with flag			129 (response)	00, 01 (start-stop)
30	2	Analog Input— 16-bit with flag			129 (response)	00, 01 (start-stop)
30	3	Analog Input— 32-bit without flag			129 (response)	00, 01 (start-stop)
30	4	Analog Input— 16-bit without flag			129 (response)	00, 01 (start-stop)
32	1	Analog Input Event— 32-bit without time			129 (response) 130 (unsol. resp)	17, 28 (index)
32	2	Analog Input Event— 16-bit without time			129 (response) 130 (unsol. resp)	17, 28 (index)
40	0	Analog Output Status— Any Variation	1 (read)	06 (no range, or all)		
40	2	Analog Output Status— 16-bit with flag			129 (response)	00, 01 (start-stop)
41	2	Analog Output— 16-bit	3 (select) 4 (operate) 5 (direct op)	17, 28 (index)	129 (response)	echo of request
			6 (dir. op, no ack)	17, 28 (index)		
50	1	Time and Date— Absolute time	2 (write)	07 (limited qty = 1)		
51	1	Time and Date CTO— Absolute time, synchronized			129 (response) 130 (unsol. resp)	07 (limited qty) (qty = 1)
51	2	Time and Date CTO— Absolute time, unsynchronized			129 (response) 130 (unsol. resp)	07 (limited qty) (qty = 1)
52	1	Time Delay— Coarse			129 (response)	07 (limited qty) (qty = 1)
52	2	Time Delay— Fine			129 (response)	07 (limited qty) (qty = 1)

ESKOM COPYRIGHT PROTECTED

Level 1 device Implementation table - continued

DNP3 OBJECT GROUP & VARIATION			REQUEST Master may issue Outstation shall parse		RESPONSE Master shall parse Outstation may issue	
Group num	Var num	Description	Function codes (dec)	Qualifier codes (hex)	Function codes (dec)	Qualifier codes (hex)
60	1	Class Objects— Class 0 data	1 (read)	06 (no range, or all)		
60	2	Class Objects— Class 1 data	1 (read)	06 (no range, or all) 07, 08 (limited qty)		
60	3	Class Objects— Class 2 data	1 (read)	06 (no range, or all) 07, 08 (limited qty)		
60	4	Class Objects— Class 3 data	1 (read)	06 (no range, or all) 07, 08 (limited qty)		
80	1	Internal Indications— Packed format	2 (write)	00 (start-stop) index=7		
No Object (function code only)			0 (confirm)			
No Object (function code only)			13 (cold restart)			
No Object (function code only)			23 (delay measurement)			

ESKOM COPYRIGHT PROTECTED

Level 2 device implementation table

DNP3 OBJECT GROUP & VARIATION			REQUEST Master may issue Outstation shall parse		RESPONSE Master shall parse Outstation may issue	
Group num	Var num	Description	Function codes (dec)	Qualifier codes (hex)	Function codes (dec)	Qualifier codes (hex)
1	0	Binary Input— Any Variation	1 (read)	06 (no range, or all)		
1	1	Binary Input— Packed format			129 (response)	00, 01 (start-stop)
1	2	Binary Input— With flags			129 (response)	00, 01 (start-stop)
2	0	Binary Input Event— Any Variation	1 (read)	06 (no range, or all) 07, 08 (limited qty)		
2	1	Binary Input Event— Without time	1 (read)	06 (no range, or all) 07, 08 (limited qty)	129 (response) 130 (unsol. resp)	17, 28 (index)
2	2	Binary Input Event— With absolute time	1 (read)	06 (no range, or all) 07, 08 (limited qty)	129 (response) 130 (unsol. resp)	17, 28 (index)
2	3	Binary Input Event— With relative time	1 (read)	06 (no range, or all) 07, 08 (limited qty)	129 (response) 130 (unsol. resp)	17, 28 (index)
10	0	Binary Output— Any Variation	1 (read)	06 (no range, or all)		
10	2	Binary Output— Output status with flags			129 (response)	00, 01 (start-stop)
12	1	Binary Command— Control relay output block (CROB)	3 (select) 4 (operate) 5 (direct op)	17, 28 (index)	129 (response)	echo of request
			6 (dir. op, no ack)	17, 28 (index)		

ESKOM COPYRIGHT PROTECTED

Level 2 device implementation table - continued

DNP3 OBJECT GROUP & VARIATION			REQUEST Master may issue Outstation shall parse		RESPONSE Master shall parse Outstation may issue	
Group num	Var num	Description	Function codes (dec)	Qualifier codes (hex)	Function codes (dec)	Qualifier codes (hex)
20	0	Counter— Any Variation	1 (read) 7 (freeze) 8 (freeze noack) 9 (freeze clear) 10 (frz. cl. noack)	06 (no range, or all)		
20	1	Counter— 32-bit with flag			129 (response)	00, 01 (start-stop)
20	2	Counter— 16-bit with flag			129 (response)	00, 01 (start-stop)
20	5	Counter— 32-bit without flag			129 (response)	00, 01 (start-stop)
20	6	Counter— 16-bit without flag			129 (response)	00, 01 (start-stop)
21	0	Frozen Counter— Any Variation	1 (read)	06 (no range, or all)		
21	1	Frozen Counter— 32-bit with flag			129 (response)	00, 01 (start-stop)
21	2	Frozen Counter— 16-bit with flag			129 (response)	00, 01 (start-stop)
21	9	Frozen Counter— 32-bit without flag			129 (response)	00, 01 (start-stop)
21	10	Frozen Counter— 16-bit without flag			129 (response)	00, 01 (start-stop)
22	0	Counter Event— Any Variation	1 (read)	06 (no range, or all) 07, 08 (limited qty)		
22	1	Counter Event— 32-bit with flag			129 (response) 130 (unsol. resp)	17, 28 (index)
22	2	Counter Event— 16-bit with flag			129 (response) 130 (unsol. resp)	17, 28 (index)

ESKOM COPYRIGHT PROTECTED

Level 2 device implementation table - continued

DNP3 OBJECT GROUP & VARIATION			REQUEST Master may issue Outstation shall parse		RESPONSE Master shall parse Outstation may issue	
Group num	Var num	Description	Function codes (dec)	Qualifier codes (hex)	Function codes (dec)	Qualifier codes (hex)
30	0	Analog Input— Any Variation	1 (read)	06 (no range, or all)		
30	1	Analog Input— 32-bit with flag			129 (response)	00, 01 (start-stop)
30	2	Analog Input— 16-bit with flag			129 (response)	00, 01 (start-stop)
30	3	Analog Input— 32-bit without flag			129 (response)	00, 01 (start-stop)
30	4	Analog Input— 16-bit without flag			129 (response)	00, 01 (start-stop)
32	0	Analog Input Event— Any Variation	1 (read)	06 (no range, or all) 07, 08 (limited qty)		
32	1	Analog Input Event— 32-bit without time			129 (response) 130 (unsol. resp)	17, 28 (index)
32	2	Analog Input Event— 16-bit without time			129 (response) 130 (unsol. resp)	17, 28 (index)
40	0	Analog Output Status— Any Variation	1 (read)	06 (no range, or all)		
40	2	Analog Output Status— 16-bit with flag			129 (response)	00, 01 (start-stop)
41	2	Analog Output— 16-bit	3 (select) 4 (operate) 5 (direct op)	17, 28 (index)	129 (response)	echo of request
			6 (dir. op, no ack)	17, 28 (index)		
50	1	Time and Date— Absolute time	2 (write)	07 (limited qty = 1)		
51	1	Time and Date CTO— Absolute time, synchronized			129 (response) 130 (unsol. resp)	07 (limited qty) (qty = 1)
51	2	Time and Date CTO— Absolute time, unsynchronized			129 (response) 130 (unsol. resp)	07 (limited qty) (qty = 1)

ESKOM COPYRIGHT PROTECTED

Level 2 device implementation table - continued

DNP3 OBJECT GROUP & VARIATION			REQUEST Master may issue Outstation shall parse		RESPONSE Master shall parse Outstation may issue	
Group num	Var num	Description	Function codes (dec)	Qualifier codes (hex)	Function codes (dec)	Qualifier codes (hex)
52	1	Time Delay—Coarse			129 (response)	07 (limited qty) (qty = 1)
52	2	Time Delay—Fine			129 (response)	07 (limited qty) (qty = 1)
60	1	Class Objects—Class 0 data	1 (read)	06 (no range, or all)		
60	2	Class Objects—Class 1 data	1 (read)	06 (no range, or all) 07, 08 (limited qty)		
60	3	Class Objects—Class 2 data	1 (read)	06 (no range, or all) 07, 08 (limited qty)		
60	4	Class Objects—Class 3 data	1 (read)	06 (no range, or all) 07, 08 (limited qty)		
80	1	Internal Indications—Packed format	2 (write)	00 (start-stop) index=7		
No Object (function code only)			0 (Confirm)			
No Object (function code only)			13 (cold restart)			
No Object (function code only)			23 (delay measurement)			

ESKOM COPYRIGHT PROTECTED

Level 3 device implementation table

DNP3 OBJECT GROUP & VARIATION			REQUEST Master may issue Outstation shall parse		RESPONSE Master shall parse Outstation may issue	
Group num	Var num	Description	Function codes (dec)	Qualifier codes (hex)	Function codes (dec)	Qualifier codes (hex)
1	0	Binary Input— Any Variation	1 (read) 22 (assign class)	00, 01 (start-stop) 06 (no range, or all)		
1	1	Binary Input— Packed format	1 (read)	00, 01 (start-stop) 06 (no range, or all)	129 (response)	00, 01 (start-stop)
1	2	Binary Input— With flags	1 (read)	00, 01 (start-stop) 06 (no range, or all)	129 (response)	00, 01 (start-stop)
2	0	Binary Input Event— Any Variation	1 (read)	06 (no range, or all) 07, 08 (limited qty)		
2	1	Binary Input Event— Without time	1 (read)	06 (no range, or all) 07, 08 (limited qty)	129 (response) 130 (unsol. resp)	17, 28 (index)
2	2	Binary Input Event— With absolute time	1 (read)	06 (no range, or all) 07, 08 (limited qty)	129 (response) 130 (unsol. resp)	17, 28 (index)
2	3	Binary Input Event— With relative time	1 (read)	06 (no range, or all) 07, 08 (limited qty)	129 (response) 130 (unsol. resp)	17, 28 (index)
10	0	Binary Output— Any Variation	1 (read)	00, 01 (start-stop) 06 (no range, or all)		
10	2	Binary Output— Output status with flags	1 (read)	00, 01 (start-stop) 06 (no range, or all)	129 (response)	00, 01 (start-stop)
12	1	Binary Command— Control relay output block (CROB)	3 (select) 4 (operate) 5 (direct op)	17, 28 (index)	129 (response)	echo of request
			6 (dir. op, no ack)	17, 28 (index)		

ESKOM COPYRIGHT PROTECTED

Level 3 device implementation table - continued

DNP3 OBJECT GROUP & VARIATION			REQUEST Master may issue Outstation shall parse		RESPONSE Master shall parse Outstation may issue	
Group num	Var num	Description	Function codes (dec)	Qualifier codes (hex)	Function codes (dec)	Qualifier codes (hex)
20	0	Counter— Any Variation	1 (read) 7 (freeze) 8 (freeze noack) 9 (freeze clear) 10 (frz. cl. noack) 22 (assign class)	00, 01 (start-stop) 06 (no range, or all)		
20	1	Counter— 32-bit with flag	1 (read)	00, 01 (start-stop) 06 (no range, or all)	129 (response)	00, 01 (start-stop)
20	2	Counter— 16-bit with flag	1 (read)	00, 01 (start-stop) 06 (no range, or all)	129 (response)	00, 01 (start-stop)
20	5	Counter— 32-bit without flag	1 (read)	00, 01 (start-stop) 06 (no range, or all)	129 (response)	00, 01 (start-stop)
20	6	Counter— 16-bit without flag	1 (read)	00, 01 (start-stop) 06 (no range, or all)	129 (response)	00, 01 (start-stop)
21	0	Frozen Counter— Any Variation	1 (read) 22 (assign class)	00, 01 (start-stop) 06 (no range, or all)		
21	1	Frozen Counter— 32-bit with flag	1 (read)	00, 01 (start-stop) 06 (no range, or all)	129 (response)	00, 01 (start-stop)
21	2	Frozen Counter— 16-bit with flag	1 (read)	00, 01 (start-stop) 06 (no range, or all)	129 (response)	00, 01 (start-stop)
21	9	Frozen Counter— 32-bit without flag	1 (read)	00, 01 (start-stop) 06 (no range, or all)	129 (response)	00, 01 (start-stop)
21	10	Frozen Counter— 16-bit without flag	1 (read)	00, 01 (start-stop) 06 (no range, or all)	129 (response)	00, 01 (start-stop)

ESKOM COPYRIGHT PROTECTED

Level 3 device implementation table - continued

DNP3 OBJECT GROUP & VARIATION			REQUEST Master may issue Outstation shall parse		RESPONSE Master shall parse Outstation may issue	
Group num	Var num	Description	Function codes (dec)	Qualifier codes (hex)	Function codes (dec)	Qualifier codes (hex)
22	0	Counter Event— Any Variation	1 (read)	06 (no range, or all) 07, 08 (limited qty)		
22	1	Counter Event— 32-bit with flag	1 (read)	06 (no range, or all) 07, 08 (limited qty)	129 (response) 130 (unsol. resp)	17, 28 (index)
22	2	Counter Event— 16-bit with flag	1 (read)	06 (no range, or all) 07, 08 (limited qty)	129 (response) 130 (unsol. resp)	17, 28 (index)
23	0	Frozen Counter Event— Any Variation	1 (read)	06 (no range, or all) 07, 08 (limited qty)		
23	1	Frozen Counter Event— 32-bit with flag	1 (read)	06 (no range, or all) 07, 08 (limited qty)	129 (response) 130 (unsol. resp)	17, 28 (index)
23	2	Frozen Counter Event— 16-bit with flag	1 (read)	06 (no range, or all) 07, 08 (limited qty)	129 (response) 130 (unsol. resp)	17, 28 (index)
30	0	Analog Input— Any Variation	1 (read) 22 (assign class)	00, 01 (start-stop) 06 (no range, or all)		
30	1	Analog Input— 32-bit with flag	1 (read)	00, 01 (start-stop) 06 (no range, or all)	129 (response)	00, 01 (start-stop)
30	2	Analog Input— 16-bit with flag	1 (read)	00, 01 (start-stop) 06 (no range, or all)	129 (response)	00, 01 (start-stop)
30	3	Analog Input— 32-bit without flag	1 (read)	00, 01 (start-stop) 06 (no range, or all)	129 (response)	00, 01 (start-stop)
30	4	Analog Input— 16-bit without flag	1 (read)	00, 01 (start-stop) 06 (no range, or all)	129 (response)	00, 01 (start-stop)

ESKOM COPYRIGHT PROTECTED

Level 3 device implementation table - continued

DNP3 OBJECT GROUP & VARIATION			REQUEST Master may issue Outstation shall parse		RESPONSE Master shall parse Outstation may issue	
Group num	Var num	Description	Function codes (dec)	Qualifier codes (hex)	Function codes (dec)	Qualifier codes (hex)
32	0	Analog Input Event—Any Variation	1 (read)	06 (no range, or all) 07, 08 (limited qty)		
32	1	Analog Input Event—32-bit without time	1 (read)	06 (no range, or all) 07, 08 (limited qty)	129 (response) 130 (unsol. resp)	17, 28 (index)
32	2	Analog Input Event—16-bit without time	1 (read)	06 (no range, or all) 07, 08 (limited qty)	129 (response) 130 (unsol. resp)	17, 28 (index)
40	0	Analog Output Status—Any Variation	1 (read)	00, 01 (start-stop) 06 (no range, or all)	129 (response)	
40	1	Analog Output Status—32-bit with flag	1 (read)	00, 01 (start-stop) 06 (no range, or all)		00, 01 (start-stop)
40	2	Analog Output Status—16-bit with flag	1 (read)	00, 01 (start-stop) 06 (no range, or all)		00, 01 (start-stop)
41	1	Analog Output—32-bit	3 (select) 4 (operate) 5 (direct op)	17, 28 (index)	129 (response)	echo of request
			6 (dir. op, no ack)	17, 28 (index)		
41	2	Analog Output—16-bit	3 (select) 4 (operate) 5 (direct op)	17, 28 (index)	129 (response)	echo of request
			6 (dir. op, no ack)	17, 28 (index)		
50	1	Time and Date—Absolute time	1 (read)	07 (limited qty = 1)	129 (response)	07 (limited qty) (qty = 1)
			2 (write)	07 (limited qty = 1)		

ESKOM COPYRIGHT PROTECTED

Level 3 device implementation table - continued

DNP3 OBJECT GROUP & VARIATION			REQUEST Master may issue Outstation shall parse		RESPONSE Master shall parse Outstation may issue	
Group num	Var num	Description	Function codes (dec)	Qualifier codes (hex)	Function codes (dec)	Qualifier codes (hex)
51	1	Time and Date CTO— Absolute time, synchronized			129 (response) 130 (unsol. resp)	07 (limited qty) (qty = 1)
51	2	Time and Date CTO— Absolute time, unsynchronized			129 (response) 130 (unsol. resp)	07 (limited qty) (qty = 1)
52	1	Time Delay— Coarse			129 (response)	07 (limited qty) (qty = 1)
52	2	Time Delay— Fine			129 (response)	07 (limited qty) (qty = 1)
60	1	Class Objects— Class 0 data	1 (read)	06 (no range, or all)		
			22 (assign class)	06 (no range, or all)		
60	2	Class Objects— Class 1 data	1 (read)	06 (no range, or all) 07, 08 (limited qty)		
			20 (enable unsol.) 21 (disable unsol.) 22 (assign class)	06 (no range, or all)		
60	3	Class Objects— Class 2 data	1 (read)	06 (no range, or all) 07, 08 (limited qty)		
			20 (enable unsol.) 21 (disable unsol.) 22 (assign class)	06 (no range, or all)		

ESKOM COPYRIGHT PROTECTED

Level 3 device implementation table - continued

DNP3 OBJECT GROUP & VARIATION			REQUEST Master may issue Outstation shall parse		RESPONSE Master shall parse Outstation may issue	
Group num	Var num	Description	Function codes (dec)	Qualifier codes (hex)	Function codes (dec)	Qualifier codes (hex)
60	4	Class Objects— Class 3 data	1 (read)	06 (no range, or all) 07, 08 (limited qty)		
			20 (enable unsol.) 21 (disable unsol.) 22 (assign class)	06 (no range, or all)		
80	1	Internal Indications— Packed format	1 (read)	00, 01 (start-stop)	129 (response)	00, 01 (start-stop)
			2 (write)	00 (start-stop) index=7		
No Object (function code only)			0 (Confirm)			
No Object (function code only)			13 (cold restart)			
No Object (function code only)			23 (delay measurement)			

ESKOM COPYRIGHT PROTECTED

Level 4 device implementation table

DNP3 OBJECT GROUP & VARIATION			REQUEST Master may issue Outstation shall parse		RESPONSE Master shall parse Outstation may issue	
Group num	Var num	Description	Function codes (dec)	Qualifier codes (hex)	Function codes (dec)	Qualifier codes (hex)
0	209	Device Attributes—Secure authentication version	1 (read)	00 (start-stop)	129 (response)	00 (start-stop) 17 (index)
0	210	Device Attributes—Number of security statistics per association	1 (read)	00 (start-stop)	129 (response)	00 (start-stop) 17 (index)
0	211	Device Attributes—Identifier of support for user-specific attributes	1 (read)	00 (start-stop)	129 (response)	00 (start-stop) 17 (index)
0	212	Device Attributes—Number of master-defined data set prototypes	1 (read)	00 (start-stop)	129 (response)	00 (start-stop) 17 (index)
0	213	Device Attributes—Number of outstation-defined data set prototypes	1 (read)	00 (start-stop)	129 (response)	00 (start-stop) 17 (index)
0	214	Device Attributes—Number of master-defined data sets	1 (read)	00 (start-stop)	129 (response)	00 (start-stop) 17 (index)
0	215	Device Attributes—Number of outstation-defined data sets	1 (read)	00 (start-stop)	129 (response)	00 (start-stop) 17 (index)
0	216	Device Attributes—Max number of binary outputs per request	1 (read)	00 (start-stop)	129 (response)	00 (start-stop) 17 (index)
0	217	Device Attributes—Local timing accuracy	1 (read)	00 (start-stop)	129 (response)	00 (start-stop) 17 (index)
0	218	Device Attributes—Duration of timing accuracy	1 (read)	00 (start-stop)	129 (response)	00 (start-stop) 17 (index)
0	219	Device Attributes—Support for analog output events	1 (read)	00 (start-stop)	129 (response)	00 (start-stop) 17 (index)

ESKOM COPYRIGHT PROTECTED

Level 4 device implementation table - continued

DNP3 OBJECT GROUP & VARIATION			REQUEST Master may issue Outstation shall parse		RESPONSE Master shall parse Outstation may issue	
Group num	Var num	Description	Function codes (dec)	Qualifier codes (hex)	Function codes (dec)	Qualifier codes (hex)
0	220	Device Attributes— Max analog output index	1 (read)	00 (start-stop)	129 (response)	00 (start-stop) 17 (index)
0	221	Device Attributes— Number of analog outputs	1 (read)	00 (start-stop)	129 (response)	00 (start-stop) 17 (index)
0	222	Device Attributes— Support for binary output events	1 (read)	00 (start-stop)	129 (response)	00 (start-stop) 17 (index)
0	223	Device Attributes— Max binary output index	1 (read)	00 (start-stop)	129 (response)	00 (start-stop) 17 (index)
0	224	Device Attributes— Number of binary outputs	1 (read)	00 (start-stop)	129 (response)	00 (start-stop) 17 (index)
0	225	Device Attributes— Support for frozen counter events	1 (read)	00 (start-stop)	129 (response)	00 (start-stop) 17 (index)
0	226	Device Attributes— Support for frozen counters	1 (read)	00 (start-stop)	129 (response)	00 (start-stop) 17 (index)
0	227	Device Attributes— Support for counter events	1 (read)	00 (start-stop)	129 (response)	00 (start-stop) 17 (index)
0	228	Device Attributes— Max counter index	1 (read)	00 (start-stop)	129 (response)	00 (start-stop) 17 (index)
0	229	Device Attributes— Number of counter points	1 (read)	00 (start-stop)	129 (response)	00 (start-stop) 17 (index)
0	230	Device Attributes— Support for frozen analog inputs	1 (read)	00 (start-stop)	129 (response)	00 (start-stop) 17 (index)

ESKOM COPYRIGHT PROTECTED

Level 4 device implementation table - continued

DNP3 OBJECT GROUP & VARIATION			REQUEST Master may issue Outstation shall parse		RESPONSE Master shall parse Outstation may issue	
Group num	Var num	Description	Function codes (dec)	Qualifier codes (hex)	Function codes (dec)	Qualifier codes (hex)
0	231	Device Attributes— Support for analog input events	1 (read)	00 (start-stop)	129 (response)	00 (start-stop) 17 (index)
0	232	Device Attributes— Maximum analog input index	1 (read)	00 (start-stop)	129 (response)	00 (start-stop) 17 (index)
0	233	Device Attributes— Number of analog input points	1 (read)	00 (start-stop)	129 (response)	00 (start-stop) 17 (index)
0	234	Device Attributes— Support for double-bit binary input events	1 (read)	00 (start-stop)	129 (response)	00 (start-stop) 17 (index)
0	235	Device Attributes— Maximum double-bit binary input index	1 (read)	00 (start-stop)	129 (response)	00 (start-stop) 17 (index)
0	236	Device Attributes— Number of double-bit binary input points	1 (read)	00 (start-stop)	129 (response)	00 (start-stop) 17 (index)
0	237	Device Attributes— Support for binary input events	1 (read)	00 (start-stop)	129 (response)	00 (start-stop) 17 (index)
0	238	Device Attributes— Max binary input index	1 (read)	00 (start-stop)	129 (response)	00 (start-stop) 17 (index)
0	239	Device Attributes— Number of binary input points	1 (read)	00 (start-stop)	129 (response)	00 (start-stop) 17 (index)
0	240	Device Attributes— Max transmit fragment size	1 (read)	00 (start-stop)	129 (response)	00 (start-stop) 17 (index)
			2 (write)	00 (start-stop)		
0	241	Device Attributes— Max receive fragment size	1 (read)	00 (start-stop)	129 (response)	00 (start-stop) 17 (index)

ESKOM COPYRIGHT PROTECTED

Level 4 device implementation table - continued

DNP3 OBJECT GROUP & VARIATION			REQUEST Master may issue Outstation shall parse		RESPONSE Master shall parse Outstation may issue	
Group num	Var num	Description	Function codes (dec)	Qualifier codes (hex)	Function codes (dec)	Qualifier codes (hex)
0	242	Device Attributes— Device manufacturer's software version	1 (read)	00 (start-stop)	129 (response)	00 (start-stop) 17 (index)
0	243	Device Attributes— Device manufacturer's hardware version	1 (read)	00 (start-stop)	129 (response)	00 (start-stop) 17 (index)
0	245	Device Attributes— User-assigned location name	1 (read)	00 (start-stop)	129 (response)	00 (start-stop) 17 (index)
			2 (write)	00 (start-stop)		
0	246	Device Attributes— User assigned ID code/number	1 (read)	00 (start-stop)	129 (response)	00 (start-stop) 17 (index)
			2 (write)	00 (start-stop)		
0	247	Device Attributes— User-assigned device name	1 (read)	00 (start-stop)	129 (response)	00 (start-stop) 17 (index)
			2 (write)	00 (start-stop)		
0	248	Device Attributes— Device serial number	1 (read)	00 (start-stop)	129 (response)	00 (start-stop) 17 (index)
0	249	Device Attributes— DNP3 subset and conformance	1 (read)	00 (start-stop)	129 (response)	00 (start-stop) 17 (index)
0	250	Device Attributes— Device manufacturer's product name and model	1 (read)	00 (start-stop)	129 (response)	00 (start-stop) 17 (index)
0	252	Device Attributes— Device manufacturer's name	1 (read)	00 (start-stop)	129 (response)	00 (start-stop) 17 (index)
0	254	Device Attributes— Non-specific all attributes request	1 (read)	00 (start-stop) 06 (no range, or all)		

ESKOM COPYRIGHT PROTECTED

Level 4 device implementation table - continued

DNP3 OBJECT GROUP & VARIATION			REQUEST Master may issue Outstation shall parse		RESPONSE Master shall parse Outstation may issue	
Group num	Var num	Description	Function codes (dec)	Qualifier codes (hex)	Function codes (dec)	Qualifier codes (hex)
0	255	Device Attributes— List of attribute variations	1 (read)	00 (start-stop) 06 (no range, or all)	129 (response)	00 (start-stop) 17 (index)
1	0	Binary Input— Any Variation	1 (read) 22 (assign class)	00, 01 (start-stop) 06 (no range, or all)		
1	1	Binary Input— Packed format	1 (read)	00, 01 (start-stop) 06 (no range, or all)	129 (response)	00, 01 (start-stop)
1	2	Binary Input— With flags	1 (read)	00, 01 (start-stop) 06 (no range, or all)	129 (response)	00, 01 (start-stop)
2	0	Binary Input Event— Any Variation	1 (read)	06 (no range, or all) 07, 08 (limited qty)		
2	1	Binary Input Event— Without time	1 (read)	06 (no range, or all) 07, 08 (limited qty)	129 (response) 130 (unsol. resp)	17, 28 (index)
2	2	Binary Input Event— With absolute time	1 (read)	06 (no range, or all) 07, 08 (limited qty)	129 (response) 130 (unsol. resp)	17, 28 (index)
2	3	Binary Input Event— With relative time	1 (read)	06 (no range, or all) 07, 08 (limited qty)	129 (response) 130 (unsol. resp)	17, 28 (index)
3	0	Double-bit Binary Input— Any Variation	1 (read) 22 (assign class)	00, 01 (start-stop) 06 (no range, or all)		
3	1	Double-bit Binary Input— Packed format	1 (read)	00, 01 (start-stop) 06 (no range, or all)	129 (response)	00, 01 (start-stop)
3	2	Double-bit Binary Input— With flags	1 (read)	00, 01 (start-stop) 06 (no range, or all)	129 (response)	00, 01 (start-stop)

ESKOM COPYRIGHT PROTECTED

Level 4 device implementation table - continued

DNP3 OBJECT GROUP & VARIATION			REQUEST Master may issue Outstation shall parse		RESPONSE Master shall parse Outstation may issue	
Group num	Var num	Description	Function codes (dec)	Qualifier codes (hex)	Function codes (dec)	Qualifier codes (hex)
4	0	Double-bit Binary Input Event—Any Variation	1 (read)	06 (no range, or all) 07, 08 (limited qty)		
4	1	Double-bit Binary Input Event—Without time	1 (read)	06 (no range, or all) 07, 08 (limited qty)	129 (response) 130 (unsol. resp)	17, 28 (index)
4	2	Double-bit Binary Input Event—With absolute time	1 (read)	06 (no range, or all) 07, 08 (limited qty)	129 (response) 130 (unsol. resp)	17, 28 (index)
4	3	Double-bit Binary Input Event—With relative time	1 (read)	06 (no range, or all) 07, 08 (limited qty)	129 (response) 130 (unsol. resp)	17, 28 (index)
10	0	Binary Output—Any Variation	1 (read) 22 (assign class)	00, 01 (start-stop) 06 (no range, or all)		
10	2	Binary Output—Output status with flags	1 (read)	00, 01 (start-stop) 06 (no range, or all)	129 (response)	00, 01 (start-stop)
11	0	Binary Output Event—Any Variation	1 (read)	06 (no range, or all) 07, 08 (limited qty)		
11	1	Binary Output Event—Status without time	1 (read)	06 (no range, or all) 07, 08 (limited qty)	129 (response) 130 (unsol. resp)	17, 28 (index)
11	2	Binary Output Event—Status with time	1 (read)	06 (no range, or all) 07, 08 (limited qty)	129 (response) 130 (unsol. resp)	17, 28 (index)
12	0	Binary Command—Control relay output block (CROB)	22 (assign class)	00, 01 (start-stop) 06 (no range, or all)		
12	1	Binary Command—Control relay output block (CROB)	3 (select) 4 (operate) 5 (direct op)	17, 28 (index)	129 (response)	echo of request

ESKOM COPYRIGHT PROTECTED

Level 4 device implementation table - continued

DNP3 OBJECT GROUP & VARIATION			REQUEST Master may issue Outstation shall parse		RESPONSE Master shall parse Outstation may issue	
Group num	Var num	Description	Function codes (dec)	Qualifier codes (hex)	Function codes (dec)	Qualifier codes (hex)
			6 (dir. op, no ack)	17, 28 (index)		
			22 (assign class)	00, 01 (start-stop) 06 (no range, or all)		
13	0	Binary Output Command Event— Any Variation	1 (read)	06 (no range, or all) 07, 08 (limited qty)		
13	1	Binary Output Command Event— Command status without time	1 (read)	06 (no range, or all) 07, 08 (limited qty)	129 (response) 130 (unsol. resp)	17, 28 (index)
13	2	Binary Output Command Event— Command status with time	1 (read)	06 (no range, or all) 07, 08 (limited qty)	129 (response) 130 (unsol. resp)	17, 28 (index)
20	0	Counter— Any Variation	1 (read) 7 (freeze) 8 (freeze noack) 9 (freeze clear) 10 (fz. cl. noack) 22 (assign class)	00, 01 (start-stop) 06 (no range, or all)		
20	1	Counter— 32-bit with flag	1 (read)	00, 01 (start-stop) 06 (no range, or all)	129 (response)	00, 01 (start-stop)
20	2	Counter— 16-bit with flag	1 (read)	00, 01 (start-stop) 06 (no range, or all)	129 (response)	00, 01 (start-stop)
20	5	Counter— 32-bit without flag	1 (read)	00, 01 (start-stop) 06 (no range, or all)	129 (response)	00, 01 (start-stop)
20	6	Counter— 16-bit without flag	1 (read)	00, 01 (start-stop) 06 (no range, or all)	129 (response)	00, 01 (start-stop)

ESKOM COPYRIGHT PROTECTED

Level 4 device implementation table - continued

DNP3 OBJECT GROUP & VARIATION			REQUEST Master may issue Outstation shall parse		RESPONSE Master shall parse Outstation may issue	
Group num	Var num	Description	Function codes (dec)	Qualifier codes (hex)	Function codes (dec)	Qualifier codes (hex)
21	0	Frozen Counter— Any Variation	1 (read) 22 (assign class)	00, 01 (start-stop) 06 (no range, or all)		
21	1	Frozen Counter— 32-bit with flag	1 (read)	00, 01 (start-stop) 06 (no range, or all)	129 (response)	00, 01 (start-stop)
21	2	Frozen Counter— 16-bit with flag	1 (read)	00, 01 (start-stop) 06 (no range, or all)	129 (response)	00, 01 (start-stop)
21	5	Frozen Counter— 32-bit with flag and time	1 (read)	00, 01 (start-stop) 06 (no range, or all)	129 (response)	00, 01 (start-stop)
21	6	Frozen Counter— 16-bit with flag and time	1 (read)	00, 01 (start-stop) 06 (no range, or all)	129 (response)	00, 01 (start-stop)
21	9	Frozen Counter— 32-bit without flag	1 (read)	00, 01 (start-stop) 06 (no range, or all)	129 (response)	00, 01 (start-stop)
21	10	Frozen Counter— 16-bit without flag	1 (read)	00, 01 (start-stop) 06 (no range, or all)	129 (response)	00, 01 (start-stop)
22	0	Counter Event— Any Variation	1 (read)	06 (no range, or all) 07, 08 (limited qty)		
22	1	Counter Event— 32-bit with flag	1 (read)	06 (no range, or all) 07, 08 (limited qty)	129 (response) 130 (unsol. resp)	17, 28 (index)
22	2	Counter Event— 16-bit with flag	1 (read)	06 (no range, or all) 07, 08 (limited qty)	129 (response) 130 (unsol. resp)	17, 28 (index)
23	0	Frozen Counter Event— Any Variation	1 (read)	06 (no range, or all) 07, 08 (limited qty)		

ESKOM COPYRIGHT PROTECTED

Level 4 device implementation table - continued

DNP3 OBJECT GROUP & VARIATION			REQUEST Master may issue Outstation shall parse		RESPONSE Master shall parse Outstation may issue	
Group num	Var num	Description	Function codes (dec)	Qualifier codes (hex)	Function codes (dec)	Qualifier codes (hex)
23	1	Frozen Counter Event— 32-bit with flag	1 (read)	06 (no range, or all) 07, 08 (limited qty)	129 (response) 130 (unsol. resp)	17, 28 (index)
23	2	Frozen Counter Event— 16-bit with flag	1 (read)	06 (no range, or all) 07, 08 (limited qty)	129 (response) 130 (unsol. resp)	17, 28 (index)
23	5	Frozen Counter Event— 32-bit with flag and time	1 (read)	06 (no range, or all) 07, 08 (limited qty)	129 (response) 130 (unsol. resp)	17, 28 (index)
23	6	Frozen Counter Event— 16-bit with flag and time	1 (read)	06 (no range, or all) 07, 08 (limited qty)	129 (response) 130 (unsol. resp)	17, 28 (index)
30	0	Analog Input— Any Variation	1 (read) 22 (assign class)	00, 01 (start-stop) 06 (no range, or all)		
30	1	Analog Input— 32-bit with flag	1 (read)	00, 01 (start-stop) 06 (no range, or all)	129 (response)	00, 01 (start-stop)
30	2	Analog Input— 16-bit with flag	1 (read)	00, 01 (start-stop) 06 (no range, or all)	129 (response)	00, 01 (start-stop)
30	3	Analog Input— 32-bit without flag	1 (read)	00, 01 (start-stop) 06 (no range, or all)	129 (response)	00, 01 (start-stop)
30	4	Analog Input— 16-bit without flag	1 (read)	00, 01 (start-stop) 06 (no range, or all)	129 (response)	00, 01 (start-stop)
30	5	Analog Input— Single-prec flt-pt with flag	1 (read)	00, 01 (start-stop) 06 (no range, or all)	129 (response)	00, 01 (start-stop)
32	0	Analog Input Event— Any Variation	1 (read)	06 (no range, or all) 07, 08 (limited qty)		

ESKOM COPYRIGHT PROTECTED

Level 4 device implementation table - continued

DNP3 OBJECT GROUP & VARIATION			REQUEST Master may issue Outstation shall parse		RESPONSE Master shall parse Outstation may issue	
Group num	Var num	Description	Function codes (dec)	Qualifier codes (hex)	Function codes (dec)	Qualifier codes (hex)
32	1	Analog Input Event—32-bit without time	1 (read)	06 (no range, or all) 07, 08 (limited qty)	129 (response) 130 (unsol. resp)	17, 28 (index)
32	2	Analog Input Event—16-bit without time	1 (read)	06 (no range, or all) 07, 08 (limited qty)	129 (response) 130 (unsol. resp)	17, 28 (index)
32	3	Analog Input Event—32-bit with time	1 (read)	06 (no range, or all) 07, 08 (limited qty)	129 (response) 130 (unsol. resp)	17, 28 (index)
32	4	Analog Input Event—16-bit with time	1 (read)	06 (no range, or all) 07, 08 (limited qty)	129 (response) 130 (unsol. resp)	17, 28 (index)
32	5	Analog Input Event—Single-prec flt-pt without time	1 (read)	06 (no range, or all) 07, 08 (limited qty)	129 (response) 130 (unsol. resp)	17, 28 (index)
32	7	Analog Input Event—Single-prec flt-pt with time	1 (read)	06 (no range, or all) 07, 08 (limited qty)	129 (response) 130 (unsol. resp)	17, 28 (index)
34	0	Analog Input Deadband—Any Variation	1 (read)	00, 01 (start-stop) 06 (no range, or all)		
34	1	Analog Input Deadband—16-bit	1 (read)	00, 01 (start-stop) 06 (no range, or all)	129 (response)	00, 01 (start-stop)
			2 (write)	00, 01 (start-stop) 17, 28 (index)		
34	2	Analog Input Deadband—32-bit	1 (read)	00, 01 (start-stop) 06 (no range, or all)	129 (response)	00, 01 (start-stop)
			2 (write)	00, 01 (start-stop) 17, 28 (index)		

ESKOM COPYRIGHT PROTECTED

Level 4 device implementation table - continued

DNP3 OBJECT GROUP & VARIATION			REQUEST Master may issue Outstation shall parse		RESPONSE Master shall parse Outstation may issue	
Group num	Var num	Description	Function codes (dec)	Qualifier codes (hex)	Function codes (dec)	Qualifier codes (hex)
34	3	Analog Input Deadband— Single-prec flt-pt	1 (read)	00, 01 (start-stop) 06 (no range, or all)	129(response)	00, 01 (start-stop)
			2 (write)	00, 01 (start-stop) 17, 28 (index)		
40	0	Analog Output Status— Any Variation	1 (read) 22 (assign class)	00, 01 (start-stop) 06 (no range, or all)		
40	1	Analog Output Status— 32-bit with flag	1 (read)	00, 01 (start-stop) 06 (no range, or all)	129 (response)	00, 01 (start-stop)
40	2	Analog Output Status— 16-bit with flag	1 (read)	00, 01 (start-stop) 06 (no range, or all)	129 (response)	00, 01 (start-stop)
40	3	Analog Output Status— Single-prec flt-pt with flag	1 (read)	00, 01 (start-stop) 06 (no range, or all)	129 (response)	00, 01 (start-stop)
41	0	Analog Output— Any Variation	22 (assign class)	00, 01 (start-stop) 06 (no range, or all)		
41	1	Analog Output— 32-bit	3 (select) 4 (operate) 5 (direct op)	17, 28 (index)	129 (response)	echo of request
			6 (dir. op, no ack)	17, 28 (index)		
41	2	Analog Output— 16-bit	3 (select) 4 (operate) 5 (direct op)	17, 28 (index)	129 (response)	echo of request
			6 (dir. op, no ack)	17, 28 (index)		

ESKOM COPYRIGHT PROTECTED

Level 4 device implementation table - continued

DNP3 OBJECT GROUP & VARIATION			REQUEST Master may issue Outstation shall parse		RESPONSE Master shall parse Outstation may issue	
Group num	Var num	Description	Function codes (dec)	Qualifier codes (hex)	Function codes (dec)	Qualifier codes (hex)
41	3	Analog Output— Single-prec flt-pt	3 (select) 4 (operate) 5 (direct op)	17, 28 (index)	129 (response)	echo of request
			6 (dir. op, no ack)	17, 28 (index)		
42	0	Analog Output Event— Any Variation	1 (read)	06 (no range, or all) 07, 08 (limited qty)		
42	1	Analog Output Event— 32-bit without time	1 (read)	06 (no range, or all) 07, 08 (limited qty)	129 (response) 130 (unsol. resp)	17, 28 (index)
42	2	Analog Output Event— 16-bit without time	1 (read)	06 (no range, or all) 07, 08 (limited qty)	129 (response) 130 (unsol. resp)	17, 28 (index)
42	3	Analog Output Event— 32-bit with time	1 (read)	06 (no range, or all) 07, 08 (limited qty)	129 (response) 130 (unsol. resp)	17, 28 (index)
42	4	Analog Output Event— 16-bit with time	1 (read)	06 (no range, or all) 07, 08 (limited qty)	129 (response) 130 (unsol. resp)	17, 28 (index)
42	5	Analog Output Event— Single-prec flt-pt without time	1 (read)	06 (no range, or all) 07, 08 (limited qty)	129 (response) 130 (unsol. resp)	17, 28 (index)
42	7	Analog Output Event— Single-prec flt-pt with time	1 (read)	06 (no range, or all) 07, 08 (limited qty)	129 (response) 130(unsol. resp)	17, 28 (index)
43	0	Analog Output Command Event— Any Variation	1 (read)	06 (no range, or all) 07, 08 (limited qty)		
43	1	Analog Output Command Event— 32-bit without time	1 (read)	06 (no range, or all) 07, 08 (limited qty)	129 (response) 130 (unsol. resp)	17, 28 (index)

ESKOM COPYRIGHT PROTECTED

Level 4 device implementation table - continued

DNP3 OBJECT GROUP & VARIATION			REQUEST Master may issue Outstation shall parse		RESPONSE Master shall parse Outstation may issue	
Group num	Var num	Description	Function codes (dec)	Qualifier codes (hex)	Function codes (dec)	Qualifier codes (hex)
43	2	Analog Output Command Event— 16-bit without time	1 (read)	06 (no range, or all) 07, 08 (limited qty)	129 (response) 130 (unsol. resp)	17, 28 (index)
43	3	Analog Output Command Event— 32-bit with time	1 (read)	06 (no range, or all) 07, 08 (limited qty)	129 (response) 130 (unsol. resp)	17, 28 (index)
43	4	Analog Output Command Event— 16-bit with time	1 (read)	06 (no range, or all) 07, 08 (limited qty)	129 (response) 130 (unsol. resp)	17, 28 (index)
43	5	Analog Output Command Event— Single-prec flt-pt without time	1 (read)	06 (no range, or all) 07, 08 (limited qty)	129 (response) 130 (unsol. resp)	17, 28 (index)
43	7	Analog Output Command Event— Single-prec flt-pt with time	1 (read)	06 (no range, or all) 07, 08 (limited qty)	129 (response) 130 (unsol. resp)	17, 28 (index)
50	1	Time and Date— Absolute time	1 (read)	07 (limited qty = 1)	129 (response)	07 (limited qty) (qty = 1)
			2 (write)	07 (limited qty = 1)		
50	3	Time and Date— Absolute time at last recorded time	2 (write)	07 (limited qty = 1)		
51	1	Time and Date CTO— Absolute time, synchronized			129 (response) 130 (unsol. resp)	07 (limited qty) (qty = 1)
51	2	Time and Date CTO— Absolute time, unsynchronized			129 (response) 130 (unsol. resp)	07 (limited qty) (qty = 1)
52	1	Time Delay— Coarse			129 (response)	07 (limited qty) (qty = 1)
52	2	Time Delay— Fine			129 (response)	07 (limited qty) (qty = 1)
60	1	Class Objects— Class 0 data	1 (read) 22 (assign class)	06 (no range, or all)		

ESKOM COPYRIGHT PROTECTED

Level 4 device implementation table - continued

DNP3 OBJECT GROUP & VARIATION			REQUEST Master may issue Outstation shall parse		RESPONSE Master shall parse Outstation may issue	
Group num	Var num	Description	Function codes (dec)	Qualifier codes (hex)	Function codes (dec)	Qualifier codes (hex)
60	2	Class Objects— Class 1 data	1 (read)	06 (no range, or all) 07, 08 (limited qty)		
			20 (enable unsol.) 21 (disable unsol.) 22 (assign class)	06 (no range, or all)		
60	3	Class Objects— Class 2 data	1 (read)	06 (no range, or all) 07, 08 (limited qty)		
			20 (enable unsol.) 21 (disable unsol.) 22 (assign class)	06 (no range, or all)		
60	4	Class Objects— Class 3 data	1 (read)	06 (no range, or all) 07, 08 (limited qty)		
			20 (enable unsol.) 21 (disable unsol.) 22 (assign class)	06 (no range, or all)		
80	1	Internal Indications— Packed format	1 (read)	00, 01 (start-stop)	129 (response)	00, 01 (start-stop)
			2 (write)	00 (start-stop) index=7		
No Object (function code only)			0 (confirm)			
No Object (function code only)			13 (cold restart)			
No Object (function code only)			23 (delay measurement)			
No Object (function code only)			24 (record current time)			

ESKOM COPYRIGHT PROTECTED