DNP3 Device Profile

Based on DNP XML Schema version 2.11.00

Document Name: MGate5119 DNP3 Master Device Profile

Document Description: MGate5119 DNP3 Master Device Profile

Showing both the Device's Capabilities and its Current Configuration

Revision History

Date	Time	Version	Reason for change	Edited by
2021-12-10		1	Version 1.0.0	Lance PH Chen

REFERENCE DEVICE:

1 Device Properties

This document is intended to be used for several purposes, including:

- Identifying the capabilities of a DNP3 device (Master Station or Outstation)

- Recording the settings of a specific instance of a device (parameter settings for a specific instance of the device in the user's total DNP3 estate)

- Matching user requirements to product capabilities when procuring a DNP3 device

The document is therefore structured to show, for each technical feature, the capabilities of the device (or capabilities required by the device when procuring).

It is also structured to show the current value (or setting) of each of the parameters that describe a specific instance of the device. This "current value" may also show a functional limitation of the device. For example when implementing secure

authentication it is not required that all DNP3 devices accept aggressive mode requests during critical exchanges (see Device Profile 1.12.4), in which case a vendor would mark this current value as "No - does not accept aggressive mode requests".

Additionally, the current value may sometimes be used to show a value that a device can achieve because of hardware or software dependencies. Users should note that if an entry in the capabilities column of the Device Profile is grayed-out then there may be information in the current value column that is pertinent to the device's capabilities.

Unless otherwise noted, multiple boxes in the second column below are selected for each parameter to indicate all capabilities supported or required. Parameters without checkboxes in the second column do not have capabilities and are included so that the current value may be shown in the third column.

The items listed in the capabilities column below may be configurable to any of the options selected, or set to a fixed value when the device was designed. Item 1.1.10 contains a list of abbreviations for the possible ways in which the configurable parameters may be set. Since some parameters may not be accessible by each of these methods supported, an abbreviation for the configuration method supported by each parameter is shown in the fourth column of the tables below.

If this document is used to show the current values, the third column should be filled in even if a fixed parameter is selected in the capabilities section ("N/A" may be entered for parameters that are Not Applicable).

If the document is used to show the current values of parameters, then column 3 applies to a single connection between a master and an outstation.

1.1 DEVICE IDENTIFICATION	**Capabilities**	**Current Value**	**If configurable list methods**
1.1.1 Device Function: *Masters send DNP requests, while Outstations send DNP responses. If a single physical device can perform both functions, a separate Device Profile Document must be provided for each function.*	◉ Master ○ Outstation	◉ Master ○ Outstation	
1.1.2 Vendor Name: *The name of the organization*		MOXA	

producing the device. *Note: The current value of this outstation parameter is available remotely using protocol object Group 0 Variation 252.*			
1.1.3 Device Name: *The model and name of the device, sufficient to distinguish it from any other device from the same organization.* *Note: The current value of this outstation parameter is available remotely using protocol object Group 0 Variation 250.*		MGate5119	
1.1.4 Device manufacturer's hardware version string: *Note: The current value of this outstation parameter is available remotely using protocol object Group 0 Variation 243.*		N/A	
1.1.5 Device manufacturer's software version string:		N/A	

Note: The current value of this outstation parameter is available remotely using protocol object Group 0 Variation 242.			
1.1.6 Device Profile Document Version Number: *Version of the Device Profile Document is indicated by a whole number incremented with each new release. This should match the latest version shown in the Revision History at the beginning of this document.*		1	
1.1.7 DNP Levels Supported for: *Indicate each DNP3 Level to which the device conforms fully. For Masters, requests and responses can be indicated independently.*	Masters Only RequestsResponses ☐ ☐ None ☐ ☐ Level 1 ☑ ☑ Level 2 ☐ ☐ Level 3 ☐ ☐ Level 4	For requests: Level 2 For responses: Level 2	
1.1.8 Supported Function Blocks:	☐ Self Address Support ☐ Data Sets ☐ File Transfer ☐ Virtual Terminal ☐ Mapping to IEC 61850 Object Models defined in a DNP3 XML file ☐ Function code 31, activate configuration	Secure Authentication	

	☑ Secure Authentication (if checked then see 1.12)		
1.1.9 Notable Additions: *A brief description intended to quickly identify (for the reader) the most obvious features the device supports in addition to the Highest DNP Level Supported. The complete list of features is described in the Implementation Table.*			
1.1.10 Methods to set Configurable Parameters:	☐ XML - Loaded via DNP3 File Transfer ☐ XML - Loaded via other transport mechanism ☐ Terminal - ASCII Terminal Command Line ☐ Proprietary file loaded via DNP3 File Transfer ☐ Proprietary file loaded via other transport mechanism ☐ Direct - Keypad on device front panel ☐ Factory - Specified when device is ordered ☐ Protocol - Set via DNP3 (e.g. assign class) ☑ Other - explain:	Other,	
1.1.11 DNP3 XML files available On-line: *XML configuration file names that can be read or written through DNP3 File Transfer to a device.*	RdWrFilename / Description of Contents ☐ dnpDP.xml — Complete Device Profile ☐ dnpDPCap.xml — Device Profile Capabilities ☐ dnpDPCfg.xml — Device Profile config values	Rd Wr Filename ☐ dnpDP.xml ☐ dnpDPCap.xml ☐ dnpDPCfg.xml	

A device's currently running configuration is returned by DNP3 on-line XML file read from the device. *DNP3 on-line XML file write to a device will update the device's configuration when the Activate Configuration (function code 31) is received.*			
1.1.12 External DNP3 XML files available Off-line: *XML configuration file names that can be read or written from an external system, typically from a system that maintains the outstation configuration.* *External off-line XML file read permits an XML definition of a new configuration to be supplied from off-line configuration tools.* *External off-line XML file write permits an XML definition of a new configuration to be supplied to*	Rd Wr Filename — Description of Contents ☐ ☐ dnpDP.xml — Complete Device Profile ☐ ☐ dnpDPCap.xml — Device Profile Capabilities ☐ ☐ dnpDPCfg.xml — Device Profile config values	Rd Wr Filename ☐ ☐ dnpDP.xml ☐ ☐ dnpDPCap.xml ☐ ☐ dnpDPCfg.xml	

off-line configuration tools.			
1.1.13 Connections Supported:	☑ Serial (complete section 1.2) ☑ IP Networking (complete section 1.3) ☐ Other, explain	Serial IP Networking	
1.1.14 Conformance Testing: *Where conformance testing has been completed for the outstation or master station, specify the version of the published DNP3 test procedures that was successfully passed. If independently tested, identify the organization that performed the test.*	☐ Self-tested, version ☐ Independently tested, version		

1.2 SERIAL CONNECTIONS	**Capabilities**	**Current Value**	**If configurable list methods**
1.2.1 Port Name: *Name used to reference the communications port defined in this section.*		COM1	
1.2.2 Serial Connection Parameters:	☑ Asynchronous - 8 Data Bits, 1 Start Bit, 1 Stop Bit, No Parity ☑ Other, explain Note: Implemented in Target Layer	AsynchronousOther,	
1.2.3 Baud Rate:	☐ Fixed at ☑ Configurable, range **1** to **115200** ☐ Configurable,	9600	

	selectable from ☐ Configurable, other, describe Note: Implemented in Target Layer		
1.2.4 Hardware Flow Control (Handshaking): *Describe hardware signaling requirements of the interface.* *Where a transmitter or receiver is inhibited until a given control signal is asserted, it is considered to require that signal prior to sending or receiving characters.* *Where a signal is asserted prior to transmitting, that signal will be maintained active until after the end of transmission.* *Where a signal is asserted to enable reception, any data sent to the device when the signal is not active could be discarded.*	☑ None **RS-232 / V.24 / V.28 Options:** Asserts: ☐ RTS Before Tx ☐ DTR Before Tx ☐ RTS Before Rx ☐ DTR Before Rx ☐ Always RTS ☐ Always DTR Requires Before Tx: CTS ☐ Asserted ☐ Deasserted DCD ☐ Asserted ☐ Deasserted DSR ☐ Asserted ☐ Deasserted RI ☐ Asserted ☐ Deasserted ☐ Requires Rx Inactive before Tx Requires Before Rx: CTS ☐ Asserted ☐ Deasserted DCD ☐ Asserted ☐ Deasserted DSR ☐ Asserted ☐ Deasserted RI ☐ Asserted ☐ Deasserted Always Ignores: ☐ CTS ☐ DCD ☐ DSR ☐ RI ☐ Other, explain **RS-422 / V.11 Options:** ☐ Requires Indication before Rx ☐ Asserts Control before Tx	None **RS-232 / V.24 / V.28 Options:** Other, **RS-422 / V.11 Options:** **RS-485Options:** Other,	Proprietary File via Other Mechanism ----------

	☐ Other, explain **RS-485 Options:** ☐ Requires Rx inactive before Tx ☐ Other, explain ☑ Other, explain **Sofware**		
1.2.5 Interval to Request Link Status: *Indicates how often to send Data Link Layer status requests on a serial connection. This parameter is separate from the TCP Keep-alive timer.*	☐ Not Supported ☑ Fixed at seconds ☐ Configurable, range to seconds ☐ Configurable, selectable from seconds ☐ Configurable, other, describe	0 seconds	
1.2.6 Supports DNP3 Collision Avoidance: *Indicates whether an Outstation uses a collision avoidance algorithm.* *Collision avoidance may be implemented by a back-off timer with two parameters that define the back-off time range or by some other vendor-specific mechanism.* *The recommended back-off time is specified as being a fixed minimum delay plus a random delay, where the random delay has a maximum value specified. This defines a range of delay times that are randomly distributed between the minimum value and the minimum plus the maximum of the random value.*	☑ No ☐ Yes, using Back-off time = (Min + Random) method ☐ Other, explain	No	

If a back-off timer is implemented with only a fixed or only a random value, select the Back-off time method and set the parameter that is not supported to "Fixed at 0 ms".			
1.2.7 Receiver Inter-character Timeout: *When serial interfaces with asynchronous character framing are used, this parameter indicates if the receiver makes a check for gaps between characters. (i.e. extensions of the stop bit time of one character prior to the start bit of the following character within a message). If the receiver performs this check and the timeout is exceeded then the receiver discards the current data link frame. A receiver that does not discard data link frames on the basis of inter-character gaps is considered not to perform this check.* *Where no asynchronous serial interface is fitted this parameter is not applicable. In this case none of the options shall be selected.*	☑ Not Checked ☐ No gap permitted ☐ Fixed at bit times ☐ Fixed at ms ☐ Configurable, range to bit times ☐ Configurable, range to ms ☐ Configurable, selectable from bit times ☐ Configurable, selectable from ms ☐ Configurable, other, describe ☐ Variable, explain	Not Checked	
1.2.8 Inter-character gaps in transmission: *When serial interfaces with asynchronous character framing are used, this parameter indicates whether extra delay is ever introduced between characters in the message, and if so,*	☑ None (always transmits with no inter-character gap) ☐ Maximumbit times ☐ Maximumms	None	

the maximum width of the gap. *Where no asynchronous serial interface is fitted this parameter is not applicable. In this case none of the options shall be selected.*			

1.3 IP NETWORKING	**Capabilities**	**Current Value**	**If configurable list methods**
1.3.1 Port Name: *Name used to reference the communications port defined in this section.*			
1.3.2 Type of End Point:	☑ TCP Initiating ☐ TCP Listening ☑ TCP Dual ☑ UDP Datagram	TCP Initiating UDP Datagram	
1.3.3 IP Address of this Device:		192.168.127.254	
1.3.4 Subnet Mask:		255.255.255.0	
1.3.5 Gateway IP Address:			
1.3.6 Accepts TCP Connections or UDP Datagrams from:	☑ Allows all (show as *.*.*.* in 1.3.7) ☐ Limits based on IP address ☑ Limits based on list of IP addresses ☐ Limits based on a wildcard IP address ☐ Limits based on list of wildcard IP addresses ☐ Other, explain	Allows all	
1.3.7 IP Address(es) from which TCP Connections or UDP Datagrams are accepted:			
1.3.8 TCP Listen Port Number:	☐ Not Applicable (Master w/o dual end point) ☐ Fixed at 20,000	20000	

If Outstation or dual end point Master, port number on which to listen for incoming TCP connect requests. Required to be configureable for Masters and recommended to be configurable for Outstations.	☑ Configurable, range **1** to **65535** ☐ Configurable, selectable from ☐Configurable, other, describe		
1.3.9 TCP Listen Port Number of remote device: *If Master or dual end point Outstation, port number on remote device with which to initiate connection. Required to be configurable for Masters and recommended to be configurable for Outstations.*	☐Not Applicable (Outstation w/o dual end point) ☐ Fixed at 20,000 ☑ Configurable, range **1** to **65535** ☐ Configurable, selectable from ☐Configurable, other, describe	20000	
1.3.10 TCP Keep-alive timer: *The time period for the keep-alive timer on active TCP connections.*	☐Timer Disabled ☑ Fixed at **60000**ms ☐ Configurable, range to ms ☐ Configurable, selectable from ms ☐Configurable, other, describe	60000 ms	
1.3.11 Local UDP port: *Local UDP port for sending and/or receiving UDP datagrams. Masters may let system choose an available port. Outstations must use one that is known by the Master.*	☐ Fixed at 20,000 ☐ Configurable, range to ☐ Configurable, selectable from ☐Configurable, other, describe ☐Let system choose (Master only)	20000	
1.3.12 Destination UDP port for DNP3 Requests (Masters Only):	☐ Fixed at 20,000 ☑ Configurable, range **1** to **65535** ☐ Configurable, selectable from ☐Configurable, other, describe	20000	
1.3.13 Destination UDP port for initial unsolicited	☑ None ☐ Fixed at 20,000 ☐ Configurable, range to	None	

null responses (UDP only Outstations): *The destination UDP port for sending initial unsolicited Null response.*	☐ Configurable, selectable from ☐Configurable, other, describe		
1.3.14 Destination UDP port for responses (UDP only Outstations): *The destination UDP port for sending all responses other than the initial unsolicited Null response.*	☐ None ☑ Fixed at 20,000 ☑ Configurable, range **1** to **65535** ☐ Configurable, selectable from ☐Configurable, other, describe ☐Use local port number (as specified in 1.3.11)	20000	Proprietary File via Other Mechanism ----------
1.3.15 Multiple outstation connections (Masters only): *Indicates whether multiple outstation connections are supported.*	☑ Supports multiple outstations (Masters only)	True	
1.3.16 Multiple master connections (Outstations only): *Indicates whether multiple master connections are supported and the method that can be used to establish connections.*	☐ Supports multiple masters (Outstations only) If supported, the following methods may be used: ☐Method 1 (based on IP address) - required ☐Method 2 (based on IP port number) - recommended ☐Method 3 (browsing for static data) - optional	Not supported	
1.3.17 Time synchronization support:	☐DNP3 LAN procedure (function code 24) ☑DNP3 Write Time (not recommended over LAN) ☐Other, explain ☐Not Supported	Write Time	

1.4 LINK LAYER	**Capabilities**	**Current Value**	**If configurable list methods**
1.4.1 Data Link Address:		3	

Indicates if the link address is configurable over the entire valid range of 0 to 65,519. Data link addresses 0xFFF0 through 0xFFFF are reserved for broadcast or other special purposes.	☐ Fixed at ☐ Configurable, range to ☐ Configurable, selectable from ☐ Configurable, other, describe		
1.4.2 DNP3 Source Address Validation: *Indicates whether the Outstation will filter out requests not from a specific source address.*	☑ Never ☐ 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	Never	
1.4.3 DNP3 Source Address (es) expected when Validation is Enabled: *Selects the allowed source address(es)*	☐ Configurable to any 16 bit DNP Data Link Address value ☑ Configurable, range **0** to **65519** ☐ Configurable, selectable from ☐ Configurable, other, describe	4	
1.4.4 Self Address Support using address 0xFFFC: *If an Outstation receives a message with a destination address of 0xFFFC it shall respond normally with its own source address. It must be possible to diasble this feature if supported.*	☑ Yes (only allowed if configurable) ☑ No	No	
1.4.5 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).*	☑ Never ☑ Always ☐ Sometimes, explain	Never	
1.4.6 Data Link Layer Confirmation Timeout: *This timeout applies to any secondary data link message that requires a confirm or*	☐ None ☐ Fixed at ms ☑ Configurable, range **0** to **65535**ms ☐ Configurable, selectable from ms	2000ms	

response (link reset, link status, user data, etc).	☐ Configurable, other, describe ☐ Variable, explain		
1.4.7 Maximum Data Link Retries: *The number of times the device will retransmit a frame that requests Link Layer confirmation.*	☐ None ☐ Fixed at ☑ Configurable, range **0** to **5** ☐ Configurable, selectable from ☐ Configurable, other, describe	1	
1.4.8 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 ☑ Configurable, range **28** to **292** ☐ Configurable, selectable from ☐ Configurable, other, describe	292	
1.4.9 Maximum number of octets that can be Received in a Data Link Frame: *This number includes the CRCs. With a field length of 255, the maximum size would be 292. The device must be able to receive 292 octets to be compliant.*	☐ Fixed at ☑ Configurable, range **28** to **292** ☐ Configurable, selectable from ☐ Configurable, other, describe	292	

1.5 APPLICATION LAYER	**Capabilities**	**Current Value**	**If configurable list methods**
1.5.1 Maximum number of octets Transmitted in an Application Layer Fragment other than File Transfer: *This size does not include any transport or frame octets.* *- Masters must provide a setting less than or equal to 249 to be compliant.* *- Outstations must provide a setting less than or equal to 2048 to be compliant.*	☐ Fixed at ☑ Configurable, range **256** to **65535** ☐ Configurable, selectable from ☐ Configurable, other, describe	2048	

Note: The current value of this outstation parameter is available remotely using protocol object Group 0 Variation 240.			
1.5.2 Maximum number of octets Transmitted in an Application Layer Fragment containing File Transfer:	☑ Same as 1.5.1 ☐ Fixed at ☐ Configurable, range to ☐ Configurable, selectable from ☐ Configurable, other, describe	2048	
1.5.3 Maximum number of octets that can be received in an Application Layer Fragment: *This size does not include any transport or frame octets.* *- Masters must provide a setting greater than or equal to 2048 to be compliant.* *- Outstations must provide a setting greater than or equal to 249 to be compliant.* *Note: The current value of this outstation parameter is available remotely using protocol object Group 0 Variation 241.*	☐ Fixed at ☑ Configurable, range **256** to **65535** ☐ Configurable, selectable from ☐ Configurable, other, describe	2048	
1.5.4 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 **0** to **65535**ms ☐ Configurable, selectable from ms ☐ Configurable, other, describe ☐ Variable, explain	10000ms	
1.5.5 Maximum number of objects	☐ Fixed at (enter 0 if controls are not supported for CROB)	Variable	

allowed in a single control request for CROB (Group 12): *Note: The current value of this outstation parameter is available remotely using protocol object Group 0 Variation 216.*	☐ Configurable, range to ☐ Configurable, selectable from ☐ Configurable, other, describe ☑ Variable, explain **Depends on Tx Fragment Size** ☐ The number of objects that can be contained in a fragment (as specified in 1.5.3)		
1.5.6 Maximum number of objects allowed in a single control request for Analog Outputs (Group 41):	☐ Fixed at (enter 0 if controls are not supported for Analog Outputs) ☐ Configurable, range to ☐ Configurable, selectable from ☐ Configurable, other, describe ☑ Variable, explain **Depends on Tx Fragment Size** ☐ The number of objects that can be contained in a fragment (as specified in 1.5.3)	Variable	
1.5.7 Maximum number of objects allowed in a single control request for Data Sets (Groups 85, 86, 87):	☐ Fixed at (enter 0 if controls are not supported for Data Sets) ☐ Configurable, range to ☐ Configurable, selectable from ☐ Configurable, other, describe ☑ Variable, explain **Depends on Tx Fragment Size** ☐ The number of objects that can be contained in a fragment (as specified in 1.5.3)	Variable	
1.5.8 Supports mixed object groups (AOBs, CROBs and Data Sets) in the same control request:	☐ Not applicable - controls are not supported ☑ Yes ☐ No	Yes	
1.5.9 Control Status Codes Supported: *Indicates which control status codes are supported by the device:* *- Masters must indicate which control status codes they accept in outstation responses.* *- Outstations must indicate which control*	☑ 1 - TIMEOUT ☑ 2 - NO_SELECT ☑ 3 - FORMAT_ERROR ☑ 4 - NOT_SUPPORTED ☑ 5 - ALREADY_ACTIVE ☑ 6 - HARDWARE_ERROR ☑ 7 - LOCAL ☑ 8 - TOO_MANY_OBJS ☑ 9 - NOT_AUTHORIZED ☑ 10 - AUTOMATION_INHIBIT		

status codes they generate in responses. *Control status code 0 (success) must be supported by Masters and Outstations.*	☑ 11 - PROCESSING_LIMITED ☑ 12 - OUT_OF_RANGE ☑ 13 - DOWNSTREAM_LOCAL ☑ 14 - ALREADY_COMPLETE ☑ 15 - BLOCKED ☑ 16 - CANCELLED ☑ 17 - BLOCKED_OTHER_MASTER ☑ 18 - DOWNSTREAM_FAIL ☐ 126 - RESERVED ☑ 127 - UNDEFINED		

1.6 FILL OUT THE FOLLOWING ITEMS FOR MASTERS ONLY	**Capabilities**	**Current Value**	**If configurable list methods**
1.6.1 Timeout waiting for Complete Application Layer Responses (ms): *Timeout on Master if all fragments of a response message are not received in the specified time.*	☐ None ☐ Fixed at ms ☑ Configurable, range **0** to **65535**ms ☐ Configurable, selectable from ms ☐ Configurable, other, describe ☐ Variable, explain	10000ms	
1.6.2 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 must never cause a Master to retransmit time sync messages.*	☑ None ☐ Fixed at ☐ Configurable, range to ☐ Configurable, selectable from ☐ Configurable, other, describe ☐ Variable, explain	None	
1.6.3 Timeout waiting for First or Next Fragment of an Application Layer Response: *Timeout between a request and the first fragment of a response, or between subsequent fragments of the same response, or between an Application Layer*	☑ None ☐ Fixed at ms ☑ Configurable, range **0** to **2147483647**ms ☐ Configurable, selectable from ms ☐ Configurable, other, describe ☐ Variable, explain	None	

Confirmation and a subsequent fragment.			
1.6.4 Issuing controls to off-line devices: *Indicates if the Master issues control requests to devices that are thought to be off-line (i.e. the Master has not seen responses to previous Master requests).*	☐ Not applicable - controls are not supported ☑ Yes ☐ No	Yes	
1.6.5 Issuing controls to off-scan devices: *Indicates if the Master issues control requests to devices that are currently off-scan (i.e. the Master has been configured not to issue poll requests to the device).*	☐ Not applicable - controls are not supported ☑ Yes ☐ No	Yes	
1.6.6 Maximum Application Layer Retries for Control Select Messages (same sequence number): *Indicates the number of times a Master will retransmit an application layer control select request message if a response is not received - using the same message sequence number.*	☑ None (required) ☐ Fixed at ☐ Configurable, range to ☐ Configurable, selectable from ☐ Configurable, other, describe ☐ Variable, explain	None	
1.6.7 Maximum Application Layer Retries for Control Select Messages (new sequence number): *Indicates the number of times a Master will retransmit an application layer control select request message if a response is not received - using a new message sequence number.*	☑ None (required) ☐ Fixed at ☐ Configurable, range to ☐ Configurable, selectable from ☐ Configurable, other, describe ☐ Variable, explain	None	

1.7 FILL OUT THE FOLLOWING ITEMS FOR OUTSTATIONS ONLY	**Capabilities**	**Current Value**	**If configurable list methods**

This section is not included in this Profile.	

1.8 OUTSTATION UNSOLICITED RESPONSE SUPPORT	Capabilities	Current Value	If configurable list methods
This section is not included in this Profile.			

1.9 OUTSTATION UNSOLICITED RESPONSE TRIGGER CONDITIONS	Capabilities	Current Value	If configurable list methods
This section is not included in this Profile.			

1.10 OUTSTATION PERFORMANCE	Capabilities	Current Value	If configurable list methods
This section is not included in this Profile.			

1.11 INDIVIDUAL FIELD OUTSTATION PARAMETERS	Value of Current Setting	If configurable list methods
This section is not included in this Profile.		

1.12 SECURITY PARAMETERS	Capabilities	Current Value	If configurable list methods
1.12.1 DNP3 device support for secure authentication: *The support for secure authentication is optional in DNP3 devices. Section 1.1.8 indicates if the device supports secure authentication.* *If the device does not support secure authentication then ignore the rest of this section.* *If the device does support secure authentication then specify the version(s) that are supported in the device. The version number is an integer value defined in the DNP3 Specification. The Secure Authentication procedure defined in IEEE 1815-2010 is version 2. The Secure Authentication*	Supported version(s): ☐ Fixed at ☑ Configurable, selectable from **5**	Version: 5	

procedure defined in IEEE 1815-2012 is version 5.			
1.12.2 Maximum number of users: *The secure authentication algorithm provides support for multiple users. The device must support details for each user (update keys, session keys, etc). A user is identified by a 16-bit user number, allowing a maximum of 65535 users. Devices are not mandated to support this number of potential users. Indicate here the actual limit to the number of simultaneous users that can be supported.*	☑ Fixed at **1** ☐ Configurable, range to	Maximum number of users supported: 1	
1.12.3 Security message response timeout: *Authentication of critical messages may involve additional message exchanges (challenges and responses) which can require an extension to the normal DNP3 message response timeout. This timeout specifies an additional time to be used when the extra security transactions are involved. The maximum allowable timeout extension should not exceed 120 seconds.*	☐ Fixed at ms ☑ Configurable, range **0** to **120**ms ☐ Configurable, selectable from ms ☐ Configurable, other, describe	2 ms	
1.12.4 Aggressive mode of operation (receive): *DNP3 devices may (optionally) accept "aggressive" mode requests, where challenge data used for authentication is appended to a critical message rather than needing to be solicited via a separate message exchange.*		◉ Yes, accepts aggressive mode requests ○ No, does not accept aggressive mode requests	
1.12.5 Aggressive mode of operation (issuing): *DNP3 devices must support the issuing of "aggressive" mode of operation, where challenge data*		◉ Yes, issues aggressive mode requests ○ No,	

used for authentication is appended to a critical message rather than needing to be solicited via a separate message exchange. Specific instances of devices may have the use of aggressive mode switched off.		does not issue aggressive mode requests	
1.12.6 Session key change interval: *To counter an attack that compromises the session key, the session key is changed by the master at regular intervals. Outstation devices invalidate the current set of session keys if they have not been changed by the master station after a period of twice this configured value.* *To accommodate systems with infrequent communications, this change interval can be disabled and just the session key change message count used (see 1.12.7)*	☑ Can be disabled When enabled ☑ Configurable, range **0** to **7200**seconds	Enabled 900 seconds	
1.12.7 Session key change message count: *In addition to changing the session key at regular intervals, the key shall also be changed after a specified number of messages have been exchanged. The maximum allowable value for this message count is 10,000*	☑ Configurable, range **0** to **10000**	1000	
1.12.8 Maximum error count (SAv2 only): *To assist in countering denial of service attacks, a DNP3 device shall stop replying with error codes after a number of successive authentication failures. This error count has a maximum value of 10. Setting the error count to zero inhibits all error messages.* *See 1.12.21 for error counts when using SAv5*	☑ Not applicable (not using SAv2) ☐ Configurable, range to	N/A	
	☑ SHA-1 (truncated to the leftmost 4 octets)		Proprietary File via

1.12.9 MAC algorithm requested in a challenge exchange: *Part of the authentication message is hashed using an MAC algorithm. Secure Authentication version 2 specifies that DNP3 devices must support SHA-1 and may optionally support SHA-256 for this hashing process. Secure Authentication version 5 specifies that SHA-256 is the default. The output of the MAC algorithm is truncated (the resulting length dependant on the media being used).*	☑ SHA-1 (truncated to the leftmost 8 octets) ☑ SHA-1 (truncated to the leftmost 10 octets) ☑ SHA-256 (truncated to the leftmost 8 octets) ☑ SHA-256 (truncated to the leftmost 16 octets) ☑ AES-GMAC ☐ Other, explain:	SHA-256 (16)	Other Mechanism ----------
1.12.10 Key-wrap algorithm to encrypt session keys: *During the update of a session key, the key is encrypted using AES-128 or optionally using other algorithms.*	☑ AES-128 ☑ AES-256 ☐ Other, explain:	AES-128	Proprietary File via Other Mechanism ----------
1.12.11 Cipher Suites used with DNP implementations using TLS: *When TLS is supported, DNP3 Secure Authentication mandates the support of TLS_RSA_WITH_AES_128_SHA. The specification has a number of recommended cipher suite combinations. Indicate the supported Cipher Suites for implementations using TLS.*	☑ Not relevant - TLS is not used ☐ TLS_RSA encrypted with AES128 ☐ TLS_RSA encrypted with RC4_128 ☐ TLS_RSA encrypted with 3DES_EDE_CBC ☐ TLS_DH, signed with DSS, encrypted with 3DES_EDE_CBC ☐ TLS_DH, signed with RSA, encrypted with 3DES_EDE_CBC ☐ TLS_DHE, signed with DSS, encrypted with 3DES_EDE_CBC ☐ TLS_DHE, signed with RSA, encrypted with 3DES_EDE_CBC ☐ TLS_DH, signed with DSS, encrypted with AES128 ☐ TLS_DH, signed with DSS, encrypted with AES256 ☐ TLS_DH encrypted	Not relevant	

	with AES128 ☐ TLS_DH encrypted with AES256 ☐ Other, explain: Note: Implemented in Target Layer		
1.12.12 Change cipher request timeout: *Implementations using TLS shall terminate the connection if a response to a change cipher request is not seen within this timeout period.*	☑ Not relevant - TLS is not used ☐ Fixed at ☐ Configurable, range to ☐ Configurable, selectable from ☐ Configurable, other, describe Note: Implemented in Target Layer	Not relevant	
1.12.13 Number of Certificate Authorities supported: *Implementations using TLS shall support at least 4 Certificate Authorities. Indicate the number supported.*		0	
1.12.14 Certificate Revocation check time: *Implementations using TLS shall evaluate Certificate Revocation Lists on a periodic basis, terminating a connection if a certificate is revoked.*	☑ Not relevant - TLS is not used ☐ Fixed at hours ☐ Configurable, range to hours ☐ Configurable, selectable from hours ☐ Configurable, other, describe Note: Implemented in Target Layer	Not relevant	
1.12.15 Additional critical function codes: *The DNP3 specification defines those messages with specific function codes that are critical and must be used as part of a secure authentication message exchange. Messages with other function codes are optional and changes to this list should be*	Additional function codes that are to be considered as "critical": ☐ 0 (Confirm) ☐ 1 (Read) ☐ 7 (Immediate freeze) ☐ 8 (Immediate freeze - no ack) ☐ 9 (Freeze-and-clear) ☐ 10 (Freeze-and-clear - no ack)		

noted here. *Note: Secure Authentication version 5 defines additional functions as critical that were not considered critical in version 2. These are shown in the next column annotated with "V2 only".*	☐ 11 (Freeze-at-time) ☐ 12 (Freeze-at-time - no ack) ☐ 22 (Assign Class) ☐ 23 (Delay Measurement) ☐ 25 (Open File) - V2 only ☐ 26 (Close File) - V2 only ☐ 27 (Delete File) - V2 only ☐ 28 (Get File Info) - V2 only ☐ 30 (Abort File) - V2 only ☑ 129 (Response) ☑ 130 (Unsolicited Response)		
1.12.16 Other critical fragments: *Other critical transactions can be defined and should be detailed here. Examples could be based on time (for example: the first transaction after a communications session is established). Other examples could be based on specific data objects (for example: the reading of specific data points).*			
1.12.17 Support for remote update key changes: *Devices implementing secure authentication version 5 or later have the option to support remote update key changes. If remote update key change is supported then the procedure using symmetric cryptography is mandatory. Additional support for the procedure using asymmetric (public key) cryptography is optional.*	☐ Remote update key change by symmetric cryptography Supported key change methods: ☐ AES-128 key wrap with SHA-1-HMAC ☐ AES-256 key wrap with SHA-256-HMAC ☐ AES-256 key wrap with AES-GMAC ☐ Remote update key change by asymmetric cryptography		

	Supported key change methods: ☐RSAES-OAEP-1024/SHA-1 with DSA SHA-1 and SHA-1-HMAC ☐RSAES-OAEP-2048/SHA-256 with DSA SHA-256 and SHA-256-HMAC ☐RSAES-OAEP-3072/SHA-256 with DSA SHA-256 and SHA-256-HMAC ☐RSAES-OAEP-2048/SHA-256 with DSA SHA-256 and AES-GMAC ☐RSAES-OAEP-3072/SHA-256 with DSA SHA-256 and AES-GMAC		
1.12.18 "Default" user credentials are permitted to expire:	☐Yes ☐No		
1.12.19 Secure Authentication enabled:	☑Configurable, selectable from On and Off ☐Always On	Off	
1.12.20 Length of the challenge data: *The length of the challenge data used when setting up session keys shall be at a minimum 4 octets. The maximum length can exceed 32 octets but if greater than 32 it must be configurable down to 32 octets.*	☐ Fixed at octets ☑ Configurable, range **4** to **64**octets ☐ Configurable, selectable from octets ☐Configurable, other, describe	4 octets	
1.12.21 Maximum statistic counts (SAv5): *The SAv5 specification allows event objects to be generated when the statistics reach certain threshold values. Indicate here how these thresholds are set if using SAv5.*	**Max Authentication Failures:** ☐Not applicable (not using SAv5) ☑ Configurable, range **1** to **65535** **Max Reply Timeouts:** ☐Not applicable (not	Max Auth Fails: 5 Max Reply T/O: 3	

Note that "Max Rekeys Due to Restarts" only applies to Masters and can be omitted from the Device Profile for Outstations.	using SAv5) ☑ Configurable, range **1** to **65535** **Max Authentication Rekeys:** ☐Not applicable (not using SAv5) ☑ Configurable, range **1** to **65535** **Max Error Messages Sent:** ☐Not applicable (not using SAv5) ☑ Configurable, range **1** to **65535** **Max Rekeys Due to Restarts:** ☐Not applicable (not using SAv5) ☑ Configurable, range **1** to **65535**	Max Auth Rekeys: 3 Max Error Msg: 4 Max Restart Rekeys: 2	

1.13 BROADCAST FUNCTIONALITY	**Capabilities**	**Current Value**	**If configurable list methods**
This section is not included in this Profile.			

2 Mapping to IEC 61850 Object Models

This optional section allows each configuration parameter or point in the DNP Data map to be tied to an attribute in the IEC 61850 object models.

Earlier versions of this section (up to version 2.07) used mappings based on an "access point" (section 2.1.1 and then a series of XPath references (section 2.1.2). Section 2.1.2 has been superseded in version 2.08 onwards with mappings defined using either predefined rules (section 2.1.3) or specified as an equation (section 2.1.4). The list of pre-defined rules is found in the IEEE 1815-1 document.

TREE MPPING BETWEEN DNP3 AND IEC 61850 OBJECTS
2.1.3 Rule based mapping Use this element when mapping to/from iec61850 using one of the predefined rules in IEEE 1815.1 Mapping is bi-directional

This section is not included in this Profile.
2.1.4 Equation based mapping Use this element when mapping to/from iec61850 using an equation to map 0 or more input parameters to a single output parameter. Direction of mapping is determined by the variable on the left hand side of the equation.
This section is not included in this Profile.

3 Capabilities and Current Settings for Device Database (Outstation only)

The following tables identify the capabilities and current settings for each DNP3 data type. Details defining the data points available in the device are shown in part 5 of this Device Profile.

This section is not included in this Master Station Profile.

4 Implementation Table

The following implementation table identifies which object groups and variations, function codes and qualifiers the device supports in both requests and responses. The *Request* columns identify all requests that may be sent by a Master, or all requests that must be parsed by an Outstation. The *Response* columns identify all responses that must be parsed by a Master, or all responses that may be sent by an Outstation.

DNP OBJECT GROUP & VARIATION			**REQUEST Master may issue Outstation must parse**		**RESPONSE Master must parse Outstation may issue**	
Object Group Number	**Variation Number**	**Description**	**Function Codes (dec)**	**Qualifier Codes (hex)**	**Function Codes (dec)**	**Qualifier Codes (hex)**
1	0	Binary Input - any variation	1 *(read)*	00, 01 *(start-stop)*, 06 *(no range, or all)*, 07, 08 *(limited qty)*,		

				17, 27, 28 *(index)*		
2	0	Binary Input Change Event - any variation	1 *(read)*	06 *(no range, or all)*, 07, 08 *(limited qty)*		
2	1	Binary Input Change Event - without time	1 *(read)*	06 *(no range, or all)*, 07, 08 *(limited qty)*	*(Response)*	17, 28 *(index)*
2	1	Binary Input Change Event - without time			*(Unsol. Resp.)*	17, 28 *(index)*
2	2	Binary Input Change Event - with absolute time	1 *(read)*	06 *(no range, or all)*, 07, 08 *(limited qty)*	*(Response)*	17, 28 *(index)*
2	2	Binary Input Change Event - with absolute time			*(Unsol. Resp.)*	17, 28 *(index)*
2	3	Binary Input Change Event - with relative time	1 *(read)*	06 *(no range, or all)*, 07, 08 *(limited qty)*	*(Response)*	17, 28 *(index)*
2	3	Binary Input Change Event - with relative time			*(Unsol. Resp.)*	17, 28 *(index)*
10	0	Binary Output - any variation	1 *(read)*	00, 01 *(start-stop)*, 06 *(no range, or all)*, 07, 08 *(limited qty)*, 17, 28 *(index)*		
10	1	Binary Output - packed format	1 *(read)*	00, 01 *(start-stop)*, 06 *(no range, or all)*, 07, 08	*(Response)*	00, 01 *(start-stop)*, 17, 28 *(index)*

				(limited qty), 17, 28 *(index)*		
10	2	Continuous Control - output status with flags	1*(read)*	00, 01 *(start-stop)*, 06 *(no range, or all)*, 07, 08 *(limited qty)*, 17, 28 *(index)*	*(Response)*	00, 01 *(start-stop)*, 17, 28 *(index)*
12	1	Binary Output Command (CROB) - control relay output block	3*(select)*	17, 27, 28 *(index)*	*(Response)*	echo of request
12	1	Binary Output Command (CROB) - control relay output block	4*(operate)*	17, 27, 28 *(index)*	*(Response)*	echo of request
12	1	Binary Output Command (CROB) - control relay output block	5*(direct op.)*	17, 27, 28 *(index)*	*(Response)*	echo of request
12	1	Binary Output Command (CROB) - control relay output block	6*(direct op, no ack)*	17, 27, 28 *(index)*	*(Response)*	echo of request
20	0	Counter - any variation	1*(read)*	00, 01 *(start-stop)*, 06 *(no range, or all)*, 07, 08 *(limited qty)*, 17, 27, 28 *(index)*		
20	0	Counter - any variation	7*(freeze)*	00, 01 *(start-stop)*, 06 *(no range, or all)*		
20	0	Counter - any variation	8*(freeze, no ack)*	00, 01 *(start-stop)*, 06 *(no*		

				range, or all)		
20	0	Counter - any variation	9*(freeze & clear)*	00, 01 *(start-stop)*, 06 *(no range, or all)*		
20	0	Counter - any variation	10*(frz & clr, no ack)*	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)*, 07, 08 *(limited qty)*, 17, 27, 28 *(index)*	*(Response)*	00, 01 *(start-stop)*, 17, 28 *(index)*
20	2	Counter - 16-bit with flag	1*(read)*	00, 01 *(start-stop)*, 06 *(no range, or all)*, 07, 08 *(limited qty)*, 17, 27, 28 *(index)*	*(Response)*	00, 01 *(start-stop)*, 17, 28 *(index)*
20	5	Counter - 32-bit without flag	1*(read)*	00, 01 *(start-stop)*, 06 *(no range, or all)*, 07, 08 *(limited qty)*, 17, 27, 28 *(index)*	*(Response)*	00, 01 *(start-stop)*, 17, 28 *(index)*
20	6	Counter - 16-bit without flag	1*(read)*	00, 01 *(start-stop)*, 06 *(no range, or all)*, 07, 08	*(Response)*	00, 01 *(start-stop)*, 17, 28 *(index)*

				(limited qty), 17, 27, 28 *(index)*		
21	0	Frozen Counter - any variation	1 *(read)*	00, 01 *(start-stop)*, 06 *(no range, or all)*, 07, 08 *(limited qty)*, 17, 27, 28 *(index)*		
21	1	Frozen Counter - 32-bit with flag	1 *(read)*	00, 01 *(start-stop)*, 06 *(no range, or all)*, 07, 08 *(limited qty)*, 17, 27, 28 *(index)*	*(Response)*	00, 01 *(start-stop)*, 17, 28 *(index)*
21	2	Frozen Counter - 16-bit with flag	1 *(read)*	00, 01 *(start-stop)*, 06 *(no range, or all)*, 07, 08 *(limited qty)*, 17, 27, 28 *(index)*	*(Response)*	00, 01 *(start-stop)*, 17, 28 *(index)*
21	9	Frozen Counter - 32-bit without flag	1 *(read)*	00, 01 *(start-stop)*, 06 *(no range, or all)*, 07, 08 *(limited qty)*, 17, 27, 28 *(index)*	*(Response)*	00, 01 *(start-stop)*, 17, 28 *(index)*
21	10	Frozen Counter - 16-bit without flag	1 *(read)*	00, 01 *(start-stop)*, 06 *(no range, or*	*(Response)*	00, 01 *(start-stop)*, 17, 28 *(index)*

				all), 07, 08 *(limited qty)*, 17, 27, 28 *(index)*		
22	0	Counter Change Event - any variation	1 *(read)*	06 *(no range, or all)*, 07, 08 *(limited qty)*		
22	1	Counter Change Event - 32-bit with flag	1 *(read)*	06 *(no range, or all)*, 07, 08 *(limited qty)*	*(Response)*	17, 28 *(index)*
22	1	Counter Change Event - 32-bit with flag			*(Unsol. Resp.)*	17, 28 *(index)*
22	2	Counter Change Event - 16-bit with flag	1 *(read)*	06 *(no range, or all)*, 07, 08 *(limited qty)*	*(Response)*	17, 28 *(index)*
22	2	Counter Change Event - 16-bit with flag			*(Unsol. Resp.)*	17, 28 *(index)*
30	0	Analog Input - any variation	1 *(read)*	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)*, 07, 08 *(limited qty)*, 17, 27, 28 *(index)*	*(Response)*	00, 01 *(start-stop)*, 17, 28 *(index)*
30	2	Analog Input - 16-bit with flag	1 *(read)*	00, 01 *(start-stop)*, 06 *(no range, or all)*, 07, 08 *(limited*	*(Response)*	00, 01 *(start-stop)*, 17, 28 *(index)*

				qty), 17, 27, 28 *(index)*		
30	3	Analog Input - 32-bit without flag	1 *(read)*	00, 01 *(start-stop)*, 06 *(no range, or all)*, 07, 08 *(limited qty)*, 17, 27, 28 *(index)*	*(Response)*	00, 01 *(start-stop)*, 17, 28 *(index)*
30	4	Analog Input - 16-bit without flag	1 *(read)*	00, 01 *(start-stop)*, 06 *(no range, or all)*, 07, 08 *(limited qty)*, 17, 27, 28 *(index)*	*(Response)*	00, 01 *(start-stop)*, 17, 28 *(index)*
32	0	Analog Input Change Event - any variation	1 *(read)*	06 *(no range, or all)*, 07, 08 *(limited qty)*		
32	1	Analog Input Change Event - 32-bit without time	1 *(read)*	06 *(no range, or all)*, 07, 08 *(limited qty)*	*(Response)*	17, 28 *(index)*
32	1	Analog Input Event – 32-bit without time			*(Unsol. Resp.)*	17, 28 *(index)*
32	2	Analog Input Change Event - 16-bit without time	1 *(read)*	06 *(no range, or all)*, 07, 08 *(limited qty)*	*(Response)*	17, 28 *(index)*
32	2	Analog Input Change Event - 16-bit without time			*(Unsol. Resp.)*	17, 28 *(index)*
33	0	Frozen Analog Input Change Event - any variation	1 *(read)*	06 *(no range, or all)*, 07, 08		

				(limited qty)		
33	1	Frozen Analog Input Change Event - 32-bit without time	1 *(read)*	06 *(no range, or all)*, 07, 08 *(limited qty)*	*(Response)*	17, 28 *(index)*
33	1	Frozen Analog Input Event – 32-bit without time			*(Unsol. Resp.)*	17, 28 *(index)*
33	2	Frozen Analog Input Change Event - 16-bit without time	1 *(read)*	06 *(no range, or all)*, 07, 08 *(limited qty)*	*(Response)*	17, 28 *(index)*
33	2	Frozen Analog Input Change Event - 16-bit without time			*(Unsol. Resp.)*	17, 28 *(index)*
33	3	Frozen Analog Input Change Event - 32-bit with time	1 *(read)*	06 *(no range, or all)*, 07, 08 *(limited qty)*	*(Response)*	17, 28 *(index)*
33	3	Frozen Analog Input Change Event - 32-bit with time			*(Unsol. Resp.)*	17, 28 *(index)*
33	4	Frozen Analog Input Change Event - 16-bit with time	1 *(read)*	06 *(no range, or all)*, 07, 08 *(limited qty)*	*(Response)*	17, 28 *(index)*
33	4	Frozen Analog Input Change Event - 16-bit with time			*(Unsol. Resp.)*	17, 28 *(index)*
33	5	Frozen Analog Input Change Event - single-precision, floating-point without time	1 *(read)*	06 *(no range, or all)*, 07, 08 *(limited qty)*	*(Response)*	17, 28 *(index)*
33	5	Frozen Analog Input Change Event - single-precision, floating-point without time			*(Unsol. Resp.)*	17, 28 *(index)*
33	6	Frozen Analog Input Change Event - double-precision,	1 *(read)*	06 *(no range, or all)*,	*(Response)*	17, 28 *(index)*

		floating-point without time		07, 08 *(limited qty)*		
33	6	Frozen Analog Input Change Event - double-precision, floating-point without time			*(Unsol. Resp.)*	17, 28 *(index)*
33	7	Frozen Analog Input Change Event - single-precision, floating-point with time	1*(read)*	06 *(no range, or all)*, 07, 08 *(limited qty)*	*(Response)*	17, 28 *(index)*
33	7	Frozen Analog Input Change Event - single-precision, floating-point with time			*(Unsol. Resp.)*	17, 28 *(index)*
33	8	Frozen Analog Input Change Event - double-precision, floating-point with time	1*(read)*	06 *(no range, or all)*, 07, 08 *(limited qty)*	*(Response)*	17, 28 *(index)*
33	8	Frozen Analog Input Change Event - double-precision, floating-point with time			*(Unsol. Resp.)*	17, 28 *(index)*
34	0	Analog Input Deadband - any variation	1*(read)*	00, 01 *(start-stop)*, 06 *(no range, or all)*, 07, 08 *(limited qty)*, 17, 27, 28 *(index)*		
34	1	Analog Input Deadband - 16-bit	1*(read)*	00, 01 *(start-stop)*, 06 *(no range, or all)*, 07, 08 *(limited qty)*, 17, 27, 28 *(index)*	*(Response)*	00, 01 *(start-stop)*, 17, 28 *(index)*
34	1		2*(write)*			

		Analog Input Deadband - 16-bit		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)*, 07, 08 *(limited qty)*, 17, 27, 28 *(index)*	*(Response)*	00, 01 *(start-stop)*, 17, 28 *(index)*
34	2	Analog Input Deadband - 32-bit	2*(write)*	00, 01 *(start-stop)*, 17, 28 *(index)*		
34	3	Analog Input Deadband - single-precision, floating-point	1*(read)*	00, 01 *(start-stop)*, 06 *(no range, or all)*, 07, 08 *(limited qty)*, 17, 27, 28 *(index)*	*(Response)*	00, 01 *(start-stop)*, 17, 28 *(index)*
34	3	Analog Input Deadband - single-precision, floating-point	2*(write)*	00, 01 *(start-stop)*, 17, 28 *(index)*		
40	0	Analog Output Status - any variation	1*(read)*	00, 01 *(start-stop)*, 06 *(no range, or all)*, 07, 08 *(limited qty)*, 17, 27, 28 *(index)*		
40	0	Analog Output Status - any variation	22*(assign class)*	00, 01 *(start-stop)*, 06 *(no range, or*		

				all), 07, 08 *(limited qty)*, 17, 27, 28 *(index)*		
40	1	Analog Output Status - 32-bit with flag	1*(read)*	00, 01 *(start-stop)*, 06 *(no range, or all)*, 07, 08 *(limited qty)*, 17, 27, 28 *(index)*	*(Response)*	00, 01 *(start-stop)*, 17, 28 *(index)*
40	2	Analog Output Status - 16-bit with flag	1*(read)*	00, 01 *(start-stop)*, 06 *(no range, or all)*, 07, 08 *(limited qty)*, 17, 27, 28 *(index)*	*(Response)*	00, 01 *(start-stop)*, 17, 28 *(index)*
40	3	Analog Output Status - single-precision, floating-point with flag	1*(read)*	00, 01 *(start-stop)*, 06 *(no range, or all)*, 07, 08 *(limited qty)*, 17, 27, 28 *(index)*	*(Response)*	00, 01 *(start-stop)*, 17, 28 *(index)*
40	4	Analog Output Status - double-precision, floating-point with flag	1*(read)*	00, 01 *(start-stop)*, 06 *(no range, or all)*, 07, 08 *(limited qty)*, 17, 27, 28 *(index)*	*(Response)*	00, 01 *(start-stop)*, 17, 28 *(index)*
41	0	Analog Output Block - any variation	22*(assign class)*	00, 01 *(start-stop)*,		

				06 *(no range, or all)*, 07, 08 *(limited qty)*, 17, 27, 28 *(index)*		
41	1	Analog Output Block - 32-bit	3*(select)*	17, 27, 28 *(index)*	*(Response)*	echo of request
41	1	Analog Output Block - 32-bit	4*(operate)*	17, 27, 28 *(index)*	*(Response)*	echo of request
41	1	Analog Output Block - 32-bit	5*(direct op.)*	17, 27, 28 *(index)*	*(Response)*	echo of request
41	1	Analog Output Block - 32-bit	6*(direct op, no ack)*	17, 27, 28 *(index)*	*(Response)*	echo of request
41	2	Analog Output Block - 16-bit	3*(select)*	17, 27, 28 *(index)*	*(Response)*	echo of request
41	2	Analog Output Block - 16-bit	4*(operate)*	17, 27, 28 *(index)*	*(Response)*	echo of request
41	2	Analog Output Block - 16-bit	5*(direct op.)*	17, 27, 28 *(index)*	*(Response)*	echo of request
41	2	Analog Output Block - 16-bit	6*(direct op, no ack)*	17, 27, 28 *(index)*	*(Response)*	echo of request
41	3	Analog Output Block - single-precision, floating-point	3*(select)*	17, 27, 28 *(index)*	*(Response)*	echo of request
41	3	Analog Output Block - single-precision, floating-point	4*(operate)*	17, 27, 28 *(index)*	*(Response)*	echo of request
41	3	Analog Output Block - single-precision, floating-point	5*(direct op.)*	17, 27, 28 *(index)*	*(Response)*	echo of request
41	3	Analog Output Block - single-precision, floating-point	6*(direct op, no ack)*	17, 27, 28 *(index)*	*(Response)*	echo of request
50	1	Time and Date - absolute time	2*(write)*	07 *(limited qty = 1)*		
51	1	Time and Date CTO - absolute time, synchronized			*(Response)*	07 *(limited qty = 1)*
51	1	Time and Date CTO - absolute time, synchronized			*(Unsol. Resp.)*	07 *(limited qty = 1)*
51	2	Time and Date CTO - absolute time, un-synchronized			*(Response)*	07 *(limited qty = 1)*

51	2	Time and Date CTO - absolute time, un-synchronized			*(Unsol. Resp.)*	07 *(limited qty = 1)*
52	1	Time Delay - coarse			*(Response)*	07 *(limited qty = 1)*
52	2	Time Delay - fine			*(Response)*	07 *(limited 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)*		
120	0	Authentication - Assign Class	22*(assign class)*	06 *(no range, or all)*		
120	1	Authentication - Challenge	32*(auth req)*	5B	*(Auth. Resp.)*	5B
120	2	Authentication - Reply	32*(auth req)*	5B	*(Auth. Resp.)*	5B
120	3	Authentication - Aggressive Mode	any of 1 to 31	07 *(limited qty = 1)*	*(Response)*	07 *(limited qty = 1)*
120	3	Authentication - Aggressive Mode			*(Unsol. Resp.)*	07 *(limited qty = 1)*
120	4	Authentication - Session Key Status Request	32*(auth req)*	07 *(limited qty = 1)*		
120	5	Authentication - Session Key Status			*(Auth. Resp.)*	5B
120	6	Authentication - Session Key Change	32*(auth req)*	5B		
120	7	Authentication - Error	33*(auth req, no ack)*	5B	*(Auth. Resp.)*	5B
120	8			5B		

		Authentication - User Certificate	32*(auth req)*			
120	9	Authentication - MAC	any of 1 to 31	5B	*(Response)*	5B
120	9	Authentication - MAC			*(Unsol. Resp.)*	5B
120	10	Authentication - User Status Change	32*(auth req)*	5B		
120	11	Authentication - Update Key Change Request	32*(auth req)*	5B		
120	12	Authentication - Update Key Change Reply			*(Auth. Resp.)*	5B
120	13	Authentication - Update Key Change	32*(auth req)*	5B		
120	14	Authentication - Update Key Change Signature	32*(auth req)*	5B		
120	15	Authentication - Update Key Change Confirmation	32*(auth req)*	5B	*(Auth. Resp.)*	5B
121	0	Security Statistic	1*(read)*	00, 01 *(start-stop)*, 06 *(no range, or all)*, 17, 28 *(index)*		
121	0	Security Statistic - Assign Class	22*(assign class)*	00, 01 *(start-stop)*, 06 *(no range, or all)*, 17, 28 *(index)*		
121	1	Security Statistic	1*(read)*	00, 01 *(start-stop)*, 06 *(no range, or all)*, 17, 28 *(index)*	*(Response)*	00, 01 *(start-stop)*, 17, 28 *(index)*
122	0	Security Statistic Event - 32-bit with flag	1*(read)*	00, 01 *(start-stop)*, 06 *(no*		

				range, or all), 17, 28 *(index)*		
122	1	Security Statistic Event - 32-bit with flag	1 *(read)*	06 *(no range, or all)*, 07, 08 *(limited qty)*	*(Response)*	17, 28 *(index)*
122	1	Security Statistic Event - 32-bit with flag and time			*(Unsol. Resp.)*	17, 28 *(index)*
122	2	Security Statistic Event - 32-bit with flag and time	1 *(read)*	06 *(no range, or all)*, 07, 08 *(limited qty)*	*(Response)*	17, 28 *(index)*
122	2	Security Statistic Event - 32-bit with flag and time			*(Unsol. Resp.)*	17, 28 *(index)*

5 Data Points List (outstation only)

This part of the Device Profile shows, for each data type, 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.

This section is not included in this Master Station Profile.

---------- End of Device Profile for Reference Device ----------

---------- End of Complete Device Profile ----------