Operational Metering Architecture for non – Transmission connected BM Participants

1 October 2024

Contents

1. Overview

Introduction

This document sets out the detailed operational metering architecture NESO has in place to facilitate the connection of Embedded Small BMU's and Licence Exempt Embedded Medium Power Stations (<100MW) to the NESO Systems and to permit participation in the GB Balancing Mechanism. This does not include any transmission connected assets.

NESO provides SCADA Data Concentrator facilities, which allows third parties to connect and to provide operational metering signals to the Electricity National Control Centre.

Aggregated Secondary BMU's may exceed the 100MW threshold, but all sub-sites must be <100MW. As the size of aggregated BMU's increase NESO may request increased resilience of the operational metering signals which would require upgrading to a private network.

Currently the NESO offers two different protocols for connecting to the Data Concentrator. IEC 60870-5 104 over a Virtual Private Network and Message Queuing Telemetry Transport (MQTT) over a secure TLS connection. Other protocols can be accommodated by the Data Concentrator, but this will extend the operational metering connection timeline. Please contact your account manager if you want to explore this further.

Data Concentrator Service

This service is designed to provide maximum benefits to all parties, with the minimum disruption to their current business operations.

Small BM Participant's Responsibilities

- Establish internet connectivity to their IT infrastructure with a publicly accessible static IP address.
- IEC 104 connections (only), establish a secure virtual private network (VPN) connection with the Data Concentrator host, over the internet.
- IEC 104 connections (only), a NAT / route RFC1918 IP address will be allocated by NESO for the metering server / hardware.
- Configure BMU operational metering to communicate with NESO utilising the agreed protocol.
- Send NESO a CSV file in the agreed format with their server / hardware configuration.
- Transmit the required operational metering signals to NESO, from all Secondary BMUs ≥ 1MW.
- Transmit the required operational metering signals to NESO at the required sample rates and accuracy.
- Test and validate operational metering data prior to commissioning.
- In the event that any part of the Market Participant Operational Metering equipment (including the communications links to the NESO data concentrator) fails, then the BM Participant will be required to repair such equipment within 5 working days of notification of the fault.
- Inform NESO of any planned outages to operational metering at least 48 hours in advance to

box.SmallBmuOpsMeter-neso@nationalenergyso.com

NESO Responsibilities

- Establish connectivity from the Data Concentrator host to the Market Participant.
- IEC 104 connections (only), establish a secure VPN connection with the Market Participant over the internet.
- Configure the Data Concentrator to receive the Market Participants data signals.
- Test and validate metering data prior to commissioning.
- Provide first line support for service.

Note this document provides an overview of the information required to physically establish the communications between a Small BM Participant and NESO. It is assumed for the purposes of the document any legal and contractual activities as part of the overall connection process will have been completed prior to carrying out the technical process described within this document.

Dynamic Containment/Moderation/Regulation Services

For Dynamic Containment service providers, the NESO will require operational metering via the same methods (IEC104 and MQTT) found in this document.

This applies to both BM and non-BM participants. Refer to the document “Appendix F5 – Technical Conditions; Other Technical Requirements” for more details.

The responsibilities for both the NESO and the Dynamic Containment/Moderation/Regulation Participants remain identical to the Data Concentrator Service.

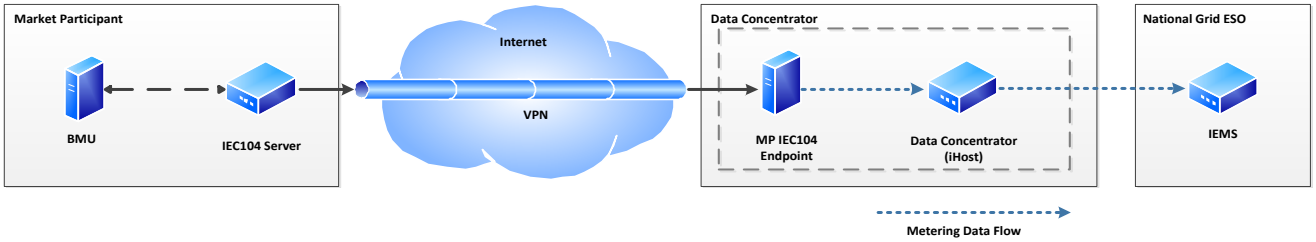
Please note in previous versions an **availability signal** was needed for Dynamic Containment services but this is longer the case because we are getting this via Ancillary Services Dispatch Platform.

System Architectures

IEC104 Overview

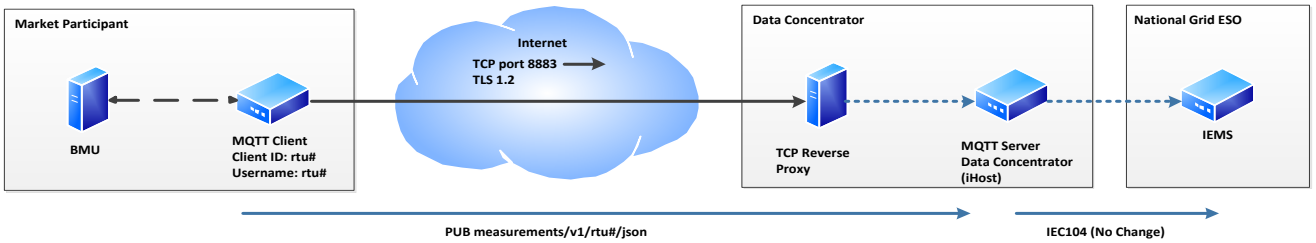
The operational metering system will use the IEC 60870-5 104 protocol over a VPN to connect to the NESO boundary.

NESO will connect a VPN to the Market Participants boundary and then initiate IEC104 communication to the Market Participants IEC104 Server.



MQTT Overview

The operational metering system will use the MQTT protocol over a TCP connection using TLS 1.2 to encrypt the communications sent from the market participant to the NESO Data Concentrator. Using “rtu#” as an example in the diagram below. This “rtu#” will be assigned to the Market Participant (MP) by the NESO and communicated to the MP through Nortech.



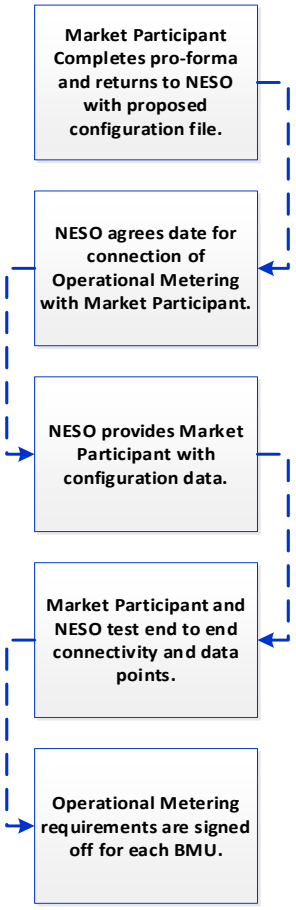
Operational Metering Commissioning

The successful provision of operational metering comprises of three phases.

- Data Exchange
- Set-up
- End to End Testing

All three phases need to be completed by the Market Participant to satisfy the operational metering requirements for participation in the Balancing Mechanism. The successful provision of operational metering is only one part of the process and completion of this stage does not mean the units are ready for BM participation.

NESO aims to complete a metering connection and to have it tested within 4 weeks of receipt of pro-forma in Section 5 (Metering Connection Pro Forma).



2. IEC104 Protocol

Supported Data Types

The following subset of data types will be supported by the IEC104 client.

Data Type	Description	Direction
1–M_SP_NA_1	Single point information	To NESO Only
3–M_DP_NA_1	Double point information	To NESO Only
5–M_ST_NA_1	Step position information	To NESO Only
9–M_ME_NA_1	Measured value, normalised value	To NESO Only
11–M_ME_NB_1	Measured value, scaled value	To NESO Only
13-M_ME_NC_1	Measured value, float value	To NESO Only
30-M_SP_TB_1	Single point information with time tag CP56Time2a	To NESO Only
31-M_DB_TB_1	Double point information with time tag CP56Time2a	To NESO Only
32-M_ST_TB_1	Step position information with time tag CP56Time2a	To NESO Only
34-M_ME_TD_1	Measured value, normalised value with time tag CP56Time2a	To NESO Only
35-M_ME_TE_1	Measured value, scaled value with time tag CP56Time2a	To NESO Only
36-M_ME_TF_1	Measured value, float value with time tag CP56Time2a	To NESO Only
70-ME_EI_NA_1	End of initialisation	To NESO Only
100-C_IC_NA_1	(General-) Interrogation command	From NESO Only
107-C_TS_TA_1	Test command with time tag CP56Time2a	From NESO Only

Table 1 – IEC104 Data Type Table

Note on Measured Values: Scaled values to be received from the Market Participant need to be scaled to an NMV over 20,000 bits.

For example:

Range	NMV	0 in 104	NMV in 104	Scale
-150 to 150	150	0	20,000	0.0075
-300 to 300	300	0	20,000	0.015
-450 to 450	450	0	20,000	0.0225

Table 2 – NMV Scaling Table

The **preferred** Measured Value Data Type is M_ME_TE_1

Note on Time Stamping: Time stamping of Data points is required from source. There is no mechanism to synchronise the time between systems. The Market Participant will be responsible for the correct time stamping at source. All times are to be provided in UTC.

Implementation

The next section details specifics about the NESO's implementation which will need to be accommodated for during the build process for the IEC104 Protocol.

Establishing Communications

The NESO IEC104 client will establish a TCP connection to the allocated RFC1918 IP address via the VPN on PORT 2404.

Once the TCP connection is established, the IEC104 client will then establish active IEC104 communication with a STARTDT_ACT command to the Market Participant IEC104 Server. The Market Participant Server should respond with a STARTDT_CON followed by an End of Initialisation Frame M_EI_NA to confirm that the system is ready.

The Market Participant Server should then begin sending the required operational metering.

General Interrogation

On system start-up after the Market Participant server has sent a M_EI_NA Frame, the NESO IEC104 client will send a General Interrogation request to the server.

The IEC104 client will then request a General Interrogation 100-C_IC_NA_1 of the IEC104 server every 30 minutes, to make sure that the latest values are being reported.

Data Buffering and the K Value

To stop links from becoming overloaded and delaying the reporting of real time data, Market Participants should limit the amount of data they are buffering while the server is not communicating to NESO. NESO would recommend only storing the last good value in the buffer for Measured Values while the IEC104 link is down.

To stop the IEC server from discarding data when the links are under heavy load, the servers should pack as many measured values into each APDU for onwards transmission. This may involve some delay in onward transmission but will reduce the risk of the IEC104 server discarding APDU's for transmission.

If the data rate is too high and the client has not acknowledged the Send counter (K Value – Maximum difference receive sequence number to send state variable) in time the Server should reduce the rate at which it sends data and clear out the buffer of stored values as new values arrive.

Data Reporting Frequency

NESO requires a time stamped value from the meter every 1 second, to arrive at the NESO Data Concentrator client within 5 seconds of the reading being taken.

For Aggregated units, the total BMU output should be recalculated every 1 second time stamped and sent onto NESO.

Analogue values (e.g. active power) should be sent every 1-second with the cause of transmission flag set to Spontaneous. A measurement value should be sent every 1-second for all analogues even if the latest known value has not changed.

Step positions (e.g. tap position indicator) and binary values (e.g. circuit breaker state) should only be reported on change with the cause of transmission flag set to Spontaneous.

Values may be split across multiple frames if required either to reduce latency or due to exceeding maximum message size, however the requirement to send analogue values every 1-second still applies.

Values should be timestamped with the time the value was sampled at source, including milliseconds. An exception to this is if communication has been lost to downstream equipment or a value becomes invalid, where the timestamp should be substituted with the current time at time of transmission.

If communication is lost to downstream equipment, then the client should immediately send last known value for all data points with quality flag set to "Invalid" ("Not Topical" is also accepted). The timestamp should be set to when the failure was detected and not time of the last known update. For analogues values, it is

acceptable to stop sending 1-second, however 1-second updates should resume as soon as downstream communication has been restored.

For binary values, an update must be reported to notify change in quality even if the state (open/closed) did not change.

VPN Specifications

The VPN connection between NESO and the Market Participant will use IKE v2 with a Pre-Shared Key. The following settings are supported.

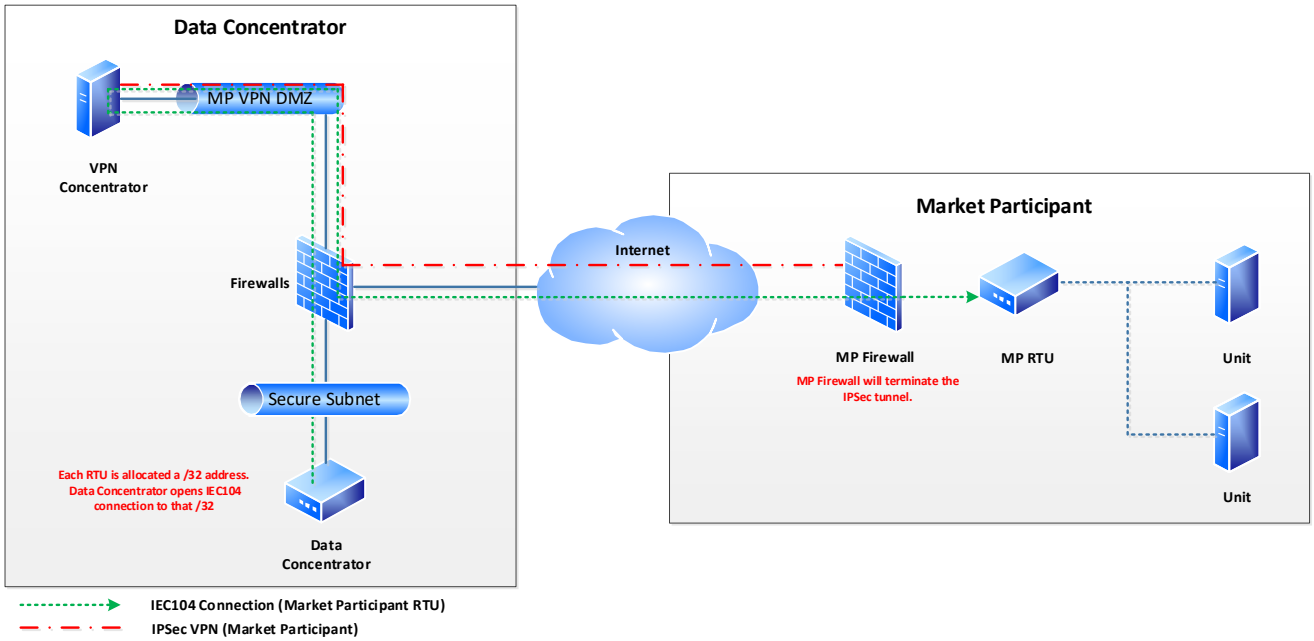
Phase 1	
Key Exchange:	**IKEv2**
Remote Gateway:	Will be provided at the appropriate time
Remote Identifier:	Will be same as Remote Gateway
Local Gateway:	Public Static IP address provided by Market Participant
Local Identifier:	Same as the Local gateway
Pre-Shared Key:	Mutual PSK
Negotiation Mode:	Main
Encryption:	AES256-GCM (128-bit key length), AES256-CBC
Hash:	SHA256, SHA384, SHA512
DH Group:	16 (MODP4096), 17 (MODP6144), 18 (MODP8096), 19 (ECP256), 20 (ECP384)
Key Lifetime:	8 hours (28800s)
Dead Peer Detection:	Yes (10s Delay, 5 Retries)

Table 3 – Phase 1 Table

Phase 2	
Protocol:	ESP
Local Network:	Allocated by NESO. Will be provided at the appropriate time
Remote Network:	Will be provided at the appropriate time
Encryption:	AES256-GCM (128-bit key), AES256-CBC
Hash:	SHA256, SHA384, SHA512, AES256-GCM
PFS Key Group:	16 (MODP4096), 17 (MODP6144), 18 (MODP8096), 19 (ECP256), 20 (ECP384)
Key lifetime:	1 hour (3600s)

Table 4 – Phase 2 Table

The VPN will create a tunnel from the Remote GW IP address and NESO address that will be provided at the same time as the PSK.



IOA and CASDU Addressing

The following IOA address scheme is required between the Market participant and NESO systems.

To enable efficient transmission of data to NESO the following addressing structure should be followed.

Type	DUT	IOA Range
Measured Value	9-M_ME_NA_1 11-M_ME_NB_1 13-M_ME_NC_1 34-M_ME_TD_1 35-M_ME_TE_1 36-M_ME_TF_1	1000 to 1699
Single Point	1-M_SP_NA_1 30-M_SP_TB_1	1700 to 1799
Double Point	3-M_DP_NA_1 31-M_DP_TB_1	1800 to 1899
Step Position	5-M_ST_NA_1 32-M_ST_TB_1	1900 to 1999

Table 5 - Measurement Object Definition

For Spontaneous changes a DUT of M_ME_TE, M_SP_TB, M_DP_TB or M_ST_TB should be used.

The General Interrogation response should not include the time tag and should use a DUT of M_ME_NB, M_SP_NA, M_DP_NA, M_ST_NA.

Data points are required to sequentially increase for each data type.

The CASDU will be assigned by NESO as part of VPN set-up. If a market participant for the Data Concentrator wants to take part within the Dynamic Containment Service, they will be allocated the same CASDU from the Data Concentrator Service.

Supported Causes of Transmission

To simplify the multiple configuration options available for sending data changes, NESO can only support a small subset of the mechanisms for sending data.

Cause of Transmission	Description	Protocol
3	Spontaneous	IEC104
4	Initialised	IEC104
5	Interrogation	IEC104
6	Activation	IEC104
7	Confirmation Activation	IEC104
8	Deactivation	IEC104
9	Confirmation Deactivation	IEC104
10	Termination Deactivation	IEC104
20	Interrogated by General Interrogation	IEC104

Table 6 – Supported Causes of Transmission Table – IEC104

All changes of state that are not in response to a general interrogation should be reported as Cause of Transmission (COT) 3, Spontaneous for IEC104.

Communication Failures to remote assets

As with all metering equipment, it is prone to occasional failures. When a Market participant detects a failure in a meter or communication link, the affected data points should have the Not Topical or Invalid flag set to indicate to NESO that these values are no longer valid.

When metering or communication failure affects an aggregated BMU, the sub-unit that has experienced a metering or communication failure should set the affected data points to Not Topical or Invalid but should use the last known good value for the aggregated BMU total output. The Market Participant should consider a method of overwriting this value, to make sure the aggregated BMU output is not unduly affected by the metering or communication failure.

NESO will automatically send an alert to the Market Participant when the client detects a prolonged period of no communication. Please send any queries for re-establishing the operational metering to **box.SmallBmuOpsMeter-neso@nationalenergyso.com**

In the event of a failure of the communication link or loss of any operational data signals, NESO may not dispatch the affected unit or units until the issue has been resolved.

IEC 104 Gateway Solution Options

Small BMU Participants requiring an IEC 104 Gateway solution could consider the following options:

- Kenda Nebula (hardware appliance)
- Siemens SIMATIC RTU3030C (hardware appliance)
- Siemens SICAM PAS (hardware appliance)
- ABB RTU 560 (hardware appliance)
- IPComm ipConv (software run on industrial PC, server, or IPComm hardware products inc. IPC191V4 and MEC2)
- COPA-DATA straton Soft PLC (software run on industrial PC or server)
- Inaccess TELOS (software platform)
- MZ Automation IEC 60870-5-104 software library (source code library available in C and .NET, this is not a usable product alone and would need to be built into a custom-built software application)

This list is by no means exhaustive and many other IEC 104 gateway solutions exist on the market.

It is the Small BMU Participant's responsibility to configure, correctly, the IEC 104 gateway equipment (including integration with BMU metering systems) to be compliant with the technical specifications provided in this document.

3. MQTT Protocol

MQTT Data Configuration

Measurements are bundled together and published as a list of measurement objects.

Field Name	JSON Field Name	JSON Data Type	Protobuf Data Type	Requirement	Description
measurements	m	array	repeated Measurement	Mandatory	List of measurements

Table 7 - Measurement List Definition Table

Each measurement object contains the following fields:

Field Name	JSON Field Name	JSON Data Type	Protobuf Data Type	Requirement	Description
address	a	number	uint32	Mandatory	Data point address
timestamp	t	number	int64	Mandatory	POSIX timestamp, milliseconds since midnight 1st Jan 1970 in UTC time zone
value	v	number	double	Mandatory	Measurement value
quality	q	number	enum	Mandatory if not default value	Quality of value, enumeration. 0 = Good 1 = Invalid 2 = Suspect The default is 0 (Good) if the field is not provided
cot	c	number	enum	Mandatory if not default value	Cause of transmission, enumeration. 0 = Data Update 1 = Integrity The default is 0 (Data Update) if the field is not provided

Table 8 - Measurement Object Definition Table

Measurements Topic (JSON)

Topic:

measurements/v1/*client_id*/json

QoS: 1

Example: measurements/v1/rtu5/json

Payload:

Each message contains an array of measurement objects UTF-8 text encoded using JSON.

The JSON message should be stripped of any white space to minimise the message size.

To further reduce the average size of a message, any optional fields may be omitted if they have default value.

Example (Pretty Printed):

```
{
  "m": [
    {"a": 1000, "t": 1582537797154, "v": 0.229, "q": 0, "c": 0},
    {"a": 1001, "t": 1582537797154, "v": 48, "q": 0, "c": 0},
    {"a": 1002, "t": 1582537797154, "v": 6.1940, "q": 0, "c": 0},
    {"a": 1003, "t": 1582537797154, "v": -6.0290, "q": 0, "c": 0}
  ]
}
```

Measurements Topic (Protocol Buffers)

Topic:

measurements/v1/*client_id*/proto3

QoS: 1

Example: measurements/v1/rtu5/proto3

Payload:

Each message contains an array of measurement objects binary encoded using Protocol Buffers Version 3.

Schema:

```
syntax = "proto3";
message MeasurementList {
  repeated Measurement measurements = 1;
}
message Measurement {
  uint32 address = 1;
  int64 timestamp = 2;
  double value = 3;
  QualityOfValue quality = 4;
  CauseOfTransmission cot = 5;
}
enum QualityOfValue {
  GOOD = 0;
  INVALID = 1;
  SUSPECT = 2;
}
enum CauseOfTransmission {
  DATAUPDATE = 0;
  INTEGRITY = 1;
}
```

Implementation

The next section details specifics about the NESO's implementation which will need to be accommodated for during the build process for the MQTT Protocol.

MQTT Version

MQTT Version 3.1, 3.1.1 or 5.0

Establishing Communications

The market participant's MQTT client initiates a persistent TCP connection to a FQDN registered in public DNS using TLS 1.2 to encrypt the communications on PORT 8883. The market participant is advised of the FQDN and port (8883) to configure their client during connection set-up.

The server DNS record has a low Time to Live (TTL) and should not be cached by the client for longer than this TTL value. Ideally, the client should perform a fresh DNS lookup request each time it attempts to connect to the MQTT server.

The Username in the MQTT CONNECT message should be set the same as the Client ID. The server does not support multiple concurrent connections using the same Client ID.

MQTT Keep Alive function must be used with a keep alive timeout set in the range 10-60 seconds.

Persistent MQTT sessions are not supported, and the clean session flag should be set on connection.

The Last Will and Testament (LWT) should not be used, and retained messages are not supported.

Once authenticated, the Market Participant Client should then begin sending the required operational metering.

Encryption, Authentication and Access Control

The use of TLS 1.2 is enforced for all connections to the MQTT server.

The market participant's client should be configured to use one of the following TLS cipher suites, which will be enforced by the server:

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xC0, 0x2F)
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xC0, 0x30)
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x00, 0x9E)
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x00, 0x9F)

The MQTT server is configured with a X509 certificate signed by a public Certificate Authority. Client machines that keep their trusted root certificate store up to date (e.g. via Windows updates) will be able to automatically verify the server's certificate's chain of trust.

Clients are authenticated using the username and password passed in the initial MQTT CONNECT message. The password will be issued to the market participant during connection set-up via secure encrypted email and will be at least 56-characters and of high entropy. The market participant should ensure this password is kept secure on their MQTT client machine.

The MQTT server is configured so that MP clients are only allowed to publish to the measurements topic and are not allowed to subscribe to any topics.

Data Integrity Checks

Transport layer:

- Data is sent over an encrypted TLS connection
- Client connects from known publicly accessible static IP address, subnet or range
- Client negotiates with TLS version (1.2) and an allowed cipher suite
- TLS integrity checks are valid (HMAC) on all packets

MQTT message:

- Each MQTT message is at least 2 bytes in length
- Client connects using allowed protocol version (3.1, 3.1.1, 5.0)
- Client uses only allowed MQTT control packet types (CONNECT, DISCONNECT, PUBLISH, PINGREQ)
- The MQTT session has been authenticated before receiving any published data
- Client publishes to an allowed topic for that connection
- Client published with Quality of Service (QOS) = 1
- MQTT payload size is not greater than 128KB

Decoded measurement data:

- Decoded measurement objects are valid, with no missing fields that are mandatory
- All data point addresses exist on the client configuration in the Data Concentrator
- The number of measurement values published in a single message does not exceed 100
- All analogue values are within valid range per the min/max configuration
- Measurement timestamps are within last 60 seconds relative to the server clock

All the above checks will be performed by the iHost (Data Concentrator) server software. If any of these checks fail, then the message will either be discarded, or the TCP connection forcibly dropped.

Data Buffering

To stop links from becoming overloaded and delaying the reporting of real time data, Market Participants should limit the amount of data they are buffering while the client is not connected. Only the latest values for each data point should be buffered in the client. If a newer value becomes available, then any older value still held in the buffer (e.g. due to loss of connection to the server) should be discarded.

The client should pack as many measurement values into each message as possible to make efficient use of the network and reduce end-to-end latency. However, there is an upper limit to the message payload size the server will accept, and the client should not send more than 100 measurement values in a single message and the encoded message payload size should not exceed 128KB.

Data Reporting Frequency

NESO requires a time stamped value from the meter every 1 second, to arrive at the NESO Data Concentrator client within 5 seconds of the reading being taken.

For Aggregated units, the total BMU output should be recalculated every 1 second time stamped and sent onto NESO.

Immediately following each reconnection to the MQTT server, the client should send measurement values for all defined data points using the last known value and the cause of transmission flag set to “Integrity”.

Analogue values (e.g. active power) should be sent every 1-second with the cause of transmission flag set to “Data Update”. A measurement value should be sent every 1-second for all analogues even if the latest known value has not changed.

Step positions (e.g. tap position indicator) and binary values (e.g. circuit breaker state) should only be reported on change with the cause of transmission flag set to “Data Update”. In addition, the client should resend the last known value at least every 30 minutes with the cause of transmission flag set to “Integrity”.

Values may be split across multiple messages if required either to reduce latency or due to exceeding maximum message size, however the requirement to send analogue values every 1-second still applies.

Values should be timestamped with the time the value was sampled at source, including milliseconds. An exception to this is if communication has been lost to downstream equipment or a value becomes invalid, where the timestamp should be substituted with the current time at time of transmission.

If communication is lost to downstream equipment, then the client should immediately send last known value for all data points with quality flag set to “Invalid” ("Suspect" is also accepted). The timestamp should be set to when the failure was detected and not time of the last known update. For analogues values, it is acceptable to stop sending 1-second, however 1-second updates should resume as soon as downstream communication has been restored.

For binary values, an update must be reported to notify change in quality even if the state (open/closed) did not change.

Representation of Measurement Values

Analogue values and step positions should be sent as an IEEE 754 double precision floating point number and in engineering units. For example, active power of 5.25MW should be JSON encoded as a number literal 5.25. For Step positions, the value is the current position.

Binary values such as those reporting circuit breaker state should be sent with a value of 0 representing open and a value of 1 representing closed. Any other value is treated as invalid. If the state is indeterminate, then the client should report last known value with the quality flag set to “Invalid” ("Suspect" is also accepted).

Client IDs and Data Point Addressing

Client IDs

Each market participant client is assigned a unique Client ID by NESO as part of the connection set-up process. This will be a lower-case string literal "rtu" followed by a unique numeric address in the range 1 to 65535. The address is equivalent to an IEC104 CASDU and will be assigned from the same address pool.

Data Point Addresses

Each device data point reported by a client is assigned a numeric address in the range 1 to 16777215. The address is unique within the address space of a client.

Each client may report data points for one or more BMUs.

The address assigned will be dependent on the data point type, and the following addressing structure should be followed.

Type	Address Range
Analogue Input (e.g. Active Power)	1000 to 1699
Binary Input (e.g. Circuit Breaker)	1700 to 1799
Step Position (e.g. Tap Position Indicator)	1900 to 1999

Table 9 - Data Point Address Ranges

Supported Causes of Transmission

To simplify the multiple configuration options available for sending data changes, NESO can only support a small subset of the mechanisms for sending data.

Cause of Transmission	Description	Protocol
0	Data Update	MQTT
1	Integrity	MQTT

Table 10 – Supported Causes of Transmission Table - MQTT

Communication Failures to remote assets

As with all metering equipment, it is prone to occasional failures. When a Market participant detects a failure in a meter or communication link, the affected data points should have the Suspect or Invalid flag set to indicate to NESO that these values are no longer valid.

When metering or communication failure affects an aggregated BMU, the sub-unit that has experienced a metering or communication failure should set the affected data points to Suspect or Invalid but should use the last known good value for the aggregated BMU total output. The Market Participant should consider a method

of overwriting this value, to make sure the aggregated BMU output is not unduly affected by the metering or communication failure.

NESO will automatically send an alert to the Market Participant when the client detects a prolonged period of no communication. Please send any queries for re-establishing the operational metering to **box.SmallBmuOpsMeter-neso@nationalenergyso.com**

In the event of a failure of the communication link or loss of any operational data signals, NESO may not dispatch the affected unit or units until the issue has been resolved.

4. Data Exchange

To allow the NESO to configure the data concentrator to receive the Market Participants' data, a common file will be used to exchange the configuration of the Market Participant's system.

A CSV file will be used to communicate the setup of the remote system.

A sample CSV file is available on request from NESO by emailing

box.SmallBmuOpsMeter-neso@nationalenergyso.com MQTT Data Exchange Exceptions:

The process for agreeing on signals and exchanging configuration will remain mostly the same as for IEC104, with the following exceptions:

- CASDU will be replaced in the CSV configuration file with Client ID. This is just a change in terminology, and they are otherwise interchangeable and will be assigned from the same address pool.
- IOA will be replaced with Address. This is just a change in terminology, and the same address ranges will be re-used for MQTT (see Section 3).

The data point naming convention, sign convention and recommended analogue scaling will remain the same.

General Data Exchange:

Header

Please update the following items within the CSV file:

- MP Config Version – Please up-rev the version number with each release of the of this file to NESO
- MP Company Name - Please add your company name to the file for easy identification
- CASDU – Once known, please add your CASDU to the file. This will be assigned by NESO

Binary Inputs (*All Single and Double Points)*

Field	Description	Example
IOA	The IOA of the Point	1001
Name	What is the point called	AG-BFLX01 CB
BMU ID	BMU-ID	AG-BFLX01
Normally Open	Should Normally be set to No	No

Table 11 – Binary Inputs Table

Note: NESO's convention for Closed Open Indications for IEC104:

Single Point: [ON (1) = OPEN], [OFF (0) = CLOSED]

Double Point: [ON (2) = CLOSED], [OFF (1) = OPEN]

Note: This is the opposite for MQTT:

Single Point: [ON (1) = CLOSED], [OFF (0) = OPEN]

Double Point: [ON (2) = OPEN], [OFF (1) = CLOSED]

Analogue Inputs *(All Measured Vales and Step Positions)*

Field	Description	Example
IOA	The IOA of the Point	1001
Name	What is the point called	AG-BFLX01 ACTIVE POWER
BMU ID	BMU-ID	AG-BFLX01
Display Min	Actual Minimum of point	-150
Display Max	Actual NMV of point	150
Display Scale	Coefficient of the point	0.0075
Units	The Unit of the Point	MW
Routine Datalogging Interval (s)	The Refresh Rate for the Analogue in seconds. Set to 0 if analogue is reported on change.	1

Table 12 – Analogue Inputs Table

All data submissions will need to be made to **box.SmallBmuOpsMeter-neso@nationalenergyso.com** at least 4 weeks ahead of the planned change.

Data Point Naming Convention

To make sure that all the data points we are receiving are unique and can be easily referenced back to the originating asset the following convention needs to be followed for the data point name.

For a BMU; The Point should reference both originating BMU and the data being sent:

BMU NAME + DATA TYPE

Data Type	Example Name	Unit
Active Power	AG-BFLX01 ACTIVE POWER	MW
Reactive Power	AG-BFLX01 REACTIVE POWER	MVAR
Voltage	AG-BFLX01 VOLTAGE	KV
Wind Speed	AG-BFLX01 WIND SPEED	M/S
Wind Direction	AG-BFLX01 WIND DIRECTION	DEG
Power Available	AG-BFLX01 POWER AVAILABLE	MW
State of Charge (Energy)	AG-BFLX01 STATE OF CHARGE	%
Energy Available	AG-BFLX01 ENERGY AVAILABLE	MWh
Global Radiation	AG-BFLX01 GLOBAL RADIATION	W/m2
Temperature	AG-BFLX01 TEMPERATURE	DEG
Tidal Flow	AG-BFLX01 TIDAL FLOW	M/S
Tide Direction	AG-BFLX01 TIDE DIRECTION	DEG
Tap Position	AG-BFLX01 TAP POSITION	TPI
Controlling Breaker	AG-BFLX01 BREAKER	CLOSED/OPEN

Table 13 – Data Point Naming Convention Table

For a sub unit or other data points, the point should reference both the BMU and Sub Unit.

BMU NAME + SUB UNIT NAME + DATA TYPE

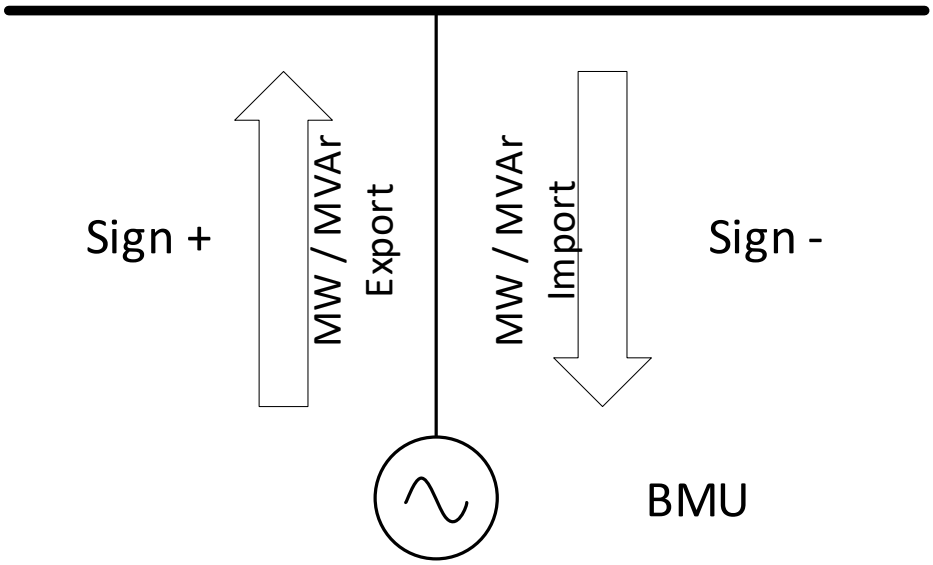
For example;

AG-BFLX01 **SUB UNIT NAME** ACTIVE POWER

Sign Convention

Where signals can be signed in either direction i.e. Active Power and Reactive Power the following convention needs to be followed.

For Active Power and Reactive Power:



For Power Available and State of Energy, the following convention needs to be used.

Recommended Analogue Scaling

Data Type	Display Max	Display Scale
Active Power (MW)	150	0.0075
Reactive Power (MVAr)	150	0.0075
Voltage (KV)	500	0.0250
Wind Speed (M/S)	50	0.0025
Wind Direction (DEG)	360	0.0180
Power Available (MW)	150	0.0075
State of Charge (Energy) (%)	100	0.0050
Energy Available (MWh)	500	0.0250
Global Radiation (W/M^2)	1000	0.0500
Temperature (DEGC)	100	0.0050

Tidal Flow	10	0.0005
Tide Direction	360	0.0180
Tap Position (TPI)	16	1

Table 14 – Analogue Scaling Table

Note: NESO backhaul communication is via IEC104 which uses a scaled value. To enable us to configure our systems we will need to know the maximum value (Display Max) for each analogue data point regardless of protocol used.

5. Testing

As part of the Operational Metering connection setup, the IEC104/MQTT connection will be tested to verify to conforms to the technical requirements outlined above in this document.

In addition to functional tests, each connection needs to go through a 48-hour stability test. The criteria for passing this stability test are outlined below:

Over a 48-hour period:

- There were no disconnects that lasted for longer than 1 minute
- The total time disconnected was less than 5 minutes
- The total number of disconnects was less than 24

6. Metering Connection Pro forma

Please refer to the complementary "***Operational Metering Pro-forma for Small (<100MW) BM Participant***s" document.

7. Glossary

Abbreviation	Meaning
BM	Balancing Mechanism
CASDU	Common Application Service Data Unit
DNP3	Distributed Network Protocol
IEC	International Electrotechnical Commission
IOA	Information Object Address
MQTT	Message Queuing Telemetry Transport
NMV	Nominal Maximum Value
OPC-UA	OPC Unified Architecture
RTU	Real-time Telemetry Unit
SCADA	Supervisory Control and Data Acquisition
TERRE	Trans European Replacement Reserves Exchange

Table 15 – Glossary Table

8. Interoperability Statement – IEC104

Interoperability

This companion standard presents sets of parameters and alternatives from which subsets must be selected to implement particular telecontrol systems. Certain parameter values, such as the choice of "structured" or "unstructured" fields of the INFORMATION OBJECT ADDRESS of ASDUs represent mutually exclusive alternatives. This means that only one value of the defined parameters is admitted per system. Other parameters, such as the listed set of different process information in command and in monitor direction allow the specification of the complete set or subsets, as appropriate for given applications. This clause summarizes the parameters of the previous clauses to facilitate a suitable selection for a specific application. If a system is composed of equipment stemming from different manufacturers, it is necessary that all partners agree on the selected parameters.

The interoperability list is defined as in IEC 60870-5-101 and extended with parameters used in this standard. The text descriptions of parameters which are not applicable to this companion standard are strike-through (corresponding check box is marked black).

NOTE In addition, the full specification of a system may require individual selection of certain parameters for certain parts of the system, such as the individual selection of scaling factors for individually addressable measured values.

The selected parameters should be marked in the white boxes as follows:

☐ Function or ASDU is not used

☒ Function or ASDU is used as standardized (default)

R Function or ASDU is used in reverse mode

B Function or ASDU is used in standard and reverse mode

The possible selection (blank, X, R, or B) is specified for each specific clause or parameter.

A black check box indicates that the option cannot be selected in this companion standard.

System or device
(system-specific parameter, indicate definition of a system or a device by marking one of the following with "**X**")

☐ System definition

☒ Controlling station definition (Master)

☐ Controlled station definition (Slave)

☐ **Network configuration**
(network-specific parameter, all configurations that are used are to be marked "**X**")

■ ~~Point-to-point~~ ■ ~~Multipoint-~~

■ ~~Multiple point-to-point~~ ■ ~~Multipoint-star~~

Physical layer
(network-specific parameter, all interfaces and data rates that are used are to be marked "**X**")

Transmission speed (control direction)

Unbalanced interchange Circuit V.24/V.28 Standard	Unbalanced interchange Circuit V.24/V.28 Recommended if >1 200 bit/s	Balanced interchange Circuit X.24/X.27	
~~100 bit/s~~	~~2 400 bit/s~~	~~2 400 bit/s~~	~~56 000 bit/s~~
~~200 bit/s~~	~~4 800 bit/s~~	~~4 800 bit/s~~	~~64 000 bit/s~~
~~300 bit/s~~	~~9 600 bit/s~~	~~9 600 bit/s~~	
~~600 bit/s~~		~~19 200 bit/s~~	
~~1 200 bit/s~~		~~38 400 bit/s~~	

Transmission speed (monitor direction)

Unbalanced interchange Circuit V.24/V.28 Standard	Unbalanced interchange Circuit V.24/V.28 Recommended if >1 200 bit/s	Balanced interchange Circuit X.24/X.27	
~~100 bit/s~~	~~2 400 bit/s~~	~~2 400 bit/s~~	~~56 000 bit/s~~
~~200 bit/s~~	~~4 800 bit/s~~	~~4 800 bit/s~~	~~64 000 bit/s~~
~~300 bit/s~~	~~9 600 bit/s~~	~~9 600 bit/s~~	
~~600 bit/s~~		~~19 200 bit/s~~	
~~1 200 bit/s~~		~~38 400 bit/s~~	

Link layer
(network-specific parameter, all options that are used are to be marked "X". Specify the maximum frame length. If a non-standard assignment of class 2 messages is implemented for unbalanced transmission, indicate the Type ID and COT of all messages assigned to class 2.)

~~Frame format FT 1.2, single character 1 and the fixed time out interval are used exclusively in this companion standard.~~

Link transmission

- ~~Balanced transmission~~
- ~~Unbalanced transmission~~

Frame length

- ~~Maximum length L (number of octets)~~

Address field of the link

- ~~not present (balanced transmission only)~~
- ~~One octet~~
- ~~Two octets~~
- ~~Structured~~
- ~~Unstructured~~

When using an unbalanced link layer, the following ASDU types are returned in class 2 messages (low priority) with the indicated causes of transmission:

☐ ~~The standard assignment of ASDUs to class 2 messages is used as follows:~~

Type identification	Cause of transmission
9, 11, 13, 21	<1>

☐ ~~A special assignment of ASDUs to class 2 messages is used as follows:~~

Type identification	Cause of transmission

~~Note: (In response to a class 2 poll, a controlled station may respond with class 1 data when there is no class 2 data available).~~

- **Application layer**

Transmission mode for application data

Mode 1 (Least significant octet first), as defined in 4.10 of IEC 60870-5-4, is used exclusively in this companion standard.

Common address of ASDU

(system-specific parameter, all configurations that are used are to be marked "**X**")

☐ ~~One octet~~ ☒ Two octets

Information object address

(system-specific parameter, all configurations that are used are to be marked "**X**")

☐ ~~One octet~~
☐ ~~Two octets~~
☒ Three octets

☒ Structured
☒ Unstructured

Cause of transmission

(system-specific parameter, all configurations that are used are to be marked "**X**")

☐ ~~One octet~~ ☒ Two octets (with originator address). Originator address is set to zero if not used

Length of APDU

(system-specific parameter, specify the maximum length of the APDU per system)

The maximum length of APDU for both directions is 253. It is a fixed system parameter.

[redacted] Maximum length of APDU per system in control direction
Maximum length of APDU per system in monitor direction

Selection of standard ASDUs

Process information in monitor direction
(station-specific parameter, mark each Type ID "**X**" if it is only used in the standard direction, "**R**" if only used in the reverse direction, and "**B**" if used in both directions).

X	<1> :=	Single-point information	M_SP_NA_1
[redacted]	~~<2> :=~~	~~Single-point information with time tag~~	~~M_SP_TA_1~~
X	<3> :=	Double-point information	M_DP_NA_1
[redacted]	~~<4> :=~~	~~Double-point information with time tag~~	~~M_DP_TA_1~~
X	<5> :=	Step position information	M_ST_NA_1
[redacted]	~~<6> :=~~	~~Step position information with time tag~~	~~M_ST_TA_1~~
	<7> :=	Bitstring of 32 bit	M_BO_NA_1
[redacted]	~~<8> :=~~	~~Bitstring of 32 bit with time tag~~	~~M_BO_TA_1~~
X	<9> :=	Measured value, normalized value	M_ME_NA_1
[redacted]	~~<10> :=~~	~~Measured value, normalized value with time tag~~	~~M_ME_TA_1~~
X	<11> :=	Measured value, scaled value	M_ME_NB_1
[redacted]	~~<12> :=~~	~~Measured value, scaled value with time tag~~	~~M_ME_TB_1~~
X	<13> :=	Measured value, short floating point value	M_ME_NC_1
[redacted]	~~<14> :=~~	~~Measured value, short floating point value with time tag~~	~~M_ME_TC_1~~
X	<15> :=	Integrated totals	M_IT_NA_1
[redacted]	~~<16> :=~~	~~Integrated totals with time tag~~	~~M_IT_TA_1~~
[redacted]	~~<17> :=~~	~~Event of protection equipment with time tag~~	~~M_EP_TA_1~~
[redacted]	~~<18> :=~~	~~Packed start events of protection equipment with time tag~~	~~M_EP_TB_1~~
[redacted]	~~<19> :=~~	~~Packed output circuit information of protection equipment with time tag~~	~~M_EP_TC_1~~
	<20> :=	Packed single-point information with status change detection	M_SP_NA_1
	<21> :=	Measured value, normalized value without quality descriptor	M_ME_ND_1
X	<30> :=	Single-point information with time tag CP56Time2a	M_SP_TB_1
X	<31> :=	Double-point information with time tag CP56Time2a	M_DP_TB_1
X	<32> :=	Step position information with time tag CP56Time2a	M_ST_TB_1
	<33> :=	Bitstring of 32 bit with time tag CP56Time2a	M_BO_TB_1
X	<34> :=	Measured value, normalized value with time tag CP56Time2a	M_ME_TD_1
X	<35> :=	Measured value, scaled value with time tag CP56Time2a	M_ME_TE_1
X	<36> :=	Measured value, short floating point value with time tag CP56Time2a	M_ME_TF_1
X	<37> :=	Integrated totals with time tag CP56Time2a	M_IT_TB_1
	<38> :=	Event of protection equipment with time tag CP56Time2a	M_EP_TD_1
	<39> :=	Packed start events of protection equipment with time tag CP56Time2a	M_EP_TE_1
	<40> :=	Packed output circuit information of protection equipment with time tag CP56Time2a	M_EP_TF_1

In this companion standard only the use of the set <30> – <40> for ASDUs with time tag is permitted.

Process information in control direction
(station-specific parameter, mark each Type ID "**X**" if it is only used in the standard direction, "**R**" if only used in the reverse direction, and "**B**" if used in both directions).

☐	<45> := Single command	C_SC_NA_1
☐	<46> := Double command	C_DC_NA_1
☐	<47> := Regulating step command	C_RC_NA_1
☐	<48> := Set point command, normalized value	C_SE_NA_1
☐	<49> := Set point command, scaled value	C_SE_NB_1
☐	<50> := Set point command, short floating point value	C_SE_NC_1
☐	<51> := Bitstring of 32 bit	C_BO_NA_1
☐	<58> := Single command with time tag CP56Time2a	C_SC_TA_1
☐	<59> := Double command with time tag CP56Time2a	C_DC_TA_1
☐	<60> := Regulating step command with time tag CP56Time2a	C_RC_TA_1
☐	<61> := Set point command, normalized value with time tag CP56Time2a	C_SE_TA_1
☐	<62> := Set point command, scaled value with time tag CP56Time2a	C_SE_TB_1
☐	<63> := Set point command, short floating point value with time tag CP56Time2a	C_SE_TC_1
☐	<64> := Bitstring of 32 bit with time tag CP56Time2a	C_BO_TA_1

Either the ASDUs of the set <45> – <51> or of the set <58> – <64> are used.

System information in monitor direction
(station-specific parameter, mark with an "**X**" if it is only used in the standard direction, "**R**" if only used in the reverse direction, and "**B**" if used in both directions).

☒	<70> := End of initialization	M_EI_NA_1

System information in control direction
(station-specific parameter, mark each Type ID "**X**" if it is only used in the standard direction, "**R**" if only used in the reverse direction, and "**B**" if used in both directions).

☒	<100>:= Interrogation command	C_IC_NA_1
☒	<101>:= Counter interrogation command	C_CI_NA_1
☐	<102>:= Read command	C_RD_NA_1
☒	<103>:= Clock synchronization command (option see 7.6)	C_CS_NA_1
■	~~<104>:= Test command~~	~~C_TS_NA_1~~
☐	<105>:= Reset process command	C_RP_NA_1
■	~~<106>:= Delay acquisition command~~	~~C_CD_NA_1~~
☒	<107>:= Test command with time tag CP56Time2a	C_TS_TA_1

Parameter in control direction
(station-specific parameter, mark each Type ID "**X**" if it is only used in the standard direction, "**R**" if only used in the reverse direction, and "**B**" if used in both directions).

☐	<110>:= Parameter of measured value, normalized value	P_ME_NA_1
☐	<111>:= Parameter of measured value, scaled value	P_ME_NB_1
☐	<112>:= Parameter of measured value, short floating point value	P_ME_NC_1
☐	<113>:= Parameter activation	P_AC_NA_1

File transfer
(station-specific parameter, mark each Type ID "**X**" if it is only used in the standard direction, "**R**" if only used in the reverse direction, and "**B**" if used in both directions).

☐	<120>:= File ready	F_FR_NA_1
☐	<121>:= Section ready	F_SR_NA_1
☐	<122>:= Call directory, select file, call file, call section	F_SC_NA_1
☐	<123>:= Last section, last segment	F_LS_NA_1
☐	<124>:= Ack file, ack section	F_AF_NA_1
☐	<125>:= Segment	F_SG_NA_1
☐	<126>:= Directory {blank or X, only available in monitor (standard) direction}	F_DR_TA_1
☐	<127>:= Query Log – Request archive file	F_SC_NB_1

Type identifier and cause of transmission assignments
(station-specific parameters)

Shaded boxes: option not required.

Black boxes: option not permitted in this companion standard

Blank: functions or ASDU not used.

Mark Type Identification/Cause of transmission combinations:

"**X**" if only used in the standard direction;

"**R**" if only used in the reverse direction;

"**B**" if used in both directions.

Type identification		**Cause of transmission**																		
		1	2	3	4	5	6	7	8	9	10	11	12	13	20 to 36	37 to 41	44	45	46	47
<1>	M_SP_NA_1		X	X		X						X	X		X					
~~<2>~~	~~M_SP_TA_1~~			■		■						■	■							
<3>	M_DP_NA_1		X	X		X						X	X		X					
~~<4>~~	~~M_DP_TA_1~~			■		■						■	■							
<5>	M_ST_NA_1		X	X		X						X	X		X					
~~<6>~~	~~M_ST_TA_1~~			■		■						■	■							
<7>	M_BO_NA_1																			
~~<8>~~	~~M_BO_TA_1~~			■		■														
<9>	M_ME_NA_1	X	X	X		X									X					
~~<10>~~	~~M_ME_TA_1~~			■		■														
<11>	M_ME_NB_1	X	X	X		X									X					
~~<12>~~	~~M_ME_TB_1~~			■		■														

Type identification		Cause of transmission																		
		1	2	3	4	5	6	7	8	9	10	11	12	13	20 to 36	37 to 41	44	45	46	47
<13>	M_ME_NC_1	x	x	x		x									x					
~~<14>~~	~~M_ME_TC_1~~																			
<15>	M_IT_NA_1															x				
~~<16>~~	~~M_IT_TA_1~~																			
~~<17>~~	~~M_EP_TA_1~~																			
~~<18>~~	~~M_EP_TB_1~~																			
~~<19>~~	~~M_EP_TC_1~~																			
<20>	M_PS_NA_1																			
<21>	M_ME_ND_1																			
<30>	M_SP_TB_1			x		x						x	x							
<31>	M_DP_TB_1			x		x						x	x							
<32>	M_ST_TB_1			x		x						x	x							
<33>	M_BO_TB_1																			
<34>	M_ME_TD_1			x		x														
<35>	M_ME_TE_1			x		x														
<36>	M_ME_TF_1			x		x														
<37>	M_IT_TB_1			x												x				
<38>	M_EP_TD_1																			
<39>	M_EP_TE_1																			
<40>	M_EP_TF_1																			
<45>	C_SC_NA_1																			
<46>	C_DC_NA_1																			
<47>	C_RC_NA_1																			
<48>	C_SE_NA_1																			
<49>	C_SE_NB_1																			
<50>	C_SE_NC_1																			
<51>	C_BO_NA_1																			
<58>	C_SC_TA_1																			
<59>	C_DC_TA_1																			
<60>	C_RC_TA_1																			
<61>	C_SE_TA_1																			
<62>	C_SE_TB_1																			
<63>	C_SE_TC_1																			
<64>	C_BO_TA_1																			
<70>	M_EI_NA_1*				x															
<100>	C_IC_NA_1						x	x			x						x	x	x	x
<101>	C_CI_NA_1						x	x			x						x	x	x	x
<102>	C_RD_NA_1																			
<103>	C_CS_NA_1						x	x									x	x	x	x
~~<104>~~	~~C_TS_NA_1~~																			
<105>	C_RP_NA_1																			
~~<106>~~	~~C_CD_NA_1~~																			
<107>	C_TS_TA_1																			
<110>	P_ME_NA_1																			
<111>	P_ME_NB_1																			
<112>	P_ME_NC_1																			
<113>	P_AC_NA_1																			
<120>	F_FR_NA_1																			
<121>	F_SR_NA_1																			
<122>	F_SC_NA_1																			
<123>	F_LS_NA_1																			
<124>	F_AF_NA_1																			
<125>	F_SG_NA_1																			
<126>	F_DR_TA_1*																			
<127>	F_SC_NB_1*																			

***** Blank or X only

Basic application functions

Station initialization
(station-specific parameter, mark "**X**" if function is used)

[X] Remote initialization

Cyclic data transmission
(station-specific parameter, mark "**X**" if function is only used in the standard direction, "**R**" if only used in the reverse direction, and "**B**" if used in both directions)

[X] Cyclic data transmission

Read procedure
(station-specific parameter, mark "**X**" if function is only used in the standard direction, "**R**" if only used in the reverse direction, and "**B**" if used in both directions)

[ ] Read procedure

Spontaneous transmission
(station-specific parameter, mark "**X**" if function is only used in the standard direction, "**R**" if only used in the reverse direction, and "**B**" if used in both directions)

[X] Spontaneous transmission

Double transmission of information objects with cause of transmission spontaneous
(station-specific parameter, mark each information type "**X**" where both a Type ID without time and corresponding Type ID with time are issued in response to a single spontaneous change of a monitored object)

The following type identifications may be transmitted in succession caused by a single status change of an information object. The particular information object addresses for which double transmission is enabled are defined in a project-specific list.

[ ] Single-point information M_SP_NA_1, M_SP_TA_1, M_SP_TB_1 and M_PS_NA_1
[ ] Double-point information M_DP_NA_1, M_DP_TA_1 and M_DP_TB_1
[ ] Step position information M_ST_NA_1, M_ST_TA_1 and M_ST_TB_1
[ ] Bitstring of 32 bit M_BO_NA_1, M_BO_TA_1 and M_BO_TB_1 (if defined for a specific project)
[ ] Measured value, normalized value M_ME_NA_1, M_ME_TA_1, M_ME_ND_1 and M_ME_TD_1
[ ] Measured value, scaled value M_ME_NB_1, M_ME_TB_1 and M_ME_TE_1
[ ] Measured value, short floating point number M_ME_NC_1, M_ME_TC_1 and M_ME_TF_1

Station interrogation
(station-specific parameter, mark "**X**" if function is only used in the standard direction, "**R**" if only used in the reverse direction, and "**B**" if used in both directions).

- [X] global
- [X] group 1
- [X] group 2
- [X] group 3
- [X] group 4
- [X] group 5
- [X] group 6
- [X] group 7
- [X] group 8
- [X] group 9
- [X] group 10
- [X] group 11
- [X] group 12
- [X] group 13
- [X] group 14
- [X] group 15
- [X] group 16

Information object addresses assigned to each group must be shown in a separate table.

Clock synchronization
(station-specific parameter, mark "**X**" if function is only used in the standard direction, "**R**" if only used in the reverse direction, and "**B**" if used in both directions).

- [X] Clock synchronization
- [X] Day of week used
- [ ] RES1, GEN (time tag substituted/ not substituted) used
- [ ] SU-bit (summertime) used

optional, see 7.6

Command transmission
(object-specific parameter, mark "**X**" if function is only used in the standard direction, "**R**" if only used in the reverse direction, and "**B**" if used in both directions).

- [ ] Direct command transmission
- [ ] Direct set point command transmission
- [ ] Select and execute command
- [ ] Select and execute set point command
- [ ] C_SE ACTTERM used

- [ ] No additional definition
- [ ] Short-pulse duration (duration determined by a system parameter in the outstation)
- [ ] Long-pulse duration (duration determined by a system parameter in the outstation)
- [ ] Persistent output

- [ ] Supervision of maximum delay in command direction of commands and set point commands

[ ] Maximum allowable delay of commands and set point commands

Transmission of integrated totals
(station- or object-specific parameter, mark "**X**" if function is only used in the standard direction, "**R**" if only used in the reverse direction, and "**B**" if used in both directions).

- [X] Mode A: Local freeze with spontaneous transmission
- [X] Mode B: Local freeze with counter interrogation
- [ ] Mode C: Freeze and transmit by counter-interrogation commands
- [ ] Mode D: Freeze by counter-interrogation command, frozen values reported

- [ ] Counter read
- [ ] Counter freeze without reset
- [ ] Counter freeze with reset
- [ ] Counter reset

- [X] General request
- [X] Request counter group 1
- [X] Request counter group
- [X] Request counter group 3
- [X] Request counter group 4

Parameter loading
(object-specific parameter, mark "**X**" if function is only used in the standard direction, "**R**" if only used in the reverse direction, and "**B**" if used in both directions).

- [ ] Threshold value
- [ ] Smoothing factor
- [ ] Low limit for transmission of measured values
- [ ] High limit for transmission of measured values

Parameter activation
(object-specific parameter, mark "**X**" if function is only used in the standard direction, "**R**" if only used in the reverse direction, and "**B**" if used in both directions).

- [ ] Act/deact of persistent cyclic or periodic transmission of the addressed object

Test procedure
(station-specific parameter, mark "**X**" if function is only used in the standard direction, "**R**" if only used in the reverse direction, and "**B**" if used in both directions).

- [X] Test procedure

File transfer
(station-specific parameter, mark "**X**" if function is used).

File transfer in monitor direction

☐ Transparent file

☐ Transmission of disturbance data of protection equipment

☐ Transmission of sequences of events

☐ Transmission of sequences of recorded analogue values

File transfer in control direction

☐ Transparent file

Background scan
(station-specific parameter, mark "**X**" if function is only used in the standard direction, "**R**" if only used in the reverse direction, and "**B**" if used in both directions).

☒ Background scan

Acquisition of transmission delay
(station-specific parameter, mark "**X**" if function is only used in the standard direction, "**R**" if only used in the reverse direction, and "**B**" if used in both directions).

■ ~~Acquisition of transmission delay~~

Definition of time outs

Parameter	Default value	Remarks	Selected value
t_0	30 s	Time-out of connection establishment	**Configurable per outstation**
t_1	15 s	Time-out of send or test APDUs	**Configurable per outstation**
t_2	10 s	Time-out for acknowledges in case of no data messages $t_2 < t_1$	**Configurable per outstation**
t_3	20 s	Time-out for sending test frames in case of a long idle state	**Configurable per outstation**

Maximum range for timeouts t_0 to t_2: 1 s to 255 s, accuracy 1 s.
Recommended range for timeout t_3: 1 s to 48 h, resolution 1 s.
Long timeouts for t_3 may be needed in special cases where satellite links or dialup connections are used (for instance to establish connection and collect values only once per day or week).

Maximum number of outstanding I format APDUs *k* and latest acknowledge APDUs (*w*)

Parameter	Default value	Remarks	Selected value
k	12 APDUs	Maximum difference receive sequence number to send state variable	**Configurable per outstation**
w	8 APDUs	Latest acknowledge after receiving *w* I format APDUs	**Configurable per outstation**

Maximum range of values *k*: 1 to 32767 (2^{15}–1) APDUs, accuracy 1 APDU

Maximum range of values *w*: 1 to 32767 APDUs, accuracy 1 APDU (Recommendation: *w* should not exceed two-thirds of *k*).

Portnumber

Parameter	Value	Remarks
Portnumber	2404	**Configurable per outstation**

Redundant connections

[0] Number N of redundancy group connections used

RFC 2200 suite

RFC 2200 is an official Internet Standard which describes the state of standardization of protocols used in the Internet as determined by the Internet Architecture Board (IAB). It offers a broad spectrum of actual standards used in the Internet. The suitable selection of documents from RFC 2200 defined in this standard for given projects has to be chosen by the user of this standard.

[X] Ethernet 802.3

[ ] Serial X.21 interface

[ ] Other selection from RFC 2200:

List of valid documents from RFC 2200

1. .....
2. .....
3. .....
4. .....
5. .....
6. .....
7. etc.

9. Recommended Metering Data standards

For all Operational Metering requirements please refer to the Bilateral Connection Agreement (BCA) templates which can be found on our website at the following address. You will find the relevant section under Appendix F5 Schedule 2.

Bilateral Connection Agreement Template