SCADAPack E IEC 60870-5-101/104 Slave Technical Manual

Schneider Electric

Documentation

Table of Contents

I IEC 60870-5-101/104 Slave Technical

Version: 8.05.4

All pertinent state, regional, and local safety regulations must be observed when installing and using this product. For reasons of safety and to help ensure compliance with documented system data, only the manufacturer should perform repairs to components.

When devices are used for applications with technical safety requirements, the relevant instructions must be followed. Failure to use Schneider Electric software or approved software with our hardware products may result in injury, harm, or improper operating results.

Failure to observe this information can result in injury or equipment damage.

1 Technical Support

Support related to any part of this documentation can be directed to one of the following support centers.

Technical Support: The Americas

Available Monday to Friday 8:00am – 6:30pm Eastern Time

Toll free within North America	1-888-226-6876
Direct Worldwide	+1-613-591-1943
Email	TechnicalSupport@controlmicrosystems.com

Technical Support: Europe

Available Monday to Friday 8:30am – 5:30pm Central European Time

Direct Worldwide	+31 (71) 597-1655
Email	euro-support@controlmicrosystems.com

Technical Support: Asia

Available Monday to Friday 8:00am – 6:30pm Eastern Time (North America)

Direct Worldwide	+1-613-591-1943
Email	TechnicalSupport@controlmicrosystems.com

Technical Support: Australia

Inside Australia	1300 369 233
Email	au.help@schneider-electric.com

2 Safety Information

Read these instructions carefully, and look at the equipment to become familiar with the device before trying to install, operate, or maintain it. The following special messages may appear throughout this documentation or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.

	The addition of this symbol to a Danger or Warning safety label indicates that an electrical hazard exists, which will result in personal injury if the instructions are not followed.
	This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety messages that follow this symbol to avoid possible injury or death.

⚠DANGER

DANGER indicates an imminently hazardous situation which, if not avoided, **will result in** death or serious injury.

⚠WARNING

WARNING indicates a potentially hazardous situation which, if not avoided, **can result** in death or serious injury.

⚠CAUTION

CAUTION indicates a potentially hazardous situation which, if not avoided, **can result** in minor or moderate injury.

CAUTION

CAUTION used without the safety alert symbol, indicates a potentially hazardous situation which, if not avoided, **can result in** equipment damage..

PLEASE NOTE

Electrical equipment should be installed, operated, serviced, and maintained only by qualified personnel. No responsibility is assumed by Schneider Electric for any consequences arising out of the use of this material.

A qualified person is one who has skills and knowledge related to the construction and operation of electrical equipment and the installation, and has received safety training to recognize and avoid the hazards involved.

BEFORE YOU BEGIN

Do not use this product on machinery lacking effective point-of-operation guarding. Lack of effective point-of-operation guarding on a machine can result in serious injury to the operator of that machine.

⚠CAUTION

EQUIPMENT OPERATION HAZARD

- Verify that all installation and set up procedures have been completed.
- Before operational tests are performed, remove all blocks or other temporary holding means used for shipment from all component devices.

• Remove tools, meters, and debris from equipment.
Failure to follow these instructions can result in injury or equipment damage.

Follow all start-up tests recommended in the equipment documentation. Store all equipment documentation for future references.

Software testing must be done in both simulated and real environments.

Verify that the completed system is free from all short circuits and grounds, except those grounds installed according to local regulations (according to the National Electrical Code in the U.S.A, for instance). If high-potential voltage testing is necessary, follow recommendations in equipment documentation to prevent accidental equipment damage.

Before energizing equipment:

- Remove tools, meters, and debris from equipment.
- Close the equipment enclosure door.
- Remove ground from incoming power lines.
- Perform all start-up tests recommended by the manufacturer.

OPERATION AND ADJUSTMENTS

The following precautions are from the NEMA Standards Publication ICS 7.1-1995 (English version prevails):

- Regardless of the care exercised in the design and manufacture of equipment or in the selection and ratings of components, there are hazards that can be encountered if such equipment is improperly operated.
- It is sometimes possible to misadjust the equipment and thus produce unsatisfactory or unsafe operation. Always use the manufacturer's instructions as a guide for functional adjustments. Personnel who have access to these adjustments should be familiar with the equipment manufacturer's instructions and the machinery used with the electrical equipment.
- Only those operational adjustments actually required by the operator should be accessible to the operator. Access to other controls should be restricted to prevent unauthorized changes in operating characteristics.

3 Overview

This document describes the functionality of the SCADAPack E RTU communication drivers for IEC 60870-5-101 and IEC 60870-5-104 communication protocols.

This document should be read in conjunction with the *SCADAPack E IEC 60870-5-101 Slave Interoperability* document and *SCADAPack E IEC 60870-5-104 Slave Interoperability* document which

describe the level of support provided by the SCADAPack E RTU, and the ***IEC 60870-5-101 Companion standard*** and ***IEC 60870-5-104 Companion standard*** which describe the transmission protocol for Telecontrol equipment and systems.

The IEC 60870-5-101 Slave driver in the RTU is implemented in accordance with the IEC 60870-5-101 Companion standard, as well as the standards defined in IEC 60870-5-1 to IEC 60870-5-5.

The IEC 60870-5-104 Slave driver in the RTU is implemented in accordance with the IEC 60870-5-101 and IEC 60870-5-104 Companion standards, as well as the standards defined in IEC 60870-5-3 to IEC 60870-5-5.

As well as standard SCADA data reporting functions, the IEC 60870-5-101 and IEC 60870-5-104 drivers provide slave file transfer functionality to support remote operations such as Configuration file transfer, ISaGRAF application transfer, firmware update, etc.

IEC 60870-5-101 and IEC 60870-5-104 functionality is only activated on SCADAPack E RTUs when appropriately licensed. Both protocols are licensed together.

Requests for licensing can be directed to:

support@controlmicrosystems.com

4 Basic Features & Terminology

IEC 60870-5-101 protocol operates over serial connections. SCADAPack E RTUs can be configured to support IEC 60870-5-101 protocol as a Slave RTU device. IEC 60870-5-101 can operate on multiple serial ports.

IEC 60870-5-104 protocol operates over IP interfaces. SCADAPack E RTUs support IEC 60870-5-104 over Ethernet interfaces and PPP serial interfaces as a Slave RTU device. IEC 60870-5-104 can operate on multiple IP interfaces.

It is highly recommended that the user be familiar with the IEC60870-5-101 and -104 international standards prior to configuring the controller.

The SCADAPack E IEC 60870-5-101 / 104 driver provides a flexible interface to the RTU database and system facilities.

Terminology

The IEC 60870-5 protocols use a number of acronyms in describing data types and addressing.

The configuration of IEC 60870-5 features in the SCADAPack E RTU uses the following protocol terms:

ASDU	Application Service Data Unit	A data item at the application layer of a IEC 60870-5 protocol
ASDU Type ID	ASDU type Identifier	IEC 60870-5 protocol numeric identifier for the ASDU type
IOA	Information Object Address	The IEC index (address) of a data item

ASDU Type IDs are referred to by a Type ID number, being the protocol value of the ASDU Type ID (e.g. 1) or sometimes by an alpha-numeric mnemonic (e.g. M_SP_NA_1). The ASDU values and mnemonics are defined by the IEC international standard. See the *SCADAPack E IEC60870-5-101 Slave Interoperability Profile Document* and *SCADAPack E IEC60870-5-104 Slave Interoperability Profile Document* for more information.

5 Point Configuration

The section describes the individual point configurations that can be used to “identify” RTU points as IEC 60870-5-101/104 Slave points, and how the different ASDUs correspond to RTU points attributes.

These include descriptions for input point types including double point configurations, control points, analog point scaling, and quality descriptor support.

This section makes reference to the SCADAPack E Configurator interface.

Consult the *SCADAPack E Configuration File Format* manual for detailed description of the relevant configuration file mnemonics for generation of RTU configuration files.

In general, the configurations for RTU database points for IEC 60870-5-101/104 protocol include the following settings:

- Information Object Address (IOA) - this is a separate configuration parameter from the DNP3 point number but has a similar purpose for IEC 60870-5 protocol
- Application Service Data Unit (ASDU) Type - this is a separate configuration parameter from the DNP3 static object type but has a similar purpose
- Analog points also have an "Enable Cyclic Scan" check-box that makes analog point data available for a cyclic/periodic Station Interrogation.

The IEC 60870-5-101/104 standards define two data classes. Class 1 data is used for time tagged or spontaneously transmitted ASDUs. Class 2 data contains periodic / cyclic data.

The IEC data classes are **NOT** user selectable, and are not related to the DNP3 point configurations of the same name.

As such, the SCADAPack E configurations for *Point Data Class* **do not apply** to IEC 60870-5-101/104 communications.

Point data is included by the RTU in the response to a periodic / cyclic requests, at the rates set by the *Background Period* and *Cyclic Period* times. Points with an IEC IOA address are returned in response to the next station interrogation when the *Background Period* time has elapsed. Analog points set for " *Enable Cyclic Scan*" are also returned to the master when the Cyclic Period time has elapsed (usually much more frequently than the *Background Period)*.

5.1 Binary Point Configuration

The configuration attributes for a binary point are listed as follows:

- Information Object Address (IOA). This attribute needs to be a **unique non-zero** value in the range of 1 – 65535.
- ASDU Type. Valid ASDU types for binary points are as follows:
  - Type ID 1: M_SP_NA_1 – Single Point Information
  - Type ID 3: M_DP_NA_1 – Double Point Information
  - Type ID 45 : C_SC_NA_1 – Single Command
  - Type ID 46 : C_DC_DA_1 – Double Command
  - Type ID 47 : C_RC_NA_1 – Regulating Step Command.
  - Type ID 58 : C_SC_TA_1 – Single Command with Time Tag (104 only)
  - Type ID 59 : C_DC_TA_1 – Double Command with Time Tag (104 only)
  - Type ID 60 : C_RC_TA_1 – Regulating Step Command with Time Tag (104 only)

See Single Point ASDU Types for information on single points.
See Double Point ASDU Types for information on double points.

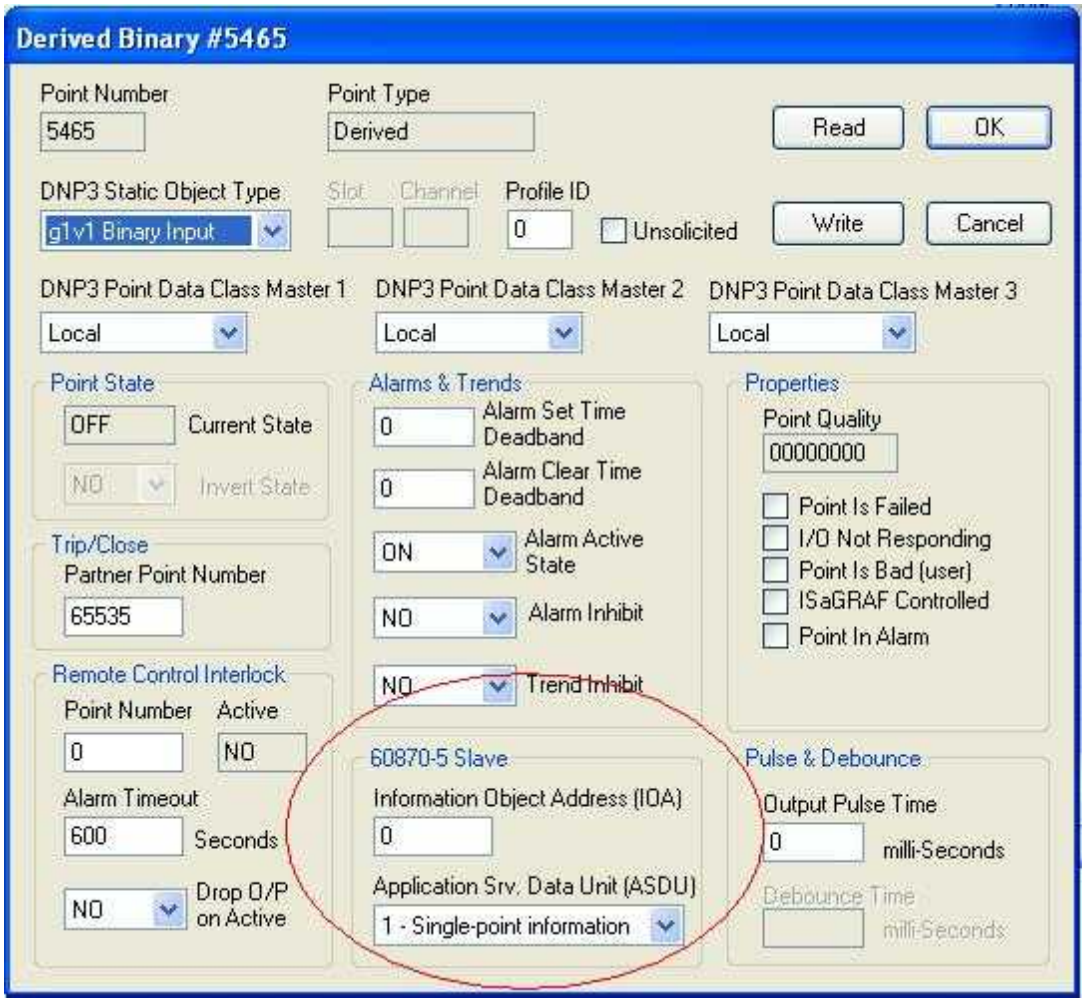

Figure 5.4: Binary Point IEC Configurations

5.1.1 Single Point ASDU Types

Single point types ASDUs include Information Objects that reference a single Information Object Address (IOA) which maps to a single SCADAPack E binary configuration point.

ASDU Type ID 1: M_SP_NA_1 - Single Point Information

For ASDU Type ID 1 (Single Point Information), the value reported in the *SPI* of the Information Object is derived from the *Current State* of the binary point.

The IV bit of the quality descriptor (SIQ) is mapped to the *Point Is Failed* property of the binary configuration point.

The NT, SB, and BL bits in the quality descriptor (SIQ) are not referenced.

ASDU Type ID 45: C_SC_DA_1 - Single Command

The following table determines how a binary output point is controlled for *Single Command* type ASDU.

Table 7.1: ASDU Type ID 45 : Control State Table

ASDU 45				RTU Binary Output
Single Command State (SCS)	SCS Description	Qualifier of Command (QU)	QU Description	
0	OFF	0	No additional definition	Latched OFF
		1	Short pulse duration	Pulsed ON (Short)
		2	Long pulse duration	Pulsed ON (Long)
		3	Persistent Output	Latched OFF
1	ON	0	No additional definition	Latched ON
		1	Short pulse duration	Pulsed ON (Short)
		2	Long pulse duration	Pulsed ON (Long)
		3	Persistent Output	Latched ON

ASDU Type ID 58: C_SC_TA_1 - Single Command with Time Tag (-104 only)

As for Type ID 45 except that the command is time tagged and only valid for the **Command Age** time.

Also see Command Age.

5.1.2 Double Point ASDU Types

When a binary point is configured as a double point ASDU type, i.e. Type ID 3 or Type ID 46, two RTU configuration points are referenced with contiguous database point numbers.

The configuration point with the lower index point number **needs** to be configured with the IEC IOA and the correct ASDU type.

The other point (i.e. the numerically next database point number) does NOT require any IEC 60870-5-101/104 configurations, and need **NOT** have an assigned IOA, otherwise a configuration error is flagged using the system error code point. See ***Applying Configurations*****.**

Section ***Double Point ASDU Types*** includes examples of double point configurations.

- ***ASDU Type ID 3: M_DP_NA_1 - Double Point Information, ASDU Type ID 60: C_RC_TA_1 - Regulating Step Command with Time Tag (104 only), & ASDU Type ID 59: C_DC_TA_1 - Double Command with Time Tag (104 only)***
- ***ASDU TypeID 46: C_DC_DA_1 - Double Command***
- ***ASDU TypeID 47: C_RC_NA_1 - Regulating Step Command***

5.1.2.1 ASDU Type ID 3, 60, & 59

ASDU Type ID 3: M_DP_NA_1 - Double Point Information

Consider the following configurations as an example

Derived Binary 41000 (i.e. DNP Index 41000)

- ASDU Type = 3 (Double Point Information)
- IOA = 22000

Derived Binary 41001 (i.e. DNP Index 41001)

- ASDU Type = 1 (Single Point Information)
- IOA = 0.

The configurations for Derived Binary 41001 are default values. The the “second” point configuration in a double point pair, is modified by the RTU on start-up whereby the ASDU type is changed from the default value (1) to be 3, i.e. *Double Point Information*.

The following state table determines how the data is returned for IOA 22000 as a *Double Point Information* type ASDU.

Table 7.2: ASDU Type ID 3 : State Table

Derived Binary 41000 (Current State)	Derived Binary 41001 (Current State)	DPI (Double Point Information)	Double Point Information Description
0	0	0	indeterminate or intermediate state
1	0	1	determined state OFF
0	1	2	determined state ON
1	1	3	indeterminate state

The IV bit of the quality descriptor (SIQ) is mapped to the logical OR of the *Point Is Failed* property of the two binary configuration points. The NT, SB, and BL bits in the quality descriptor (SIQ) are not referenced.

ASDU Type ID 60: C_RC_TA_1 - Regulating Step Command with Time Tag (-104 only)

As Type ID 47 except that the command is time tagged and only valid for the **Command Age** time.

ASDU Type ID 59: C_DC_TA_1 - Double Command with Time Tag (-104 only)

As Type ID 46 except that the command is time tagged and only valid for the **Command Age** time.

5.1.2.2 ASDU Type ID 46

Consider the following configurations as an example

Physical Binary Output 8 (i.e. DNP Index 8)

- ASDU Type = 46 (Double Command)
- IOA = 10600

Physical Binary Output 9 (i.e. DNP Index 9)

- ASDU Type = X (any value)
- IOA = 0

The configurations for Physical Binary Output 9 are default values, i.e. the second point in a *double command* pair does NOT have to be configured as a *double command* ASDU type. The following state table determines how the output points are controlled for IOA 10600 as a *Double Command* type ASDU.

Table 7.3: ASDU Type ID 46 : Control State Table (using example config)

ASDU 46				RTU Binary Outputs	
Double Command State (DCS)	DCS Description	Qualifier of Command (QU)	QU Description	Binary Output 8 (State)	Binary Output 9 (State)
0	Not permitted	X (any value)	-	No action	No action
1	OFF	0	No additional definition	Latched ON	Latched OFF
		1	Short pulse duration	Pulsed ON (Short)	No action
		2	Long pulse duration	Pulsed ON (Long)	No action
		3	Persistent Output	Latched ON	Latched OFF
2	ON	0	No additional definition	Latched OFF	Latched ON
		1	Short pulse duration	No action	Pulsed ON (Short)
		2	Long pulse duration	No action	Pulsed ON (Long)
		3	Persistent Output	Latched OFF	Latched ON
3	Not permitted	X (any value)	-	No action	No action

5.1.2.3 ASDU Type ID 47

Consider the following configurations as an example

Physical Binary Output 15 (i.e. DNP Index 15)

- ASDU Type = 47 (Regulating Step Command)
- IOA = 10700

Physical Binary Output 16 (i.e. DNP Index 16)

- ASDU Type = X (any value)
- IOA = 0

The configurations for Physical Binary Output 16 are default values, i.e. the second point in a *regulating step* (*double command)* pair does NOT have to be configured as a *Regulating Step command* ASDU type. The following state table determines how the output points are controlled for IOA 10700 as a *Regulating Step* type ASDU.

Table 7.4: ASDU Type ID 47 : Control State Table (using example config)

ASDU 47				RTU Binary Outputs	
Regulating Step Command State (RCS)	RCS Description	Qualifier of Command (QU)	QU Description	Binary Output 15 (State)	Binary Output 16 (State)
0	Not permitted	X (any value)	-	No action	No action
1	next Step LOWER	0	No additional definition	Latched ON	Latched OFF
		1	Short pulse duration	Pulsed ON (Short)	No action
		2	Long pulse duration	Pulsed ON (Long)	No action
		3	Persistent Output	Latched ON	Latched OFF
2	next Step LOWER	0	No additional definition	Latched OFF	Latched ON
		1	Short pulse duration	No action	Pulsed ON (Short)
		2	Long pulse duration	No action	Pulsed ON (Long)
		3	Persistent Output	Latched OFF	Latched ON
3	Not permitted	X (any value)	-	No action	No action

5.2 Analog Point Configuration

The valid configuration attributes for an analog point are listed as follows

- Information Object Address (IOA). This attribute needs to be a **unique non-zero** value in the range of 1 – 65535.
- ASDU Type. Valid ASDU types for analog points are listed as follows
  - Type ID 5: M_ST_NA_1 – Step Position Information
  - Type ID 9: M_ME_NA_1 – Measured Value, normalized value
  - Type ID 11: M_ME_NB_1 – Measured Value, scaled value
  - Type ID 13: M_ME_NC_1 – Measured Value, short floating point value
  - Type ID 21: M_ME_ND_1 – Measured Value, normalized value without quality descriptor
  - Type ID 48: C_SE_NA_1 – Set point command, normalized value
  - Type ID 49: C_SE_NB_1 – Set point command, scaled value
  - Type ID 50: C_SE_NC_1 – Set point command, short floating point value
  - Type ID 61: C_SE_TA_1 – Set point command, normalized value with Time tag
  - Type ID 62: C_SE_TB_1 – Set point command, scaled value with time tag
  - Type ID 63: C_SE_TC_1 – Set point command, short float, time tag

- "Enable Cyclic Scan" check-box makes the value of the analog point available for a cyclic Station Interrogation - at the **Cyclic Period** set in the Master Configuration.

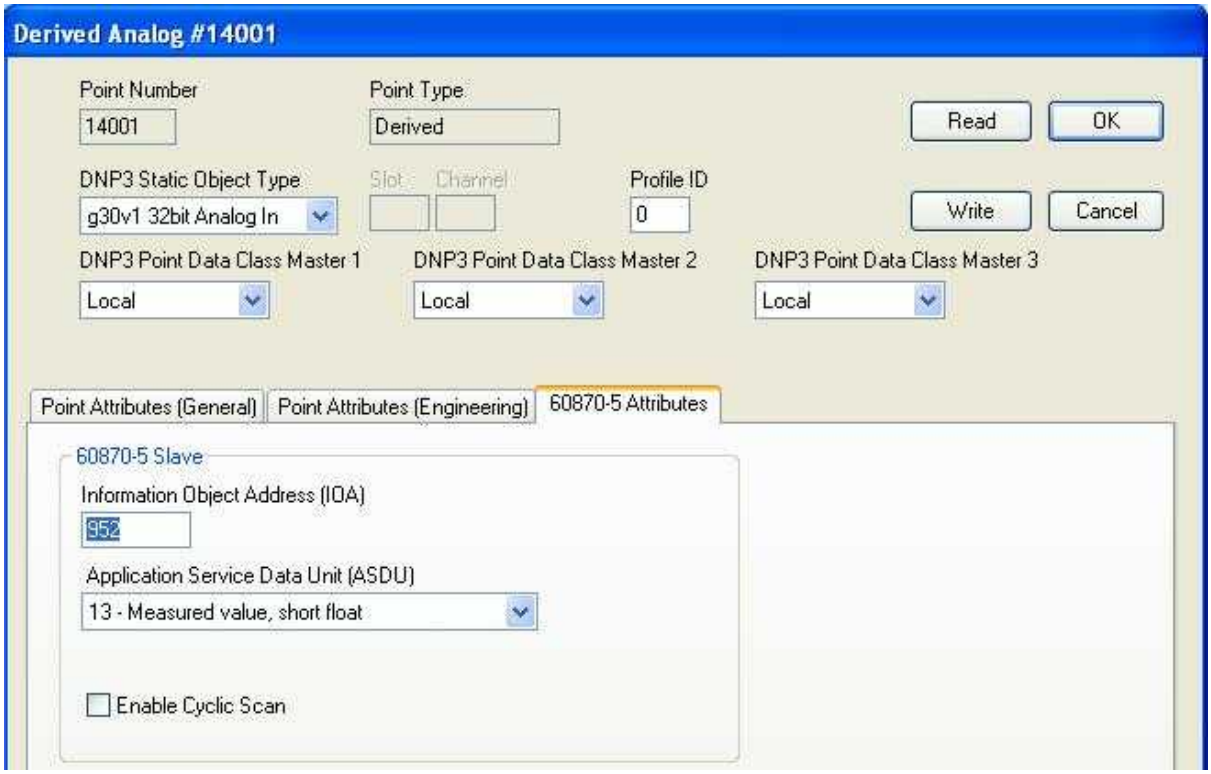

Figure 5.5: Analog Point IEC Configuration

5.2.1 Analog Point ASDU Types

Analog configuration points may be identified as scaled, normalized or floating points in IEC 60870-5-101 slave responses.

The following sections describe how the RTU point's current value is represented in these ASDU types.

Normalized and Scaled ASDU Types

The Normalized and Scaled ASDU types include a 16-bit value in the Information Object and apply to analog point integer values in the SCADAPack E RTU database.

The literal interpretation of this value is specified in the IEC 60870-5-101 standard, being IEC F16 (Fixed Point) and I16 (Integer) information elements as defined in IEC 60870-5-4.

The *Current Integer Value* of the analog configuration point is mapped to this 16-bit value as shown as in the following table.

The *Raw Min* and *Raw Max* attributes are the standard scaling parameters for RTU analog points. These default to values of 0 and 10000 respectively but may be set to any value for use in the RTU. When converted for transmission via IEC60870-5 protocols, the following representations are used :

Table 7.5: Analog Point Integer Scaling - Normalized and Scaled ASDU Types

RTU Analog Point Current Integer Value	IEC fixed point math format **ASDU 21, measured value (normalized val)**	IEC integer format **ASDU 11, measured value (scaled val)**
Raw Min	-1	-32768 (-2^{15})
Raw Max	$1 - 2^{-15}$	32767 ($2^{15} - 1$)

The integer values for an analog point presented in IEC 60870-5 protocols are bipolar (signed) and are either fixed point math (ASDU 21) or integer scaled (ASDU 11) from the Raw Min. to Raw Max. range of the analog point. Choose the ASDU type according to the requirement of the master station.

Example 1: for an analog point with Raw Min = 0, Raw Max = 10000, a *current integer value* of 5000 would map to a value of 0 in an ASDU 21 normalized value Information Object, and a value of 0 in an ASDU 11 scaled value Information Object.

Example 2: to send an analog point in ASDU 11 format and send the same value as in the RTU analog point *current integer value*, set Raw Min = -32768, Raw Max = 32768.

If the *Current Integer Value* is outside of the reportable 16-bit range, the included value is clamped to the appropriate IEC format end point, and the OVERFLOW bit in the quality descriptor is set.

Floating Point ASDU Types

The Floating Point ASDU types reference a short float value in the Information Object whereby the *Current Engineering Value (float value)* of the analog point is mapped to the IEC point value as defined in IEC 60870-5-4 R32.23 information elements .

Step Position ASDU (M_ST_NA_1)

The *Current Integer Value* of the analog point is directly mapped to the 7-bit *Value* included on the Information Object. If the *Current Integer Value* is outside of the valid *Value* range, i.e. -64 to 63, the OVERFLOW bit in the quality descriptor (QDS) is set. The *Transient* bit in the *VTI* field is not referenced.

Quality Descriptor Support

For each of the supported *analog* type ASDUs, there is limited support for quality descriptor fields.

- The *IV* bit of the quality descriptor (QDS) is mapped to the *Point Is Failed* property of the analog configuration point.
- The OV bit is set if the current value of the point is beyond the reportable range according to the specific ASDU type.
- The NT, SB, and BL bits in the quality descriptor (QDS) are not referenced.

5.3 Counter Point Configuration

The valid configuration attributes for a counter point are listed as follows

- Information Object Address (IOA). This attribute needs to be a **unique non-zero** value in the range of 1 – 65535.
- ASDU Type = **ID 15 : M_IT_NA_1 – Integrated Totals**. This is the only ASDU type allowed for RTU counter points.

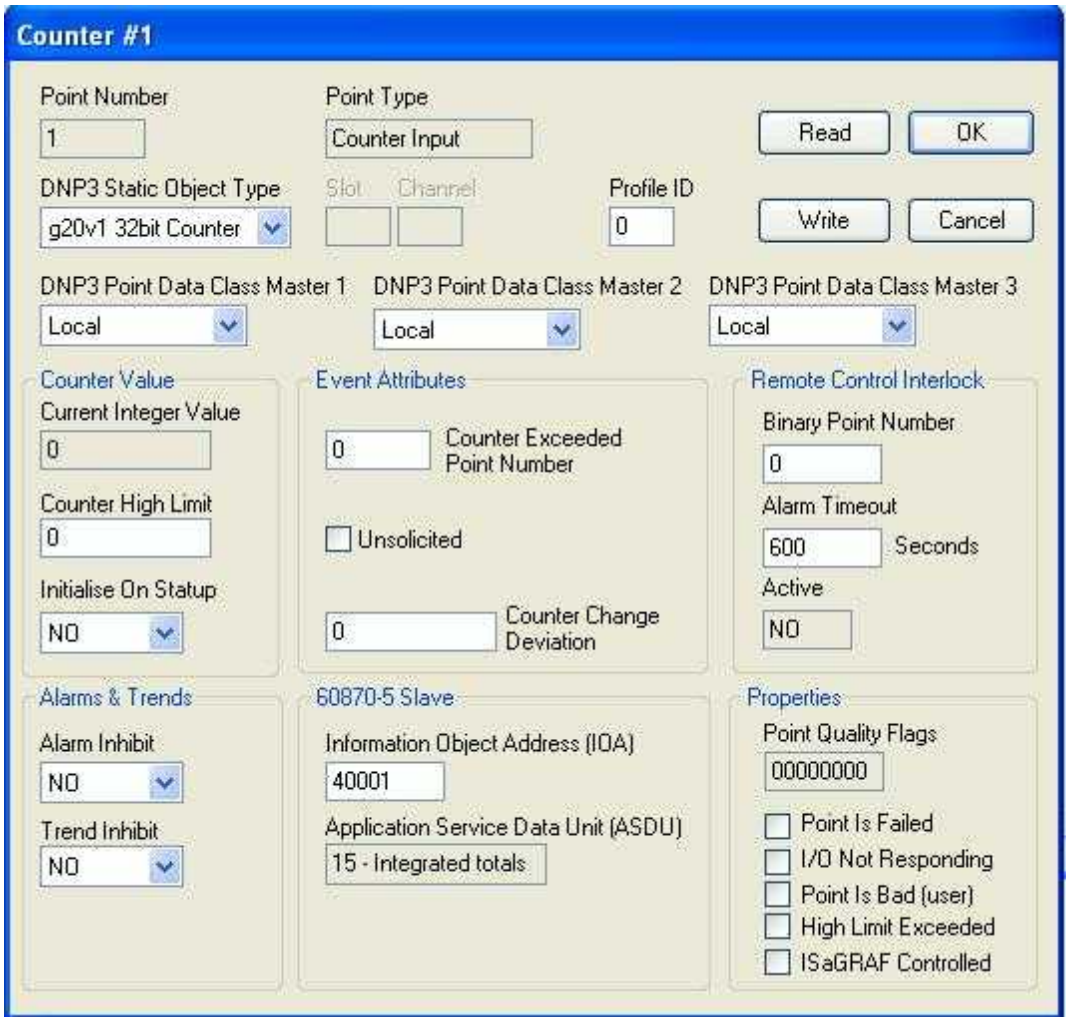

Figure 5.6: Counter Point Configurations

5.3.1 Counter Point ASDU Types

The counter points may only be configured as ASDU type 15, i.e. M_IT_NA_1 (Integrated Totals). The counter values reported in this ASDU type are frozen values. Counter (integrated total) values are retrieved from the RTU using Counter Interrogation Commands. For more details regarding counter support in the RTU's 60870-5-101 Slave driver, refer to Section ***ASDU TypeID 100, 101, 103, 104, 105, & 107* (ASDU Type ID 101 : C_CI_NA_1 – Counter Interrogation Command)**.

ASDU Type ID 15: M_IT_NA_1 - Integrated Totals

The information object in the Integrated Totals ASDU includes a **signed** 32-bit value, which is identified as a Binary Counter Reading (BCR). The *Current Integer Value* of the counter point (unsigned 32-bit) is copied into the cached frozen value for the particular *Information Object Address* (IOA) when a "Counter Freeze" request is made via a Counter Interrogation Command. For every COUNTER FEEZE command received from the relevant Master, the sequence number (SQ) for that IOA is incremented.

The invalid (*IV)* bit included in the information object is mapped to the *Point Is Failed* property of the counter configuration point.

The Counter Adjusted (*CA*) bit included in the information object is set if the counter value has been reset due to a COUNTER FREEZE request, and is only asserted for the first READ after the COUNTER FREEZE. The *CA* bit is also set on RTU start-up if the *Counter Reset* attribute of the counter configuration point was set to TRUE (see the *SCADAPack E RTU Configuration Technical Reference Manual* for more details regarding counter point attributes).

The Carry (CY) bit is not referenced by the RTU's 60870-5-101 Slave driver.

6 System Configuration

The primary interface for configuring the SCADAPack E RTU IEC 60870-5-101/104 Slave is the SCADAPack E Configurator software.

- ***IEC60870-5-101 Serial Port Configurations***
- ***IEC 60870-5-101 / -104 System Configurations***
- ***Applying Configurations & Configuration Diagnostics***

Compatibility between SCADAPack E or SCADAPack E Configurator versions 7.84 (and newer) and previous versions.

In previous versions, 7.83 or earlier, the ASDU Size, ASDU Address and the IOA Size did not use sperate system points.These parameters were set to default values and were not configurable. With SCADAPack E firmware version 7.84 and SCADAPack E Configurator version 7.84 the ASDU size and address and the IOA size have individual system points and are user configurable. When upgrading to SCADAPack E or SCADAPack E Configurator versions 7.84 and newer some important compatibility questions need to be considered. See the Compatibility between SCADAPack E or SCADAPack E Configurator versions 7.84 (and newer) and previous versions topic for full details.

6.1 IEC60870-5-101 Serial Port Configurations

The SCADAPack E RTU's IEC 60870-5-101 Slave functionality is only supported on RTU serial ports.

In order to define a specific serial port as an IEC 60870-5-101 Slave port, the *Port Function* needs to be set to "**IEC--101 Slave**"**.** The RTU must then be restarted to allow the IEC 60870-5-101 driver to start.

Figure 5.2: SCADAPack E Configurator Ports Page IEC60870-5-101 Settings

The *Port Mode* must be to RS-232 and the *Port Data Mode* needs to use E**ven parity** (as specified in the IEC 60870-5-101 Companion standard).

Figure 5.2 shows an example configuration from the Ports Page in the SCADAPack E Configurator.

Consult the *SCADAPack E Configuration Technical Reference Manual* for a detailed list of the serial port system points.

6.2 IEC 60870-5-101 System Configurations

The IEC 60870-5-101/104 Slave configurations support communications with up to two (2) IEC 60870-5-101 Masters and two (2) IEC 60870-5-104 Masters to a total of 4. The first 101 master and first 104 master share common configurations. The second 101 master and second 104 master share common configurations. Each Master session has its own event list such that a given IEC 60870-5-101/104 event will NOT be removed from the RTU's 60870-5-101/104 event list until it has been retrieved by every enabled Master session.

Figure 5.3 shows a screen shot of the 60870-5-101 page in the SCADAPack E Configurator.

The "***Event Enabled ASDU type***" configurations apply to every Master session.

The RTU's IEC 60870-5-101/104 Slave driver needs to be restarted for any changed system configurations to take effect. SCADAPack E Configurator automatically performs this operation when a configuration containing changed IEC configurations are downloaded to the RTU.

Consult the *SCADAPack E Configuration Technical Reference* manual for detailed information on IEC internal system configuration points.

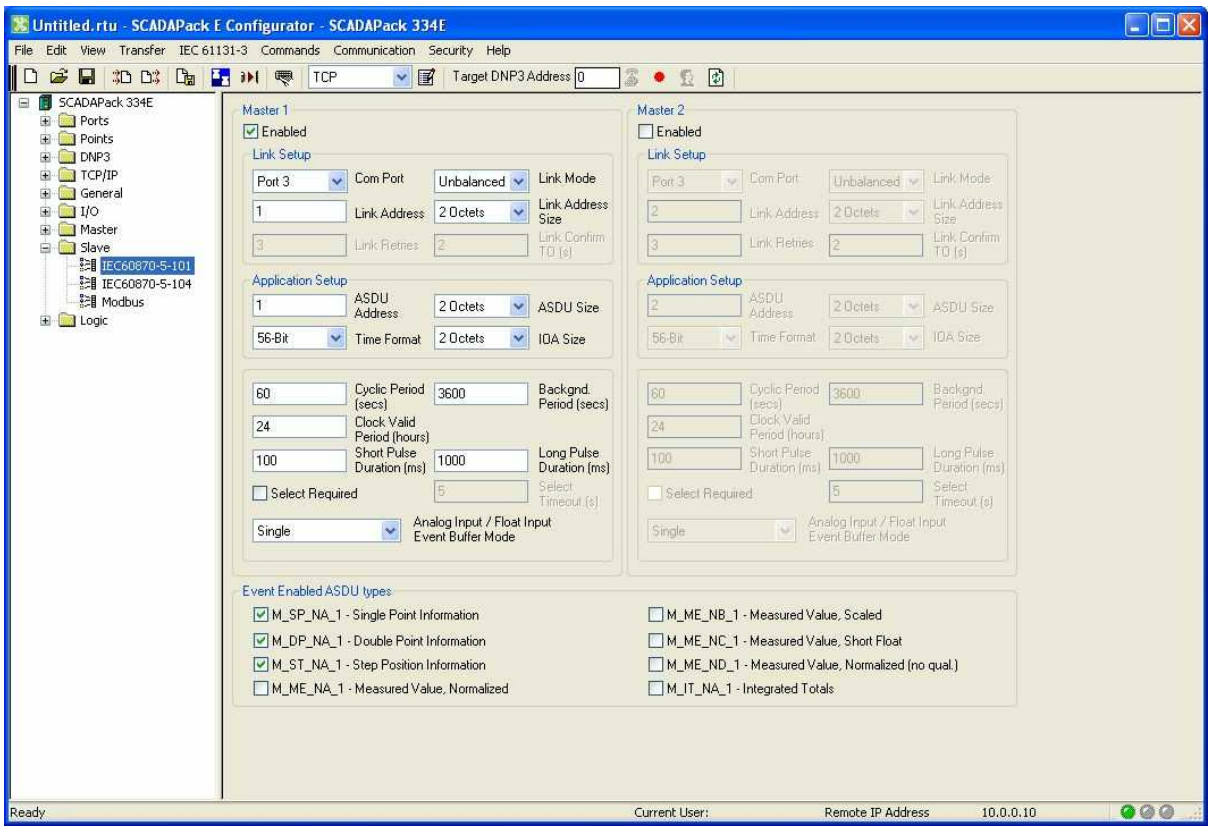

Figure 5.3: SCADAPack E Configurator - IEC 60870-5-101 Page

The IEC 60870-5-101 page in SCADAPack E Configurator allows for configuration of up to 2 Master sessions in the RTU.

The following sections describe each field shown in ***Figure 5.3***.

- ***Master Enable and Link Setup***

- ***Application Setup***
- ***Background Period, Cyclic Period Clock Period and Short & Long Pulse Duration***
- ***Event Enabled ASDU Types***
- ***System Event Capacity***
- ***System Point Listing***

6.2.1 Master Enable and Link Setup

Master Enabled

The **Master Enabled** checkbox determines whether the respective slave session (for the specified Master address) is enabled in the RTU. The default configurations are listed as follows

- Master 1 Enabled = ON
- Master 2 Enabled = OFF.

If a given Master session is NOT enabled, the RTU will NOT respond to any messages received on the specified COM port for that Master session.

Com Port

The **Com Port** field specifies the serial COM port on the RTU for the relevant Master session. For this configuration to be valid, the specified Port needs to also be configured with a PORT FUNCTION of "**IEC--101 Slave**" on the SCADAPack E Configurator Ports Page.

If both Master sessions are enabled, they can use the same **COM Port only** if they are both running IEC 60870-5-101 Unbalanced Mode. (See Link Mode below).

Link Address

The **Link Address** configuration field is used to assign the Link addresses for the relevant Master session. The valid range of values for this configuration field is dependent on the Link Address Size field (see Section Link Address Size below), i.e. 0 – 255 for 1 octet Link Address size and 0 – 65535 for 2 octet Link Address size.

Link Retries

The **Link Retries** configuration field is only relevant when in **Balanced** mode.

This field specifies the number of link retries for a given message before reporting that particular message unsuccessful. The default value for this field is 3. Valid values are 0 to 65535.

This field is only used for -101 slave sessions as the -104 protocol has no IEC link layer.

Link Mode

The **Link Mode** configuration field sets the **Link Mode** for the respective Master session.

The Link Mode may be set to one of the following Options

- Unbalanced (default)
- Balanced.

When operating in **Unbalanced** mode, communications are initiated by the Master whereby the Master typically makes frequent requests for data (Class 1 or Class 2 polls).

When operating in **Balanced** Mode, the Master does NOT initiate communications, and data is reported by the RTU as required by its configurations. In this mode, the RTU initiates communications typically with a **Request Link Status** message.

Irrespective of the **Link Mode**, the RTU (IEC 60870-5-101 Slave) presents data in responses according to its configurations.

SCADAPack E data configured with a valid IEC IOA is reported every **Background Period**. See ***Background Period***

"Cyclic" data is reported every **Cyclic Period**. See Section ***Cyclic Period***

Event data is reported spontaneously as required.

This field is only used for -101 slave sessions. The -104 protocol has no IEC protocol link layer.

Link Address Size

The **Link Address Size** configuration field sets the size of the Link Address field specified in *Link* transactions for the relevant Master session.

The Link Address may be set to one of the following options

- None (invalid in Unbalanced mode)
- 1 Octet
- 2 Octets (default).

This field is only used for -101 slave sessions as the -104 protocol has no IEC link layer.

Link Confirm Time Out

The **Link Confirm Timeout** configuration field is specified in seconds, and is only relevant when in **Balanced** mode.

This field specifies the time (in seconds) that the RTU's IEC 60870-5-101 Slave driver will wait for a response to a Link message before issuing a retry. The default value for this field is 2 seconds. Valid values are 0 to 65535.

This field is only used for -101 slave sessions as the -104 protocol has no IEC link layer.

6.2.2 Application Setup

ASDU Address

The **ASDU Address** configuration field is used to assign the ASDU addresses for the relevant Master session. The valid range of values for this configuration field is dependent on the ASDU Address Size field (see Section ASDU Address Size below), i.e. 1 – 255 for 1 octet ASDU Address size and 1 – 65535 for 2 octet ASDU Address size.

Time Format

The **Time Format** configuration field determines which timestamp format is included with generated event data. The Time Format may be set to one of the following options

- 56-bit (default)
- 24-bit

The 56-bit *Time Format* is an absolute time format, whereas the 24-bit *Time Format* is an incremental time format that only specifies minutes and milliseconds.

This field is only used for 101 slave sessions, as the -104 protocol uses 56-bit time format.

ASDU Size

The **ADSU Size** configuration field sets the size of the ASDU Address field for the relevant Master session.

The ASDU Address Size may be set to one of the following options:

- 1 Octet
- 2 Octets (default)

This field is only used for -101 slave sessions as for the -104 protocol; it has a fixed length of 2 octets (bytes).

The ASDU size must be set to the same value in both the master station and the slave station for communication to work between the stations.

IOA Size

The **IOA Size** configuration field sets the size of the IOA field for the relevant points.

The IOA Size may be set to one of the following options:

- 1 Octet
- 2 Octets (default)
- 3 Octets

This field is only used for -101 slave sessions as for the -104 protocol; it has a fixed length of 3 octets (bytes).

A value of 0 is not valid for -101 or -104 protocols. Writing a 0 to the IOA Size will result in:

1. ASDU Address being set to the same value as the configured Link Address for the master
2. ASDU Address Size being set to the default value of 2 for the master
3. IOA size set to the default value of 2 for the master

It should be noted that a value of 0 will not remain visible in this status point as it will be changed to a

value of 2. Accepting a value of 0 is being permitted for compatibility reasons. Please refer to the compatibility section for more details.

The IOA size must be set the to the same value in both the master station and the slave station for communication to work between the stations.

6.2.3 Background Period, Cyclic Period, Clock Period and Short & Long Pulse Duration

Cyclic Period

The **Cyclic Period** configuration field is specified in seconds and determines the rate at which Cyclic data is returned by the RTU's IEC 60870-5-101 driver.

Cyclic data is identified as those **analog** RTU configuration points which have a valid non-zero Information Object Address, and whose ***Enable Cyclic Scan*** attribute is set to TRUE. See Analog Point Attributes.

This default value for this field is 60 seconds.

Background Period

The **Background Period** configuration field is specified in seconds and determines the rate at which Background data is returned by the RTU's IEC 60870-5-101/104 driver.

Background data is defined as RTU configuration points which have a valid non-zero Information Object Address (IOA) and a valid ASDU Type. This default value for this field is 3600 seconds.

Clock Valid Period

The **Clock Valid Period** field sets the period of time for which timestamps are considered valid after receiving a clock synchronization command.

When the RTU's IEC 60870-5-101/104 driver starts, timestamps issued are identified as invalid until a clock synchronization command has been received for that specific master session.

The default value for this field is 24 hours.

Short Pulse Duration

The **Short Pulse Duration** configuration field is specified in milliseconds and determines the PULSE ON duration utilized when a valid binary control is received by the RTU, when the ***qualifier of command*** for the relevant control object specifies *Short Pulse Duration*. This default value for this field is 100 milliseconds.

Long Pulse Duration

The **Long Pulse Duration** configuration field is specified in milliseconds and determines the PULSE ON duration utilized when a valid binary control is received by the RTU, when the ***qualifier of command*** for the relevant control object specifies *Long Pulse Duration*. This default value for this field is 1000 milliseconds (1 second).

Select Required

The **Select Required** configuration field specifies whether or not a Select message is required before an Execute message in order to invoke the specified control.

If **Select Required** is set to TRUE, then a **Select** message needs to first be issued, and then followed by an **Execute** message.

The **Execute** message must be received within the **Select Timeout** (see Select Timeout below) period for the control to be invoked.

If **Select Required** is set to FALSE, then an **Execute** message only is required for the control to be

invoked.

Select Timeout

The **Execute** command needs to be received within this period after the **Select** command is received.

The **Select Timeout** configuration field is specified in seconds.

If an **Execute** command (matching a recently received **Select** command) is not received within this period then the control operation is aborted.

The default value for this field is 5 seconds.

6.3 IEC 60870-5-104 System Configuration

The IEC 60870-5-101/104 Slave configurations support communications with up to two (2) IEC 60870-5-101 Masters and two (2) IEC 60870-5-104 Masters to a total of 4. The first 101 master and first 104 master share common configurations. The second 101 master and second 104 master share common configurations. Each Master session has its own event list such that a given IEC 60870-5-101/104 event will NOT be removed from the RTU's 60870-5-101/104 event list until it has been retrieved by every enabled Master session.

Figure 5.4 shows a screen shot of the 60870-5-104 page in the SCADAPack E Configurator.

The "***Event Enabled ASDU type***" configurations apply to every Master session.

The RTU's IEC 60870-5-101/104 Slave driver needs to be restarted for any changed system configurations to take effect. SCADAPack E Configurator automatically performs this operation when a configuration containing changed IEC configurations are downloaded to the RTU.

Consult the *SCADAPack E Configuration Technical Reference* manual for detailed information on IEC internal system configuration points.

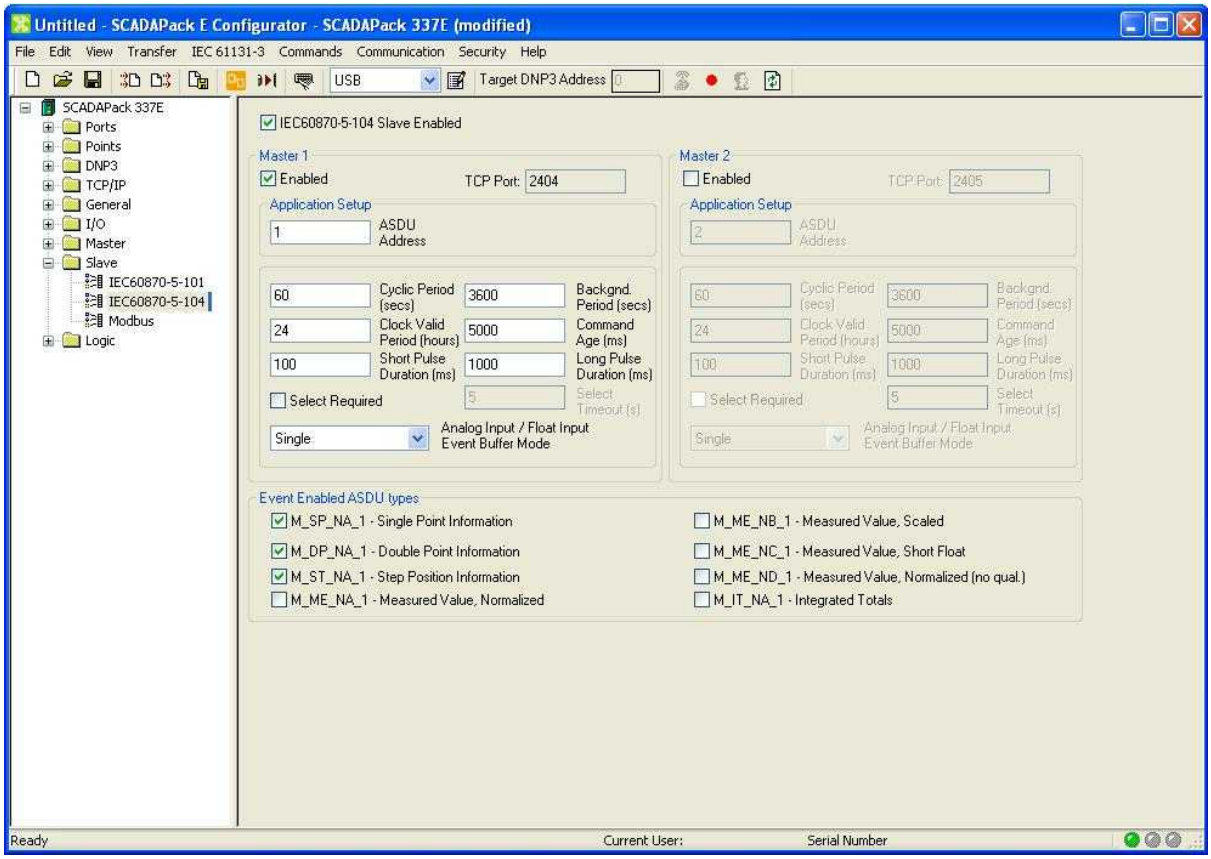

Figure 5.4: SCADAPack E Configurator - IEC 60870-5-104 Page

The IEC 60870-5-104 page in SCADAPack E Configurator allows for configuration of up to 2 Master sessions in the RTU.

The following sections describe each field shown in **Figure 5.4**.

- ***Master Enable and TCP Port Setup***

- ***Application Setup***
- ***Background Period, Cyclic Period, Clock Period, Command Age and Short & Long Pulse Duration***
- ***Event Enabled ASDU Types***
- ***System Event Capacity***
- ***System Point Listing***

6.3.1 Master Enable and TCP Port Setup

Master Enabled

The **Master Enabled** checkbox determines whether the respective slave session (for the specified Master address) is enabled in the RTU. The default configurations are listed as follows

- Master 1 Enabled = ON
- Master 2 Enabled = OFF.

If a given Master session is NOT enabled, the RTU will NOT respond to any messages received on the specified COM port for that Master session.

TCP Port

The **TCP Port** configuration field sets the TCP port that the master sessions will listen to.

To establish a connection, a 104 Master will attempt a TCP connection to the appropriate IP address using the TCP port listed below.

- 104 Master session 1 listens on TCP port **2404**
- 104 Master session 2 listens on TCP port **2405**

6.3.2 Application Setup

ASDU Address

The **ASDU Address** configuration field is used to assign the ASDU addresses for the relevant Master session. The valid range of values for this configuration field is dependent on the ASDU Address Size field (see Section ASDU Address Size below), i.e. 1 – 255 for 1 octet ASDU Address size and 1 – 65535 for 2 octet ASDU Address size.

6.3.3 Background Period, Cyclic Period, Clock Period, Command Age and Short & Long Pulse Duration

Cyclic Period

The **Cyclic Period** configuration field is specified in seconds and determines the rate at which Cyclic data is returned by the RTU's IEC 60870-5-101 driver.

Cyclic data is identified as those **analog** RTU configuration points which have a valid non-zero Information Object Address, and whose ***Enable Cyclic Scan*** attribute is set to TRUE. See Analog Point Attributes.

This default value for this field is 60 seconds.

Background Period

The **Background Period** configuration field is specified in seconds and determines the rate at which Background data is returned by the RTU's IEC 60870-5-101/104 driver.

Background data is defined as RTU configuration points which have a valid non-zero Information Object Address (IOA) and a valid ASDU Type. This default value for this field is 3600 seconds.

Clock Valid Period

The **Clock Valid Period** field sets the period of time for which timestamps are considered valid after receiving a clock synchronization command.

When the RTU's IEC 60870-5-101/104 driver starts, timestamps issued are identified as invalid until a clock synchronization command has been received for that specific master session.

The default value for this field is 24 hours.

Command Age

The **Command Age** configuration field is specified in milliseconds.

Time tagged commands need to have a time tag no older than this period. If a time tagged command is older than this period allows then the control operation is not taken. The default value for this field is 30000 milliseconds.

Short Pulse Duration

The **Short Pulse Duration** configuration field is specified in milliseconds and determines the PULSE ON duration utilized when a valid binary control is received by the RTU, when the ***qualifier of command*** for the relevant control object specifies *Short Pulse Duration*. This default value for this field is

100 milliseconds.

Long Pulse Duration

The **Long Pulse Duration** configuration field is specified in milliseconds and determines the PULSE ON duration utilized when a valid binary control is received by the RTU, when the ***qualifier of command*** for the relevant control object specifies *Long Pulse Duration*. This default value for this field is 1000 milliseconds (1 second).

Select Required

The **Select Required** configuration field specifies whether or not a Select message is required before an Execute message in order to invoke the specified control.

If **Select Required** is set to TRUE, then a **Select** message needs to first be issued, and then followed by an **Execute** message.

The **Execute** message must be received within the **Select Timeout** (see Select Timeout below) period for the control to be invoked.

If **Select Required** is set to FALSE, then an **Execute** message only is required for the control to be invoked.

Select Timeout

The **Execute** command needs to be received within this period after the **Select** command is received.

The **Select Timeout** configuration field is specified in seconds.

If an **Execute** command (matching a recently received **Select** command) is not received within this period then the control operation is aborted.

The default value for this field is 5 seconds.

6.4 Event ASDUs

ASDUs without Time Tags

Each configuration point in the RTU may be configured as an IEC 60870-5-101/104 Slave point.

As there is no fixed limit to the number of configuration points that may exist in the RTU, the upper bound of system capacity is determined by available configuration memory and operational design considerations, e.g.. the baud rate of the connection and the correct background and cyclic periods for proper operation, which therefore determines the amount of data that may be transported using the available bandwidth.

ASDUs with Time Tags (Events)

There is an event list created for each relevant ASDU type. The following is a list of ASDU types for which events may be generated by the SCADAPack E RTU:

- ASDU Type ID 1: M_SP_NA_1 – Single Point Information
- ASDU Type ID 3: M_DP_NA_1 – Double Point Information
- ASDU Type ID 5: M_ST_NA_1 – Step Position Information
- ASDU Type ID 9: M_ME_NA_1 – Measured Value, Normalized
- ASDU Type ID 11: M_ME_NB_1 – Measured Value, Scaled
- ASDU Type ID 13: M_ME_NC_1 – Measured Value, Short Float
- ASDU Type ID 15: M_IT_NA_1 – Integrated totals
- ASDU Type ID 21: M_ME_ND_1 – Measured Value, Normalized - no quality

SCADAPack E Configurator allows the user to configure the ASDU types which are enabled to generate events. See **Figure 4.1**

When an ASDUs type is enabled to generate events and the same ASDU type is selected as the IEC60870-5 ASDU type for a point, events are generated by the SCADAPack E RTU according to the RTU point configurations. E.g. not Alarm Inhibited, at Analog Deviation change, at Analog alarm threshold crossing, etc.

Figure 4.1: Event Enabled ASDU Types

6.5 System Event Capacity

The RTU allows for a maximum of **500 events for each supported Event ASDU type**.

As there are 7 supported Event ASDU types, total buffering capacity of SCADAPack E RTU is up to 3500 IEC 60870-5 events.

If excess events are generated beyond the limit of 500 for a particular Event ASDU type, the oldest events of that particular type are overwritten.

IEC 60870-5 events are volatile in the SCADAPack E RTU. I.e. they are not retained if the RTU is restarted.

6.6 System Point Listing

This section details the analog and binary system points used for IEC 60870-5-101/104 configurations. The RTU's IEC 60870-5-101/104 Slave driver needs to be restarted for any changed system configurations to take effect.

Table 5.1: Analog System Points

Analog System Point Name	Point Number		Point Type
	Start	End	
Master 1 : Enabled	57000		16-bit Integer
Master 1 : Link Address	57001		16-bit Integer
Master 1 : Com Port	57002		16-bit Integer
Master 1 : Link Confirm Timeout (s)	57003		16-bit Integer
Master 1 : Link Address Size	57004		16-bit Integer
Master 1 : Link Mode *	57005		16-bit Integer
Master 1 : Link Retries	57006		16-bit Integer
Unused	57007		16-bit Integer
Master 1 : Clock Valid Period (hours)	57008		16-bit Integer
Master 1 : Cyclic Period (s)	57009		16-bit Integer
Master 1 : Select Timeout (s)	57010		16-bit Integer
Master 1 : Background Period (s)	57011		16-bit Integer
Master 1 : Short Pulse Duration (ms)	57012		16-bit Integer
Master 1 : Long Pulse Duration (ms)	57013		16-bit Integer
Master 1 : Time Format **	57014		16-bit Integer
Master 1 : Select Required	57015		16-bit Integer
Master 1 : Command Age	57016		16-bit Integer
Master 1: RTU Command IOA	57017		16-bit Integer
Master 1: Analog Event Mode	57018		16-bit Integer
Unused	57019	57029	16-bit Integer
Master 2 : Enabled	57030		16-bit Integer
Master 2 : Link Address	57031		16-bit Integer
Master 2 : Com Port	57032		16-bit Integer
Master 2 : Link Confirm Timeout (s)	57033		16-bit Integer
Master 2 : Link Address Size	57034		16-bit Integer
Master 2 : Link Mode 0 = balanced, 1 = unbalanced	57035		16-bit Integer
Master 2 : Link Retries	57036		16-bit Integer
Unused	57037		16-bit Integer
Master 2 : Clock Valid Period (hours)	57038		16-bit Integer
Master 2 : Cyclic Period (s)	57039		16-bit Integer
Master 2 : Select Timeout (s)	57040		16-bit Integer
Master 2 : Background Period (s)	57041		16-bit Integer
Master 2 : Short Pulse Duration (ms)	57042		16-bit Integer
Master 2 : Long Pulse Duration (ms)	57043		16-bit Integer
Master 2 : Time Format 0 = 24 Bit Time, 1 = 56 Bit Time	57044		16-bit Integer
Master 2 : Select Required	57045		16-bit Integer
Master 2 : Command Age	57046		16-bit Integer

Master 2 : RTU Command IOA (currently unused)	57047		16-bit Integer
Master 2: Analog Event Mode	57048		16-bit Integer
Unused	57049	57299	16-bit Integer
Master 1 : ASDU Address	57340		16-bit Integer
Master 1 : ASDU Address Size	57341		16-bit Integer
Master 1 : IOA Size	57342		16-bit Integer
Master 2 : ASDU Address	57343		16-bit Integer
Master 2 : ASDU Address Size	57344		16-bit Integer
Master 2 : IOA Size	57345		16-bit Integer
Unused	57346	57369	16-bit Integer

Table 5.2: Binary System Points

Binary System Point Name	Point Number		Point Type
	Start	End	
M_SP_NA_1 (SPI) Event Enabled	50700		Read / Write
M_DP_NA_1 (DPI) Event Enabled	50701		Read / Write
M_ST_NA_1 (Step Position) Event Enabled	50702		Read / Write
M_ME_NA_1 (Measured Value, Normalised) Event Enabled	50703		Read / Write
M_ME_NB_1 (Measured Value, Scaled) Event Enabled	50704		Read / Write
M_ME_NC_1 (Measured Value, Short Float) Event Enabled	50705		Read / Write
M_ME_ND_1 (Measured Value, Normalised – no quality) Event Enabled	50706		Read / Write
M_IT_NA_1 (Integrated Total) Event Enabled	50707		Read / Write
Not used	50708	50719	Read / Write

6.7 Applying Configurations & Configuration Diagnostics

Applying Configurations

Every required configuration may be included in a single configuration file.

These configurations may be generated OFFLINE, and then applied to the RTU as required using the ***Write RTU Configuration*** facility in the SCADAPack E Configurator. The RTU configuration procedures are detailed in the *SCADAPack E Configuration Technical Reference Manual*.

The serial port configurations required to activate the IEC 60870-5-101 Slave driver are detailed in Section ***Serial Port Configurations***. The RTU needs to be restarted after applying changed serial port configurations for them to take effect.

The IEC 60870-5-101/104 System configurations detailed in ***IEC 60870-5-101 System Configurations*** require a restart of the RTU's IEC 60870-5-101/104 driver for these configurations to take effect.

SCADAPack E Configurator will restart the IEC 60870-5-101/104 driver where required to have configuration changes take effect. Consult the *SCADAPack E Operational Reference Manual* for other methods to restart various SCADAPack E drivers.

Individual point configurations also require a restart of the RTU's 60870-5-101/104 driver for these changed configurations to take effect.

See Point Configuration.

If these individual point configurations have been applied using the SCADAPack E Configurator ***Record Exchange*** write or ***Point Attributes*** dialog write, a 30 second timer is started. If any subsequent ***Record Exchange*** writes with modified IEC 60870-5 configurations are received by the RTU within that 30 seconds, this timer is restarted. Once the timer expires, the 60870-5-101/104 driver is automatically restarted by the RTU.

Configuration Diagnostics

IEC 60870-5-101/104 configuration diagnostics are generated whenever the IEC 60870-5-101/104 driver is restarted. On detection of a configuration mismatch, the status code system point (analog 50020) is written with the value 3004.

Consult the *SCADAPack E Operational Reference Manual* for detailed descriptions of RTU status codes.

The following conditions may cause a 60870-5-101/104 configuration diagnostics:

- IEC 60870-5-101/104 system configurations invalid
- invalid double point configuration, e.g. second point doesn't exist OR second point has a non-zero Information Object Address (IOA)
- duplicate Information Object Address (IOA) detected
- invalid ASDU type for specified point type
- insufficient memory on driver start-up

6.8 Compatibility between SCADAPack E or SCADAPack E Configurator versions 7.84 (and newer) and previous versions.

In previous versions, 7.83 or earlier, the **ASDU Size** and **ASDU Address Size** and the **IOA Size** did not use sperate system points.These parameters were set to default values and were not configurable. With SCADAPack E firmware version 7.84 and SCADAPack E Configurator version 7.84 the ASDU size and address size and the IOA size have individual system points and are user configurable. When upgrading to SCADAPack E or SCADAPack E Configurator versions 7.84 and newer some important compatibility questions need to be considered.

Using new SCADAPack E Configurator (Version 7.84 and newer) to Read From Older SCADAPack E (Version 7.83 and older) Firmware

Older versions of firmware do not have the new system points defined for ASDU and IOA parameters. SCADAPack E Configurator version 7.84 and newer updates the SCADAPack E Configurator display values and the configuration file based on the system point values it reads from the older firmware. The result is that any of the new system points for ASDU and IOA will be set to default values.

- If the **Link + ASDU Address** parameter was set to the default value then the value for ASDU address will be correct.
- If the **Link + ASDU Address** parameter was not set to the default value then the value for ASDU address displayed could be different from the real value in the firmware.

When using SCADAPack E firmware versions 7.83 and older the ASDU addresses parameter **must** be set to the default value.

Using new SCADAPack E Configurator (Version 7.84 and newer) to Write to Older SCADAPack E (Version 7.83 and older) Firmware

Older versions of firmware do not have the new system points defined for ASDU and IOA parameters.

- If the **ASDU Address** is the same as the **Link Address**, the **ASDU Size** is set to the default value and the **IOA Size** is set to the default value the configuration will function as expected.
- If the conditions listed in the above bullet are not met then the configuration will not function as expected. The system points used for the new configuration will not be compatible with the system points available in the older firmware.

When using SCADAPack E firmware versions 7.83, and older, the ASDU Address Size or the IOA Size parameters **must** be set to the default values. In addition the ASDU Address and the Link Address must be the same.

There will be informational messages in the config.log file as the new system points are not defined in the older firmware.

Older SCADAPack E Configurator (Version 7.83 and older) Reading From new SCADAPack E (Version 7.84 and newer) Firmware

When an older version of SCADAPack E Configurator is used to read from newer firmware, information for the new system points will not be available in the SCADAPack E Configurator or in the configuration file.

If only older versions of SCADAPack E Configurator are used, i.e. no newer versions are used to write configurations, then there are no issues when reading the configuration from the newer firmware. The ASDU Address and Link Address will be the same, the ASDU Address Size will be set to the default value and the IOA Size will be set to the default values.

When using SCADAPack E Configurator versions 7.83, and older, the ASDU Address Size and the IOA Size parameters **must** be set to the default values. In addition the ASDU Address and the Link Address must be the same.

Older SCADAPack E Configurator (Version 7.83 and older) Writing to New SCADAPack E (Version 7.84 and newer) Firmware

If only older versions of SCADAPack E Configurator are used, i.e. no newer versions are used to write configurations, then there are no issues when writing the configuration to the newer firmware. The ASDU Address and Link Address will be the same, the ASDU Address Size will be set to the default value and the IOA Size will be set to the default values.

When using SCADAPack E Configurator versions 7.83, and older, the ASDU Address Size and the IOA Size parameters **must** be set to the default values. In addition the ASDU Address and the Link Address must be the same.

7 IEC 60870-5-104 TCP Connections

IEC 60870-5-104 TCP/IP Service

In order for IEC 60870-5-104 Master sessions to be initialized, the IEC 60870-5-104 TCP/IP Service needs to be selected.

This service has no impact on -101 sessions. If this service is initialized and the RTU is licensed for IEC 60870-5-101/104 then TCP port listeners will be started and 104 channels initialized.

Connecting to -104 Slave Sessions

The section describes how to establish a TCP connection to the -104 slave sessions in the RTU.

A connection to a 104 master session can be established on any Ethernet port or PPP port that has been configured with an IP address.

To establish a connection, a 104 Master needs to attempt a TCP connection to the appropriate IP address using TCP port described below.

- 104 Master session 1 listens on TCP port **2404**
- 104 Master session 2 listens on TCP port **2405**

Redundant TCP Connections

The 60870-5-104 driver also supports redundant connections.

The master needs to support redundant connections in order to use redundancy with the RTU. The connections to any given Master session form a single Redundancy Group.

Data transfer is valid on only one connection in the redundancy group at a time.

The connection to be used for data transfer is nominated by the Master using the *STARTDT* command in the protocol.

It is the Master's role to establish and manage the connections and there is no configuration required for this in the RTU.

8 IEC 60870-5 File Transfer

The RTU provide facilities to interface to some of the elements of IEC 60870-5 file transfer.

In particular, IEC transparent data is supported, but without support for directories or other IEC 60870-5 file types. For more information see the relevant IEC -101 or -104 interoperability documents.

> IEC file transfer of large files can take a long period of time - e.g. in excess of 15 mins. This timing should be considered with respect to Master Station communication requirements and timeouts.

Files are referenced in the RTU file system by their IOA protocol number (i.e. the file's name is the IOA number). Alternatively if they appear in the *Filename to IOA Mapping Table*, a file operation referring to IOA protocol number accesses a file by name, in the RTU. The default mapping table is shown below.

The IOA has an addressable range of 1 to 65535 and is shared between database points and files. It is unique and the same value cannot appear multiple times, hence high IOA numbers are used to represent files. The RTU will allow a maximum file size of 2MB for download via IEC -101 or -104 protocols. Requests to download files greater than 2MB will be rejected by the RTU.

Table 4.1: Filename to IOA default mappings

File Name	IOA
System.rtk	60001
Config.rtu	60002
Config.inc	60003
Config.log	60004
Isa11	60005
Isa21	60006
Ntp.conf	60007
eNet.lic	60008
7xxe586.biz	60009
Mon_2xx_586x.bin	60010
M386v1xx.bin	60011
Readconfig.rtu	60012

Filename to IOA Mapping Table

A mapping table provides protocol Information Object Addresses (IOAs) to filename translation in the RTU. This allows the user to download and upload configuration files using 60870-5-101/104. A default

mapping table is provided in the RTU configuration file. This can be modified manually if required.

Default Filename IOA Mapping table as it appears in text of a *.rtu file

SLT IF #IOA/File Name mapping
“System.rtk” 60001
“Config.rtu” 60002
“Config.inc” 60003
“Config.log” 60004
“lsa11” 60005
“lsa21“ 60006
“Ntp.conf” 60007
“eNet.lic” 60008
“7xxe586.biz” 60009
“Mon_2xx_586x.bin” 60010
“M386v1xx.bin” 60011
“Readconfig.rtu” 60012

8.1 RTU commands issued via IEC 60870-5

The RTU supports a mechanism for issuing commands via IEC 60870-5-101 and -104 protocol.

An ASDU type 49 *Setpoint Command Scaled Value* can be sent to an IOA address in the RTU to cause a command to be executed. The **RTU command IOA** system point sets which IOA address is the appropriate address for command (default is IOA 60000).

Different values set in the command IOA address correspond to different commands.

The response to the *Setpoint Command* is an acknowledgement. This does not indicate that the command was successful but rather that it was accepted.

The RTU will not respond to any further IEC 60870-5-101 or -104 messages until after the command has been processed.

The execution of the command will be rapid, though applying particularly large configurations or restarting the RTU could take a longer period of time.

Also see RTU Command IOA.

Restarting services will impact process control and RTU availability. Assess the impact prior to performing a restart operation.

⚠ WARNING

UNEXPECTED EQUIPMENT OPERATION

Evaluate the operational state of the equipment monitored and controlled by the SCADAPack E RTU prior to restarting services.

Failure to follow these instructions can result in death, serious injury or equipment damage.

Table 4.2 IOA command codes

Value Sent	RTU Command executed	What this does:
1	RESTART CONFIG config.rtu	Reconfigures the RTU using a file named *config.rtu*
2	RESTART CONFIG config.inc	Applies an incremental configuration to the RTU from file *config.inc*
3	RESTART ISAGRAF	Restarts ISaGRAF user applications
4	RESTART RTU	Restarts an RTU (same as power on start)
5	RESTART LICENCE enet.lic	Applies a new license contained in file *enet.lic*
6	RESTART PATCH 7xxe586.biz	Loads new RTU firmware from a filename in the format *7xxe586.biz*

7	RESTART BOOTMON mon_2xx_586x.bin	Loads new Boot Monitor firmware from a filename in the format mon_2xx_586x.bin
8	RESTART IOFIRM m386v1xx.bin	Applicable only to the SCADAPack ER RTU. Loads new i/o processor firmware from a filename in the format m386v1xx.bin
9	GETCONFIG readconfig.rtu	Generates a file *readconfig.rtu* from the RTU's current configuration

9 System Information Commands

This section details the additional system commands supported by the RTU's IEC 60870-5-101/104 Slave driver. The RTU will respond to the ASDU types as follows:

- Type ID 100: C_IC_NA_1 – Interrogation Command
- Type ID 101: C_CI_NA_1 – Counter Interrogation Command
- Type ID 103: C_CS_NA_1 – Clock Synchronization Command
- Type ID 104: C_TS_NA_1 – Test Command
- Type ID 105: C_RP_NA_1 – Reset Process Command
- Type ID 107: C_TS_TA_1 – Test Command with Time Tag(104 only)

See the following sections for details of these ASDUs.

- ASDU Type ID 100, 101, 103, 104, 105, & 107

9.1 ASDU Type ID 100, 101, 103, 104, 105, & 107

ASDU Type ID 100 : C_IC_NA_1 - Interrogation Command

The RTU's IEC 60870-5-101/104 Slave driver will present Background and Cyclic data as determined by the system configuration parameters *Background Period* (for IEC data) and *Cyclic Period* (for Analog Points so configured).

This data may also be reported in response to an *Interrogation Command* (ASDU Type ID 100). The only qualifier supported for the *Interrogation Command* is the Station Interrogation (20).

The *Interrogation Command* may be issued by the Master in order to synchronize information between the controlling station (Master) and the controlled station (RTU), or to update the controlling station database after an initialization procedure has taken place in the RTU.

ASDU Type ID 101 : C_CI_NA_1 - Counter Interrogation Command

The RTU's IEC 60870-5-101/104 Slave driver supports Counter Interrogations only in **Mode C (**Freeze and transmit by counter interrogation commands**)**. The integrated totals (counter points) in the RTU can only be frozen, reset, or read using the Counter Interrogation Command. The only qualifier supported for the *Counter Interrogation Command* is the General Request Counter (5) which references EVERY counter in the RTU.

Counter values retrieved from the RTU are frozen values. If the *Counter Interrogation Command* specifies a FREEZE in the qualifier, the sequence number reported for subsequent READ is incremented. If the *Counter Interrogation Command* specifies a FREEZE WITH RESET in the qualifier, the *Current Integer Value* of the counter configuration point is set to 0, and the Counter Adjusted (*CA*) bit included in the information object is set for the first READ after the FREEZE WITH RESET.

ASDU Type ID 103 : C_CS_NA_1 - Clock Synchronization Command

The *Clock Synchronization Command* specifies a CP56Time2a object in the Information Object which will used to set the RTU's real time clock. If the RTU is configured to use NTP time synchronization, the *Clock Synchronization Command* will NOT set the RTU's real time clock but will still respond with a positive activation response to the *Clock Synchronization Command*.

There are multiple methods to time synchronize time in the RTU. If NTP Time Synchronization is NOT being used, check that ONLY ONE of the slave protocols is being used for time synchronization, as IEC 60870-5-101 Slave, IEC60870-5-104 Slave and DNP3 Slave communications can be used to process time synchronization messages.

ASDU Type ID 104: C_TS_NA_1 - Test Command

The *Test Command* is supported by the RTU's IEC 60870-5-101/104 Slave driver such that specified fixed bit pattern is included in the response to the *Test Command*.

ASDU Type ID 105: C_RP_NA_1 - Reset Process Command

The *Reset Process Command* will be processed by the RTU and a positive activation response will be issued. Currently there is no support for restarting any of the RTU's internal processes. Support for the *Reset Process Command* will be extended in future firmware releases.

ASDU Type ID 107 : C_TS_TA_1 - Test Command with Time Tag (104 only)

The *Test Command* is supported by the RTU's IEC 60870-5-101/104 Slave driver such that incrementing sequence numbers are included in the response to the *Test Command*.

10 Multiple Master Support

The RTU's IEC 60870-5-101/104 Slave driver will support communications with up to two (2) IEC 60870-5-101 Masters and two (2) IEC 60870-5-104 Masters to a total of 4. The first -101 master and first -104 master share common configurations. The second -101 master and second -104 master share common configurations.

When the IEC 60870-5-101/104 facility is licensed on the SCADAPack E RTU, Multiple Master facilities are automatically enabled not requiring an additional license.

The default configuration enables a single -101 and -104 Master session. The IEC 60870-5-101/104 system configurations are duplicated for each enabled Master session. See ***60870-5-101 System Configurations***. This allows the first and second 101 or 104 Master session to be independently configured.

Each Master session has its own event list such that a given IEC 60870-5-101/104 event will NOT be removed from the RTU's 60870-5-101/104 event list until it has been retrieved by each enabled Master session.

The Integrated Totals sequence numbers (see *Counter Point ASDU Types*) are maintained for each enabled Master session, i.e. a FREEZE *Counter Interrogation Command* received from -101 Master 1 will only increment the sequence number returned to the next READ request from the -101 Master 1 and -104 Master 1. The sequence number for -101 and -104 Master 2 will remain unmodified.

The two sets of masters must use different serial ports. The second -101 master and second -104 master will be disabled if their configuration uses the same serial port as the first -101 master and first -104 master.

11 Command Line Diagnostics

The RTU provides a diagnostic display which can be used to verify IEC 60870-5-101/104 communications between the RTU (as a Slave) and the connected Master. These IEC 60870-5 diagnostics can be obtained using one of the following methods

- direct serial connection to a **Cmd Line** port
- TELNET connection
- FILEDIAG (logged diagnostics to RTU File System).

Refer to the *SCADAPack E Operational Reference* manual for more details on these methods of accessing RTU diagnostics.

The **S101DIAG** command is used to filter IEC 60870-5-101/104 diagnostics displays when in Diagnostic Session display mode (type DIAG at the command line to enter diagnostic mode).

The format of the S101DIAG command is:

S101DIAG mode filter [filter ….]

Where: mode = ENABLE DISABLE

filter = * APPL BYTES LINK TIMESTAMP USER

For example: **S101DIAG ENABLE APPL TIMESTAMP**

Enabling IEC 60870-5-101/104 diagnostics can have some impact on system performance. It is suggested that these diagnostics be disabled when not in use.

The command filters can be individually enabled or disabled (these are retained in NV memory).

*	All filters enabled / disabled
APPL	60870-5-101/104 Application Layer information
BYTES	60870-5-101/104 Link Layer packet bytes (requires LINK filter)
LINK	60870-5-101/-104 Link Layer packet header information
TIMESTAMP	Time of 60870-5-101/104 message diagnostic
USER	user application response information

The following sections are examples of filtered diagnostic information where the RTU Link and ASDU (common) address is 21. These examples are time-stamped (i.e. TIMESTAMP filter has been enabled). Outbound link messages are indicated as <---- whereas inbound messages are indicated as ---->.

11.1 Link, Application, & User Layer Diagnostics

Link Layer Diagnostics (including Bytes)

...> PORT0 Primary Frame - Request User Data Class 2

DIR(0) PRM(1) FCV(1) FCB(0) ADDR(21)
10 5b 15 00 70 16

<... PORT0 Secondary Frame - Respond Data Not Available

DIR(0) PRM(0) DFC(0) ACD(0) ADDR(21)
10 09 15 00 1e 16

Application Layer Diagnostics

~~~> Master 1 Addr(21) Sector(21) Application Header, Clock synchronization command

Quantity(1) SQ(0) COT(6, activation)

<~~~ Master 1 Addr(21) Sector(21) Application Header, Clock synchronization command

Quantity(1) SQ(0) COT(7, positive activation confirmation)

User Layer Diagnostics

<=== Master 1 Insert request in queue: Background Response
~~~