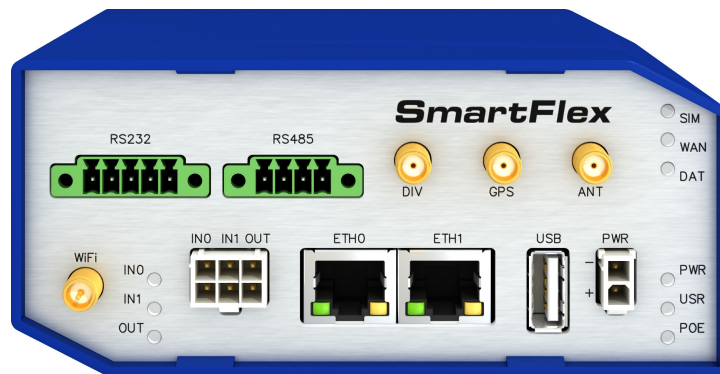User module

Protocol IEC101/104

APPLICATION NOTE

B+B SmartWorx

Powered by ADVANTECH

Used symbols

Danger – Information regarding user safety or potential damage to the router.

Attention – Problems that can arise in specific situations.

Information, notice – Useful tips or information of special interest.

Contents

List of Figures

List of Tables

1. User Module Description

IEC 60870-5-101 is a standard for power system monitoring, control & associated communications for telecontrol, teleprotection, and associated telecommunications for electric power systems. IEC 60870-5-104 protocol is an analogy to IEC 60870-5-101 protocol with the changes in transport, network, link & physical layer services to suit the complete network access: TCP/IP.

This user module does a **bidirectional conversion** between IEC 60870-5-101 and IEC 60870-5-104 protocols specified by the IEC 60870-5 standard (see [3, 4]). IEC 60870-5-101 serial communication is converted to the IEC 60870-5-104 TCP/IP communication and vice versa. It is possible to configure some parameters of IEC 60870-5-101 and IEC 60870-5-104.
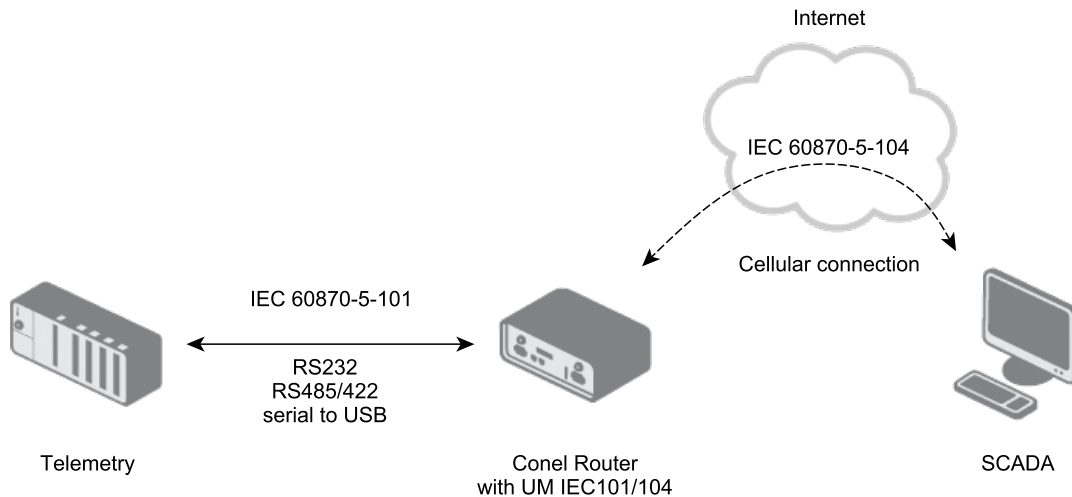
Figure 1: Scheme of communication using Protocol IEC101/104 user module

Parameters of serial communication and parameters of IEC 60870-5-101 protocol can be set separately for every serial port of the router. It is possible to use the USB port of the router with USB-serial converter. If using more serial ports in the router, there will be multiple instances of the user module running and independent IEC 60870-5-101/IEC 60870-5-104 conversions can be done. Only the *TCP Port* parameter can be configured on the side of IEC 60870-5-104. It is the port the TCP server listens on when conversion activated. Remote IEC 60870-5-104 applicaton has to communicate on this port. The data for IEC 60870-5-101 side are sent as soon as they arrive from SCADA. The IEC 60870-5-101 side asks periodically for the data according to *Data polling time* parameter configured. Regular asking is launched when the first test frame arrives from SCADA.

Protocol IEC 60870-5-101 defines an *Application Service Data Unit (ASDU)*. In ASDU there is *ASDU identifier* (with type of ASDU in it) and *information objects*. When converting from IEC 60870-5-104 to IEC 60870-5-101 all ASDU types defined in the IEC 60870-5-101 standard in compatible 1–127 range of ASDU types are converted accordingly. Proprietary types of ASDU in the private range 127–255 are not converted. Both commands and data (payload) in ASDUs are converted. Additionally, other ASDUs are converted by default – those for control and monitoring with time tag. These are not defined the same way in IEC 60870-5-101 and IEC 60870-5-104 protocols, so it is possible to configure the conversion of these ASDUs in the user module: either drop, or mapping to equivalent in opposite protocol, or mapping to same ASDU in opposite protocol. More details in chapter 3.3, list of these ASDUs on Figure 5. A number of unknown ASDUs is logged and displayed on the *Module status* page.

Figure 2: User module menu

When uploaded to the router, user module is accessible in the *Customization* section in the *User Modules* item of the router's web interface. Click on the title of the user module to see the user module menu as on the fig. 2. The *Status* section provides the *Module status* page with running communication information and the *System Log* page with the messages logged. Configuration of both serial ports and USB port of the router and IEC 60870-5-101/IEC 60870-5-104 parameters is accessible in the *Configuration* section. The *Return* item in the *Customization* section is to return to the higher menu of the router.

User module *Protocol IEC101/104* is not a part of the router's firmware. Uploading of the user module is described in the Configuration Manual (see [1, 2]). This user module is v2 and v3 router platform compatible. It is necessary to have either the serial expansion port installed in the router or use the USB-serial converter and router's USB port for proper work of this user module. The **unbalanced serial communication mode** is supported. This means the router is the *master* and connected IEC 60870-5-101 telemetry is a *slave*. SCADA initiates the first connection with router on IEC 60870-5-104 side. User module in router then asks connected IEC 60870-5-101 telemetry regularly for events and required information.

2. Protocol IEC-101/104 Status

2.1 Module status

There are protocol information about running communication on this page. These are individual for every serial port of the router. Detected type of the port is displayed at the *Port type* parameter. Parameters of IEC 60870-5-104 and IEC 60870-5-101 are described in the tables below.


```
            IEC 60870-5-101 / IEC 60870-5-104 module state
                            Expansion Port 1
Port type                   RS232

IEC104
IEC104  state       : Connected
I frame NS          : 2719
I frame NR          : 2490
S frame ACK         : 2719
U frame test        : 13
Unknown Inf.Objects : 0
TCP/IP remote host  : 172.16.188.6
TCP/IP reconnect    : 44

IEC101
IEC101 state        : Connected
Unknown frame count : 14

                            Expansion Port 2
Port type                   NONE
                                USB Port
Port type                   EMPTY
```

Figure 3: Module status page

Item	Description
IEC104 state	State of connection of the superior IEC 60870-5-104 server.
I frame NS	Sent – number of last sent frame
I frame NR	Received – number of last received frame
S frame ACK	Acknowledgment – number of last acknowledged sent frame
U frame test	Number of test frames
Unknown Inf.Objects	Number of unknown information objects (thrown away)
TCP/IP remote host	IP address of the last connected IEC 60870-5-104 server.
TCP/IP reconnect	Number of TCP/IP reconnections

Table 1: IEC 60870-5-104 status information

Item	Description
IEC101 state	IEC 60870-5-101 connection state
Unknown frame count	Number of unknown frames

Table 2: IEC 60870-5-101 status information

2.2 System Log

On the *System Log* page there are log messages displayed. It is the same system log as the one in the main menu of the router. Messages of the user module are introduced by the `iec14d` string (messages from running iec14d daemon). Here you can check out the run of the user module or see the messages in troubles with configuration and connection. You can download the messages and save it to your computer as a text file clicking the *Save* button.

On the screenshot of a log you can see the start of the user module and messages of unknown object type detected. Other errors are logged, too.
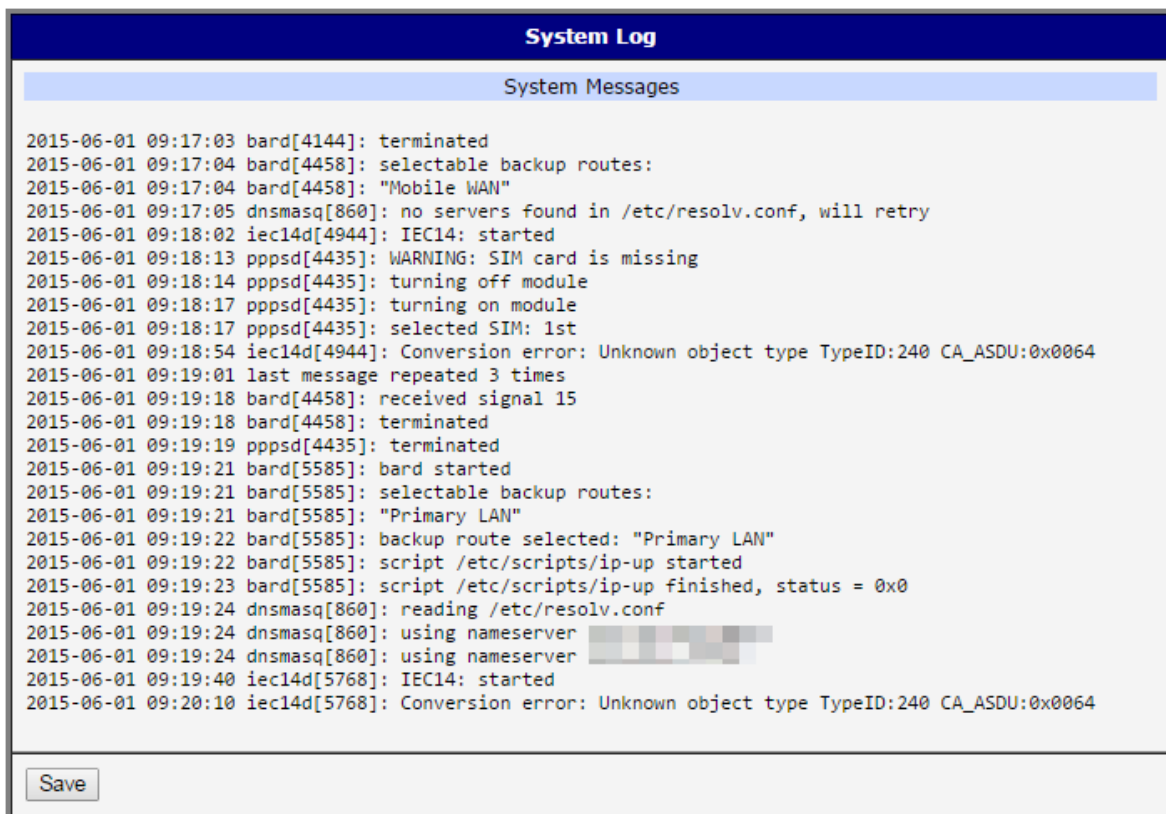

Figure 4: System Log

4

3. Conversion Configuration

Configuration of the IEC 60870-5-101 and IEC 60870-5-104 parameters is accessible in the *Expansion Port 1*, *Expansion Port 2* and *USB Port* items. More separate IEC 60870-5-101/IEC 60870-5-104 conversions are possible, individual for every serial port of the router. Parameters for every expansion/USB port are the same.

Enable the conversion for the proper expansion port ticking the *Enable conversion module* checkbox up on the page. Any changes will take effect after clicking the *Apply* button. There are four parts of the configuration form – for IEC 60870-5-101 parameters, IEC 60870-5-104 parameters, ASDU converting in monitoring direction (IEC 60870-5-101 to IEC 60870-5-104) and ASDU conversion in control direction (IEC 60870-5-104 to IEC 60870-5-101).

> ⚠ The paramaters of both – the Protocol IEC101/104 user module and the used system telemetry – has to be the same to make the communication work properly.

3.1 IEC 60870-5-101 Parameters

In the *Port Type* item there is a detected type of an Expansion Port in the router displayed. The parameters on top are for the serial line communication. The parameters for IEC 60870-5-101 itself are below. These parameters has to be configured according to the IEC 60870-5-101 telemetry used in the system. The parameters are described in the following table. The other IEC 60870-5-101 parameters are static and can not be changed.

Number	Description
Baudrate	The speed of the communication. The range is 9600 to 57600.
Data Bits	The number of data bits. 8 only.
Parity	The control parity bit. None, even or odd.
Stop Bits	The number of stop bits. 1 or 2.
Link address length	The length of the link address. 1 or 2 bytes.
Link address	Link address is the address of connected serial device.
COT transmition length	Cause Of Transmission length – the length of the "cause of transmission" information (spontaneous, periodical, etc.). 1 or 2 bytes.

Continued from previous page

Item	Description
COT MSB source	Cause Of Transmission - Most Significant Byte. COT is given by the code according to the type of event the transmission was caused by. Optionally the source address (of the data originator) can be added. 0 – standard address, 1 to 255 – specific address.
CA ASDU length	Common Address of ASDU (Application Service Data Unit) length. 1 or 2 bytes.
IOA length	Information Object Address length – IOAs are in the ASDU. 1 to 3 bytes.
Data polling time	The interval of regular requests from router to IEC 60870-5-101 telemetry for data. Time in milliseconds. Default value 1000 ms.

Table 3: IEC 60870-5-101 parameters

3.2   IEC 60870-5-104 Parameters

There is only one parameter available for the IEC 60870-5-104 configuration: *IEC-104 TCP Port*. It is a port the TCP server is listening on. The TCP server is running in the router when IEC 60870-5-101/IEC 60870-5-104 conversion enabled. The 2404 prepared value is the official IEC 60870-5-104 TCP port reserved for this service. In the *Expansion Port 2* configuration there is 2405 value prepared (not reserved by the standard). For USB Port it is 2406 TCP port.

The other IEC 60870-5-104 parameters are fixed according to standard. If the IOA lengths differ, the bytes of length are added or removed automatically. Conflict situations are always logged.

IEC 60870-5-101 / IEC 60870-5-104 Conversion Configuration

Expansion Port 1

☑ Enable conversion module

IEC 60870-5-101 parameters

Port Type	NONE
Baudrate	9600
Data Bits	8
Parity	even
Stop Bits	1
Link address length	2 bytes
Link address	100
COT transmition length	1 byte
COT MSB source	0
CA ASDU length	2 bytes
IOA length	2 bytes
Data polling time	1000 msec

IEC 60870-5-104 parameters

IEC104 - TCP Port	2404

ASDU conversions in monitoring direction (101 --> 104)

Single-point information with time tag	M_SP_TA_1 (2)	-->	M_SP_TB_1 (30)
Double-point information with time tag	M_DP_TA_1 (4)	-->	M_DP_TB_1 (31)
Step position information with time tag	M_ST_TA_1 (6)	-->	M_ST_TB_1 (32)
Bitstring of 32 bit with time tag	M_BO_TA_1 (8)	-->	M_BO_TB_1 (33)
Measured value, normalised value with time tag	M_ME_TA_1 (10)	-->	M_ME_TD_1 (34)
Measured value, scaled value with time tag	M_ME_TB_1 (12)	-->	M_ME_TE_1 (35)
Measured value, short floating point value with time tag	M_ME_TC_1 (14)	-->	M_ME_TF_1 (36)
Integrated totals with time tag	M_IT_TA_1 (16)	-->	M_IT_TB_1 (37)
Event of protection equipment with time tag	M_EP_TA_1 (17)	-->	M_EP_TD_1 (38)
Packed start events of protection equipment with time tag	M_EP_TB_1 (18)	-->	M_EP_TE_1 (39)
Packed output circuit information of protection equipment with time tag	M_EP_TC_1 (19)	-->	M_EP_TF_1 (40)

ASDU conversions in control direction (104 --> 101)

Single command with time tag CP56Time2a	C_SC_TA_1 (58)	-->	C_SC_NA_1 (45)
Double command with time tag CP56Time2a	C_DC_TA_1 (59)	-->	C_SC_NA_1 (46)
Regulating command with time tag CP56Time2a	C_RC_TA_1 (60)	-->	C_SC_NA_1 (47)
Set point command, normalised value with time tag CP56Time2a	C_SE_TA_1 (61)	-->	C_SE_NA_1 (48)
Set point command, scaled value with time tag CP56Time2a	C_SE_TB_1 (62)	-->	C_SE_NB_1 (49)
Set point command, short floating point value with time tag CP56Time2a	C_SE_TC_1 (63)	-->	C_SE_NC_1 (50)
Bitstring of 32 bit with time tag CP56Time2a	C_BO_TA_1 (64)	-->	C_BO_NA_1 (51)

CP24Time2a to CP56Time2a Conversion Method for Hour and Date	Use fixed values

Apply

Figure 5: Serial port and conversion configuration

3.3 ASDU Conversions in Monitoring Direction (101 to 104)

IEC 60870-5-101 to IEC 60870-5-104 conversion can be configured in this part. These ASDUs use 24 bits long time tag in IEC 60870-5-101 (milliseconds, seconds, minutes), but in IEC 60870-5-104 the 56 bits long time tags are used (milliseconds, seconds, minutes, hours, days, months, years). That's why the conversion configuration is possible – enabling different time tag handling according to specific needs of the application.

For every ASDU listed in this part on Figure 5, these ways of conversion can be selected: **DROP**, **Convert to same ASDU** and **Convert to equivalent ASDU** (default).

DROP When this option selected, the ASDU is dropped and conversion is not done.

Convert to same ASDU If this option is selected, the ASDU is mapped on the same ASDU in the opposite protocol. It means there is no conversion of time tag – IEC 60870-5-104 application receives unchanged shorter (24 bits) time tag from IEC 60870-5-101 device.

Convert to equivalent ASDU If this option is selected, the ASDU is mapped on the equivalent ASDU type in the opposite protocol. See the names and numbers of these opposite ASDU types on Figure 5. This means the conversion of time tag has to be done – the time tag has to be completed up to 56 bits. The conversion of time tag can be set via **CP24Time2a to CP56Time2a Conversion Method for Hour and Date** item at the bottom of the page. These are the options:

- **Use fixed values** – Default configuration. The time original time tag (24 bits) is completed with fixed values 0 hours, 1st day and 1st month of year 00 (2000).

- **Use router time values** – The time original time tag (24 bits) is completed with the hours, day, month and year taken from the router's time. It depends on the time setting on the router (Either manually or from NTP server). There is another risk – see the box bellow.

> **Attention!** *Use router time values* item from *CP24Time2a to CP56Time2a Conversion Method for Hour and Date* – is risky. Use it at your's own risk, because unintentional jumps in data can appear when converted this way. This can happen at the edges of time units (days, months, years). Let's have a situation when the monitoring ASDU is sent at 23 hours, 59 minutes, 59 seconds and 95 milliseconds. Due to network latency it will pass the router just after midnight – on the next day. And the completed time tag is now 0 hours, 59 minutes, 59 seconds and 95 milliseconds of the next day – there is unintentional one hour jump in the converted time tag.

Note: If the IEC 60870-5-101 device supports long (56 bits) time tags for IEC 60870-5-104, it will send the ASDUs readable by IEC 60870-5-104, so the time tag is not converted and will be delivered to SCADA directly from the device.

3.4   ASDU Conversions in Control Direction (104 to 101)

IEC 60870-5-104 to IEC 60870-5-101 conversion can be configured in this part. Again it is related to different time tag length, but here the long time tags are just cut for the IEC 60870-5-101 device.

For every ASDU listed in this part on Figure 5, these ways of conversion can be selected: **DROP**, **Convert to same ASDU** and **Convert to equivalent ASDU** (default).

DROP   When this option selected, the ASDU is dropped and conversion is not done.

Convert to same ASDU   If this option is selected, the ASDU is mapped on the same ASDU in the opposite protocol. It means there is no conversion of time tag – IEC 60870-5-101 device receives unchanged long time tag from IEC 60870-5-104 application (some IEC 60870-5-101 devices support long time tags).

Convert to equivalent ASDU   If this option is selected, the ASDU is mapped on the equivalent ASDU type in the opposite protocol. See the names and numbers of these opposite ASDU types on Figure 5. Conversion of time tag is done by cutting it's length from 56 bits to 24 bits – only minutes, seconds and milliseconds are kept.

All configuration changes will take effect after pressing *Apply* button.

4. Recommended Literature

[1] Advantech B+B SmartWorx: **Configuration Manual for v2 Routers**

[2] Advantech B+B SmartWorx: **Configuration Manual for v3 Routers**

[3]   IEC: **IEC 60870-5-101 (2003)**: Telecontrol equipment and systems
– Part 5-101: Transmission protocols – Companion standard
for basic telecontrol tasks

[4]   IEC: **IEC 60870-5-104 (2006)**: Telecontrol equipment and systems
– Part 5-104: Transmission protocols – Network access for
IEC 60870-5-101 using standard transport profiles