Notes on the Implementation of “I87” IO Driver 870-5-101&104

The IEC 870-5-101 spec is broad based and this document explains how this IO driver integrates the standard with the iFix SCADA or an OPC client.

The following table lists the internal driver data types & how they map to IEC 870-5 protocol messages. Note that many IEC messages map to the same Internal datatype if this is logically achievable. For example the analog integer type MV (measured value) handles both IEC Scaled & normalised values based on the assumption that Scaling & signal conditioning is handled in the SCADA database or OPC server in its native way. In addition this driver specifically allows the user to read & write to the same address. If this is undesirable, simply use different addresses.

“When written” means the operator sets a new value to an AO,DO,AR,AO block in the database. It is desirable from a SCADA point of view that the RTU should send the Value of these addresses back during General Interrogation. Some of the driver “datatypes” are not actually used for IO but rather trigger another action, example TSYNC & Interrogate. Normally the Interrogate Poll block is the only one that has a poll time configured (SPI,DPI,MV should have polltime disabled by typing “-”).

**Glossary**

MV 16 bit analog measured value
SPI Single point Input
ASDU Application data unit, refers to the Common address of the data ()

**Driver Features**

- Each Serial port can operate in Master Mode OR Slave mode OR Listen Only
  - The Slave & listen modes may be used for debugging or test set applications
  - If interface to a third party SCADA is required without removing the national control Master station, you can use this driver in parallel
  - Slave mode may simulate an RTU in remote scada & protocol conversion applications.
  - 104 TCP/IP supports:
    - Master where the driver is TCP client
    - Slave where the driver is the TCP server
- Most IEC parameters are set-able
- Timestamps are sent to OPC client in master mode (the ability to support time stamps in slave mode may be supported in future versions via OPC V 3 if this is required)
- Timestamped events are logged to text files and to an ODBC database
Select & Execute Secure Commands are supported, however this requires an understanding of the implementation at the application level.
Configuring the driver

Main Configuration window

- First thing you should do is Save as to your desired configuration name (Vista, 2008 & Win7 will not allow in Program Files).
- When making changes you need to File > Reload before they become active.
- Create Arrays of data objects example 1:100 of type SPI is common address 1 object 100

Single point (Input or setpoint)
Channel Settings

For 104 these are not changeable.

2 types of 16 bit analog, this is for sending. MV data types receive both.
Data Block settings

Format of addresses: `<Common ASDU>:<Object number>`

This driver allows blocks of many common addresses to be used on the same RTU/Station number. On most devices the common address & the RTU address are the same.

You configure blocks/arrays of objects per line, make more than actually exist in the RTU. If you see “block not found” errors then these blocks do not exist or are too small.

Set poll time to disabled & Access Time to disabled

### Configuring Interrogation (Master Mode)

- On a Master Driver configure one poll block a Interrogate with a slow poll time – It is not necessary to poll fast. Set access time to disabled.
- You can force a manual Interrogation by writing to the address.
- The Common ASDU address of the Interrogate block is the Common address you are interrogating. A common address is a ‘Group’ of tags/objects in the RTU.
- Make multiple Interrogate blocks if the RTU contains Data with multiple common addresses
- Always make the Start object address “0”, Unless the RTU supports interrogating individual objects.
- The length of the block does not matter – set to 1
Configuring Time sync (Master Mode)

- On a Master Driver configure one poll block a time sync with a slow polltime – It is not necessary to poll fast. Set access time to disabled.
- You can force a manual time sync by writing to the address.
- The Common ASDU address of the Interrogate block is the Common address you are time syncing.
- Always make the Start object address “0”. Unless the RTU supports interrogating individual objects.
- The length of the block does not matter – set to 1
Slave Mode

Slave mode is where the IO driver (PC) emulates a RTU. This can be used as a gateway to feed data from any other source like a SCADA System or another OPC Server. The concepts & applications are OPC-OPC bridge, Slave-Master. Scada data upto National grid control

Configuring Slave mode

- In the channel settings set the IP address to 0.0.0.0 For must configurations with one slave via one Network adapter. Then you are limited to only 1 slave channel(TCP Server) & only 1 RTU but unlimited Common addresses
- For a "Multi homed" system with multiple network adapters, set the IP address to the address of the Adapter. One channel per adapter.

Setting the Firewall (Slave mode)

Slave mode is a TCP/IP server with incoming connections, by default the Firewall blocks this. You need to enable incoming TCP/IP connections on port 2404.

- Set an inbound rule as below
- Ping the "server/slave" from the client side, if fail ping client from server (my test setup here requires this - have not figured it out yet) then ping server again – must work
- Last test, only if still not working in console run "TELNET <server ip> 2404<enter> fail is connection refused, success is blinking cursor.
Command Mapping for MASTER mode

The following table lists which IEC message types correspond to which Internal IO addresses.

<table>
<thead>
<tr>
<th>I87 Driver Internal Address Type</th>
<th>Description</th>
<th>Messages for received data (IEC 870 names)</th>
<th>Messages sent when written to</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPI</td>
<td>Single-point information</td>
<td>M_SP_NA_1, M_SP_TA_1, C_SC_NA_1, M_SP_TB_1</td>
<td>C_SC_NA_1, C_SC_TA_1</td>
</tr>
<tr>
<td>DPI</td>
<td>Double-point information</td>
<td>M_DP_NA_1, M_DP_TA_1, C_DC_NA_1, M_DP_TB_1</td>
<td>C_DC_NA_1, C_DC_TA_1</td>
</tr>
<tr>
<td>MV</td>
<td>16 bit Measured values, Normalised &amp; Scaled. (receives both, sends selection in channel settings)</td>
<td>M_ME_NA_1, M_ME_TA_1, M_ME_NB_1, M_ME_TB_1, M_ME_ND_1, C_SE_NA_1, M_ME_TD_1</td>
<td>C_SE_NA_1, C_SE_TA_1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Or C_SE_NB_1, C_SE_TB_1</td>
</tr>
<tr>
<td>TSYNC</td>
<td>Time sync RTU's</td>
<td>C_CS_NA_1</td>
<td>C_CS_NA_1</td>
</tr>
<tr>
<td>Interrogate</td>
<td>Force RTU to send update data</td>
<td>C_IC_NA_1</td>
<td>C_IC_NA_1</td>
</tr>
<tr>
<td>FLOAT</td>
<td>Floating point / real numbers</td>
<td>M_ME_NC_1, M_ME_TC_1, M_ME_TF_1</td>
<td>C_SE_NC_1, C_SE_TC_1</td>
</tr>
<tr>
<td>BITS</td>
<td>Packed bit strings of 32 bits</td>
<td>M_BO_NA_1, M_BO_TA_1, M_BO_TB_1</td>
<td>C_BO_NA_1, C_BO_TA_1</td>
</tr>
<tr>
<td>IT</td>
<td>Integrated totals (counters)</td>
<td>M_IT_NA_1, M_IT_TA_1, M_IT_TB_1</td>
<td>C_CI_NA_1, C_CI_TA_1</td>
</tr>
<tr>
<td>STP</td>
<td>Step positions</td>
<td>M_ST_NA_1, M_ST_TA_1, M_ST_TB_1</td>
<td>C_RC_NA_1, C_RC_TA_1</td>
</tr>
</tbody>
</table>

Internal Address format (Both OPC & iFix)

RTU:TYPE:ASDU:OBJECT::<BIT>

General rules: Driver configuration is setup with arrays of information objects. Most of these objects are 16 bit words, in OPC the presence of the <BIT> specifies a Digital/Boolean address otherwise it is an Analog address.

For examples of valid I/O addresses (OPC Item ID’s), refer to Supported Mnemonics table below. The following are descriptions of the parts of the I/O Address:

RTU (Remote Terminal Unit) indicates the name you assigned in the RTU Name field of the Device Definition in the I/O Driver Configuration program. It is an alphanumeric tag that the Database Builder uses to differentiate poll records collected from different field devices (RTU’s). The RTU name associates a name with a RTU Data link address.
TYPE specifies the data type area in the Driver memory (see table above)

One of (SPI,DPI,MV,BITS,FLOAT,IT,STATUS).

*Note The STATUS type is used to access the COMMS status of the RTU see the section Controlling Alarms and Comms Alarms

ASDU IEC870-5-101,. Specifies the ASDU number of the I/O point within the RTU. Also referred to as the “Common address”. Many systems set this to the same as the Datalink/RTU address.

OBJECT The object number of the desired address also referred to as the Information Object address.

BIT Optional, The Bit is only used on Digital addresses SPI & DPI & BITS. Desired address may be entered as a number OR TEXT address. The bit entry is used for Digital blocks and ranges from 0 – 15. Note this driver copies all the data received from the RTU into a 16 bit word. For an SPI address this means Bit 0 is the value. For the BITS datatype the range is 0-31. Read more below under Format of Digital input data

Format of Internal Status addresses

Each RTU has a assigned range of internal addresses, that do not map to a configured poll block, these addresses are used for status information about health of the communications to each RTU

Master mode RTU Communication status (read only)
DI address <devname>:STATUS:0:0:0 = 0 means successfully polling this device
DI address <devname>:STATUS:0:0:0 = 1 means communication failure to this device

AI Address <devname>:STATUS:0:0 = 0 means ok, Non zero means comms fail

Reset RTU Communications (Write only)
DO address <devname>:STATUS:0:1:0 In master mode write a 1 to force communication reset to RTU

Slave mode RTU Communication status (read only)
Analog Address <devname>:STATUS:0:2 is a monostable timer that is set to channel timeout time x 60 x 1000 milliseconds every time a poll is received for this RTU. If the value is Zero then no poll has been received for at least timeout x 60 seconds. So alarm = 0.
Control Master / Listen only mode (read & write)

This address is used to change the Listen only mode at runtime (startup state is set in channel settings). This allows dual redundant SCADA masters to use the same communications channel. SCADA side scripting must force one of the two SCADA’s to master mode & the other to Listen only mode.

DI address <devname>:STATUS:0:5:0 = 1 means Listen only
**Format of Digital Input data**

**Note: you can use the bit number OR the text equivalents e.g. SPI:1:1:INVALID and SPI:1:1:7 are the same.**

### SPI data (Single point inputs)

<table>
<thead>
<tr>
<th>Bit def</th>
<th>IEC def</th>
<th>Input Description</th>
<th>values</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bit 0</td>
<td>7.2.6.1 SPI</td>
<td>value for SPI (on/off)</td>
<td>1/0 Bool</td>
<td>&lt;rtu&gt;:SPI:1:1:VAL</td>
</tr>
<tr>
<td>Bit 1</td>
<td>Not used</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bit 2</td>
<td>Not used</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bit 3</td>
<td>Not used</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bit 4</td>
<td>7.2.6.1 SPI</td>
<td>Blocked / not Blocked</td>
<td>1/0 Bool</td>
<td>&lt;rtu&gt;:SPI:1:1:BLOCK</td>
</tr>
<tr>
<td>Bit 5</td>
<td>7.2.6.1 SPI</td>
<td>Substituted / not substituted</td>
<td>1/0 Bool</td>
<td>&lt;rtu&gt;:SPI:1:1:SUB</td>
</tr>
<tr>
<td>Bit 6</td>
<td>7.2.6.1 SPI</td>
<td>topical / not topical</td>
<td>1/0 Bool</td>
<td>&lt;rtu&gt;:SPI:1:1:TOP</td>
</tr>
<tr>
<td>Bit 7</td>
<td>7.2.6.1 SPI</td>
<td>Invalid=1</td>
<td>1/0 Bool</td>
<td>&lt;rtu&gt;:SPI:1:1:INVALID</td>
</tr>
<tr>
<td>Bit 8-15</td>
<td>NA</td>
<td>COT of last received data</td>
<td>1-30 Analog</td>
<td>&lt;rtu&gt;:SPI:1:1</td>
</tr>
</tbody>
</table>

**IO address for Digital Addresses**

<rtu>:SPI:<asdu>:<obj>:bit (bit=0 usually)

**IO address for Analog Addresses**

<rtu>:SPI:<asdu>:<obj>

Note **for OPC the Last “:” indicates a Boolean / digital address otherwise analog Many SCADA’s prefer to read the array of bits as an analog value.

### DPI data (Double point inputs)

<table>
<thead>
<tr>
<th>Bit def</th>
<th>IEC def</th>
<th>Input Description</th>
<th>Clientvalues</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bit 0,1</td>
<td>7.2.6.2 DPI</td>
<td>value for DPI (on/off)</td>
<td>0..3 Analog</td>
<td>&lt;rtu&gt;:DPI:1:1</td>
</tr>
<tr>
<td>Bit 2</td>
<td>Not used</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bit 3</td>
<td>Not used</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bit 4</td>
<td>7.2.6.2 DPI</td>
<td>Blocked / not Blocked</td>
<td>1/0 Boolean</td>
<td>&lt;rtu&gt;:DPI:1:1:BLOCK</td>
</tr>
<tr>
<td>Bit 5</td>
<td>7.2.6.2 DPI</td>
<td>Substituted / not substituted</td>
<td>1/0 Boolean</td>
<td>&lt;rtu&gt;:DPI:1:1:SUB</td>
</tr>
<tr>
<td>Bit 6</td>
<td>7.2.6.2 DPI</td>
<td>topical / not topical</td>
<td>1/0 Boolean</td>
<td>&lt;rtu&gt;:DPI:1:1:TOP</td>
</tr>
<tr>
<td>Bit 7</td>
<td>7.2.6.2 SPI</td>
<td>Invalid=1</td>
<td>1/0 Boolean</td>
<td>&lt;rtu&gt;:DPI:1:1:INVALID</td>
</tr>
<tr>
<td>Bit 8-15</td>
<td>NA</td>
<td>COT of last data</td>
<td>1-30 Analog</td>
<td>&lt;rtu&gt;:DPI:1:1</td>
</tr>
</tbody>
</table>

**IO address for DI/DO/DR/MDI blocks**

<rtu>:DPI:<asdu>:<obj>:bit (bit=0 usually)

With iFix you would normally use an MDI block addressing bits 0 & 1 with text descriptions of the 4 states

OPC example “RTU1:DPI:1:100|S&M,,.0:3” results in analog shift(0) & mask(3) results in analog values 0..3

### SPI & DPI Slave mode notes

- **On startup the master receives data with the “invalid” flag set** Until the SCADA client writes a value, after which the value written is sent (:INVALID defaults to 0, i.e. OK)
- **If you write from the SCADA client to any bit including bits like :INVALID it sends a spontaneous update to the master.**
- **If you set a bit like :INVALID it retains this value so if set & you then write to the :VALUE the master receives “invalid” spontaneous data.**
**MV data (analogs)**

Normally you would use an AI/AR block addressing `<rtu>:MV:<asdu>:<obj>`. Scaling the data to engineering units is done with FIX / OPC signal conditioning.

*note if you enable outputs in the SCADA database you can write to the same addresses (setpoints)

OPC example “RTU1:MV:1:100|LIN,-100.0,100.0” will result in the IEC normalised values scaling from -100 to 100 % you can replace the 100 with your engineering unit range.

Read in the manual about the LIN Signal conditioning & many others

Example 4-20ma live zero input with 15 bit AD converter scaled to 0-100% (PROP=Proportional signal conditioning)

“RTU1:MV:1:100|PROP,0.0,100.0,6553:32767,%”

“RTU1:MV:1:100” = address of MV

will scale inputs of 6553-32767 to 0 - 100 %, you can replace the 100.0 with your engineering unit range.

**Analog Status Bits**

By Specifying an extra :<> bit parameter after the info object the status bits may be read

**MV Status data**

<table>
<thead>
<tr>
<th>Bit def</th>
<th>IEC def</th>
<th>Input Description</th>
<th>values</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bit 0</td>
<td>QDS</td>
<td>1=Overflow (OV)</td>
<td>1/0 Bool</td>
<td><code>&lt;rtu&gt;:MV:1:0V</code></td>
</tr>
<tr>
<td>Bit 1</td>
<td>Not used</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bit 2</td>
<td>Not used</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bit 3</td>
<td>Not used</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bit 4</td>
<td>QDS</td>
<td>Blocked / not Blocked</td>
<td>1/0 Bool</td>
<td><code>&lt;rtu&gt;:MV:1:BLOCK</code></td>
</tr>
<tr>
<td>Bit 5</td>
<td>QDS</td>
<td>Substituted / not substituted</td>
<td>1/0 Bool</td>
<td><code>&lt;rtu&gt;: MV:1:SUB</code></td>
</tr>
<tr>
<td>Bit 6</td>
<td>QDS</td>
<td>topical / not topical</td>
<td>1/0 Bool</td>
<td><code>&lt;rtu&gt;: MV:1:TOP</code></td>
</tr>
<tr>
<td>Bit 7</td>
<td>7.2.6.1 SPI</td>
<td>Invalid=1</td>
<td>1/0 Bool</td>
<td><code>&lt;rtu&gt;: MV:1:INVALID</code></td>
</tr>
<tr>
<td>Bit 8-15</td>
<td>NA</td>
<td>COT of last received data</td>
<td>1-30 Analog</td>
<td>`&lt;rtu&gt;: MV:1:1</td>
</tr>
</tbody>
</table>
**Format of Output Command data**

**SPI & DPI commands**

***Note both master & slave mode use the same internal addresses of Input / Commands, by simply writing to an address it sends a command to the address. This means you can have inputs & outputs at the same address which is not actually allowed by the IEC standard.***

The I87 driver sends the 8 bits of data at the specified address, for this reason you can use DR & DO blocks in FIX addressed to <rtu>:SPI:<asdu>:<obj>:0 (bit 0). However it is recommended that you use AR/AO blocks instead as this will allow full control of the IEC 870 features. The 8 bits are defined as in the IEC spec SCO 7.2.6.15 which is:

<table>
<thead>
<tr>
<th>Bit def</th>
<th>IEC def</th>
<th>Description</th>
<th>Value to write from OPC Script for on/off</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bit 0 &amp; 1</td>
<td>SCS &amp; DCS the on/ off state of the command</td>
<td>Bit 0 is the command value for SPI (on/off)</td>
<td>0/1 for SP 0/1/2/3 for DP</td>
</tr>
<tr>
<td>Bit 2..7</td>
<td>QOC 7.2.6.26</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bit 2..6 = 0</td>
<td>No additional definition</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Bit 2..6 = 1</td>
<td>Short pulse duration</td>
<td>5/NA</td>
<td></td>
</tr>
<tr>
<td>Bit 2..6 = 2</td>
<td>Long pulse duration</td>
<td>9/NA</td>
<td></td>
</tr>
<tr>
<td>Bit 2..6 = 3</td>
<td>Persistent output</td>
<td>13/12</td>
<td></td>
</tr>
<tr>
<td>Bit 7</td>
<td>Execute</td>
<td>Execute command</td>
<td>0/1 for SP 0/1/2/3 for DP</td>
</tr>
<tr>
<td>Bit 7 = 0</td>
<td>Select</td>
<td>Select Control object</td>
<td>128</td>
</tr>
<tr>
<td>Bit 8-Bit13</td>
<td>NA</td>
<td>COT of Confirmation</td>
<td></td>
</tr>
<tr>
<td>Bit 14</td>
<td>NA</td>
<td>Negative Confirm</td>
<td>1=Negative Confirm</td>
</tr>
<tr>
<td>Bit 15</td>
<td>NA</td>
<td>Select Bit of Confirm</td>
<td>1=Selected</td>
</tr>
</tbody>
</table>

Example: Select & Execute Secure DP command using 1 Analog tag

1. Create analog Integer read / write address “<rtu>:SPI:<asdu>:<obj>”
2. Set value 128 (bit 7 =1 means Select)
3. wait for value to go >= 32767, means => selected (driver sets bit 15 when RTU returns selected confirm)
   a. Close contactor, Write value = 1 (bit 7 =0 means Execute)
   b. Open contactor, Write value = 0 (bit 7 =0 means Execute)

For Feedback Monitoring of commands, use bit 14(:NEG) & 15(:SEL). If Bit 14 goes high after a command then the RTU sent back a Negative Activation Termination.
**SPI & DPI commands Slave mode notes**

- If the Slave addresses of a Block are to be setpoints written by the master the Flag “Disable Interrogation response” should be set in the block settings, otherwise the value is returned as an Input during interrogation.

**Actions that occur at Slave side during command write from the Master**

1. Commands sent by the Master set the :VALUE bits & set the timestamp of local PC time of receipt.
2. In addition the following bits are set: Bit 13 (:TOG) is toggled (changed) everytime a command is received, this allows the SCADA to sense the command even if Master sends the same value. Bit 12 (:WRIT) is set after first write, this may be used to indicated that a value has been received by the slave since startup.
3. The OPC server sends a OnChange() with new timestamp even if the value does not change.
4. For SPI & DPI commands: in the block settings set “Select timeout” to “0” if using direct execute (not select execute). This timer is the select timeout time i.e. user needs to send execute AFTER select within this time or execute fails. Do not set too long, if user fails to cancel or tries to select another, will fail until timeout.

**MV Setpoints**

**MV Setpoints Slave mode notes**

- If the Slave addresses of a Block are to be setpoints written by the master the Flag “Disable Interrogation response” should be set in the block settings, otherwise the value is returned as an Input during interrogation.

Actions that occur during setpoint write:

5. Setpoints sent by the Master set the analog value & set the timestamp of local PC time of receipt.
6. In addition the following status bits are set Bit 10 (:TOG) is toggled (changed) everytime a command is received, this allows the SCADA to sense the command even if Master sends the same value. Bit 12 (:WRIT) is set, this may be used to indicated that a value has been received by the slave since startup.
7. The OPC server sends a OnChange() with new timestamp even if the value does not change.

**Format of Integrated totals (Counters)**

The value returned by OPC address `<rtu>:IT:<asdu>:<obj>` is the count value. If the IEC data is invalid the value is 0.

**Note for OPC please use this address “<rtu>:IT:<asdu>:<obj>|DWRD” this forces the datatype to Double word.**
To read the IT Sequence number use the address "<rtu>:IT:<asdu>:<obj>|ITSQ

Counter Interrogation

Sending Counter interrogations is performed by writing to addresses <rtu>:IT:<asdu>:<obj> the value of the bits 0-7 written are sent directly to the RTU.

Format of Step Position Information

The value returned by OPC address <rtu>:STP:<asdu>:<obj> is the VTI (value with transient state as defined in IEC section 5.2.1.5).

VTI := CP8(Value,Transient)
Value := I7[1..7]<64..+63>
Transient := BS1[8]

<0> := equipment is not in transient state
<1> := equipment is in transient state

Example 1: “RTU1:STP:1:22|S&M,,,0:127” Will read the step pos 22 & apply the Shift & mask signal conditioning shifting 0 bits & AND’ing with 127 (bits 0-7) which results in the +63 step position

Example 2: “RTU1:STP:1:22|S&M,,7:1” Will read the step pos 22 & apply the Shift & mask signal conditioning shifting 7 bits & AND’ing with 1 (bit 8) which results in the transient state

If a Digital Block in fix OR the extra :<bit> filed is used via OPC the QDS information may be accessed

QDS := CP8(OV,RES,BL,SB,NT,IV)
OV := BS1[1]<0..1>
<0> := no overflow
<1> := overflow
RES = RESERVE := BS3[2..4]<0>
BL := BS1[5]<0..1>
<0> := not blocked
<1> := blocked
SB := BS1[6]<0..1>
<0> := not substituted
<1> := substituted
NT := BS1[7]<0..1>
<0> := topical
<1> := not topical
IV := BS1[8]<0..1>
<0> := valid
<1> := invalid

Example:

RTU1:STP:1:22:7 is the IV-invalid bit

Regulating Step commands

Regulating Step commands use the same addresses as the Step positions

RCO := CP8(RCS,QOC)
RCS=Regulating step
command state := UI2[1..2]<0..3>
  <0> := not permitted
  <1> := next step LOWER
  <2> := next step HIGHER
  <3> := not permitted

QOC := CP6[3..8]{QU,S/E} see below QOC

QOC := CP6{QU, S/E}

QU := UI5[3..7]<0..31>
  <0> := no additional definition *
  <1> := short pulse duration (circuit-breaker), duration determined by a system parameter in the outstation
  <2> := long duration pulse, duration determined by a system parameter in the outstation
  <3> := persistent output
  <4..8> := reserved for standard definitions of this companion standard (compatible range)
  <9..15> := reserved for the selection of other predefined functions **
  <16..31> := reserved for special use (private range)

S/E := BS1[8]<0..1>
  <0> := Execute
  <1> := Select

Example 1 Address “RTU1:STP:1:22” is an analog value

Writing a value of 1 means STEP UP
Writing a value of 2 means STEP DOWN
8 Interoperability

This document serves to specify which options and features of the IEC 870-5-101 standard protocol are supported by the ProScada “I87” IO driver for OPC Clients.

Note that all supported and edited notes in red were added by the developers of the I87 driver.

8.1 Network configuration (network-specific parameters)

Note: The I87 driver supports Master Mode when it communicates with slave devices. The driver can also be set to Slave mode, in this case the driver passively waits to be polled by the device on the other end. The data sent to the master is the current data written from the SCADA database. In addition, the I87 driver supports a “Listen” Mode. The Listen mode allows a SCADA node to Read & Log data being polled by another Master. This mode may also be used for Dual redundant masters.

- **Point-to-point**
- **Multiple point-to-point**
- **Multipoint-party line**
- **Multipoint-star**

8.2 Physical layer

(network-specific parameter)

**Transmission speed (control direction)**

<table>
<thead>
<tr>
<th>Standard</th>
<th>Unbalanced interchange V.24/V.28</th>
<th>Unbalanced interchange V.24/V.28</th>
<th>Balanced interchange X.24/X.27</th>
</tr>
</thead>
<tbody>
<tr>
<td>100 bit/s</td>
<td>2400 bit/s</td>
<td>2400 bit/s</td>
<td>56000 bit/s</td>
</tr>
<tr>
<td>200 bit/s</td>
<td>4800 bit/s</td>
<td>4800 bit/s</td>
<td>64000 bit/s</td>
</tr>
<tr>
<td>300 bit/s</td>
<td>9600 bit/s</td>
<td>9600 bit/s</td>
<td></td>
</tr>
<tr>
<td>600 bit/s</td>
<td>19200 bit/s</td>
<td>19200 bit/s</td>
<td></td>
</tr>
<tr>
<td>1200 bit/s</td>
<td>38400 bit/s</td>
<td>38400 bit/s</td>
<td></td>
</tr>
</tbody>
</table>

**Transmission speed (monitor direction)**

<table>
<thead>
<tr>
<th>Standard</th>
<th>Unbalanced interchange V.24/V.28</th>
<th>Unbalanced interchange V.24/V.28</th>
<th>Balanced interchange X.24/X.27</th>
</tr>
</thead>
<tbody>
<tr>
<td>100 bit/s</td>
<td>2400 bit/s</td>
<td>2400 bit/s</td>
<td>56000 bit/s</td>
</tr>
<tr>
<td>200 bit/s</td>
<td>4800 bit/s</td>
<td>4800 bit/s</td>
<td>64000 bit/s</td>
</tr>
<tr>
<td>300 bit/s</td>
<td>9600 bit/s</td>
<td>9600 bit/s</td>
<td></td>
</tr>
<tr>
<td>600 bit/s</td>
<td>19200 bit/s</td>
<td>19200 bit/s</td>
<td></td>
</tr>
<tr>
<td>1200 bit/s</td>
<td>38400 bit/s</td>
<td>38400 bit/s</td>
<td></td>
</tr>
</tbody>
</table>

Note: The I87 driver does allow RTS/CTS with RTS toggling, which may be used with 2 wire RS485 line drivers where the RTS line is used to energise the transmitter. The same
configuration may be used for Radio modems. However in both cases it is recommended that you use automatic flow control modems. The driver polls continuously as fast as possible i.e. next poll occurs immediately on completion of previous. This behaviour can be controlled with the “Interpoll timer setting” to slow it down.
8.3 Link layer
(network-specific parameter)

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

<table>
<thead>
<tr>
<th>Link transmission procedure</th>
<th>Address field of link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Balanced transmission</td>
<td>Not present (balanced transmission only)</td>
</tr>
<tr>
<td>Unbalanced transmission</td>
<td>One octet (serial only)</td>
</tr>
<tr>
<td></td>
<td>Two octets</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Frame length</th>
<th>Maximum length L (number of octets)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>255</td>
<td>Unstructured</td>
</tr>
</tbody>
</table>

Note We can Modify the Link Field address size on request

8.4 Application Layer

Transmission mode for application data

Mode 1 (Least significant octet first), as defined in clause 4.10 of IEC 870-5-4, is used exclusively in this companion standard.

Common address of ASDU
(system-specific parameter)

| One octet | Two octets |

Information object address
(system-specific parameter)

<table>
<thead>
<tr>
<th>One octet</th>
<th>Two octets</th>
<th>Three octets</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>structured</td>
<td>unstructured</td>
</tr>
</tbody>
</table>
Cause of transmission
(system-specific parameter)

- One octet
- Two octets (with originator address, 104 Only)
Selection of standard ASDUs

Process information in monitor direction
(station-specific parameter)

Note The supported information below, simply represents that which has been requested so far. If your application requires more functionality please request what you need. We can add most of these at no extra cost.

Note on Time tagging in iFix
This IO driver is capable of displaying the time tagged information in the iFix alarm summary. I.e. the time you see in the alarm summary IS the remote time tagged time. In addition all time tagged events may be logged to an ODBC datasource.

\[<1> := \text{Single-point information} \quad \text{M\_SP\_NA\_1}\]
\[<2> := \text{Single-point information with time tag} \quad \text{M\_SP\_TA\_1}\]
\[<3> := \text{Double-point information} \quad \text{M\_DP\_NA\_1}\]
\[<4> := \text{Double-point information with time tag} \quad \text{M\_DP\_TA\_1}\]
\[<5> := \text{Step position information} \quad \text{M\_ST\_NA\_1}\]
\[<6> := \text{Step position information with time tag} \quad \text{M\_ST\_TA\_1}\]
\[<7> := \text{Bitstring of 32 bit} \quad \text{M\_BO\_NA\_1}\]
\[<8> := \text{Bitstring of 32 bit with time tag} \quad \text{M\_BO\_TA\_1}\]
\[<9> := \text{Measured value, normalized value} \quad \text{M\_ME\_NA\_1}\]
\[<10> := \text{Measured value, normalized value with time tag} \quad \text{M\_ME\_TA\_1}\]
\[<11> := \text{Measured value, scaled value} \quad \text{M\_ME\_NB\_1}\]
\[<12> := \text{Measured value, scaled value with time tag} \quad \text{M\_ME\_TB\_1}\]
\[<13> := \text{Measured value, short floating point value} \quad \text{M\_ME\_NC\_I}\]
\[<14> := \text{Measured value, short floating point value with time tag} \quad \text{M\_ME\_TC\_I}\]
\[<15> := \text{Integrated totals} \quad \text{M\_IT\_NA\_1}\]
\[<16> := \text{Integrated totals (counter) with time tag} \quad \text{M\_IT\_TA\_1}\]
\[<17> := \text{Event of protection equipment with time tag} \quad \text{M\_EP\_TA\_1}\]
\[<18> := \text{Packed start events of protection equipment with time tag} \quad \text{M\_EP\_TB\_1}\]
\[<19> := \text{Packed output circuit information of protection equipment with time tag} \quad \text{M\_EP\_TC\_1}\]
\[<20> := \text{Packed single-point information with status change detection} \quad \text{M\_PS\_NA\_1}\]
\[<21> := \text{Measured value, normalized value without quality descriptor} \quad \text{M\_ME\_ND\_1}\]
\[<30> := \text{Single-point information with CP56Time2a timetag} \quad \text{M\_SP\_NB\_1}\]
\[<31> := \text{Double-point information with CP56Time2a timetag} \quad \text{M\_DP\_NB\_1}\]
\[<32> := \text{Step position with CP56Time2a timetag} \quad \text{M\_ST\_TB\_1}\]
\[<33> := \text{Bitstring of 32 bits with CP56Time2a timetag} \quad \text{M\_BO\_TB\_1}\]
\[<34> := \text{Measured value normalised with CP56Time2a timetag} \quad \text{M\_ME\_TF\_1}\]
\[<35> := \text{Measured value scaled with CP56Time2a timetag} \quad \text{M\_ME\_TE\_1}\]
<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;36&gt;</td>
<td>Measured value floating point with CP56Time2a timetag</td>
<td>M_ME_TF_1</td>
</tr>
<tr>
<td>&lt;37&gt;</td>
<td>Integrated totals (counter) CP56Time2a timetag</td>
<td>M_IT_TB_1</td>
</tr>
</tbody>
</table>

**Process information in control direction**  
(station-specific parameter)

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;45&gt;</td>
<td>Single command</td>
<td>C_SC_NA_1</td>
</tr>
<tr>
<td>&lt;46&gt;</td>
<td>Double command</td>
<td>C_DC_NA_1</td>
</tr>
<tr>
<td>&lt;47&gt;</td>
<td>Regulating step command</td>
<td>C_RC_NA_1</td>
</tr>
<tr>
<td>&lt;48&gt;</td>
<td>Set point command, normalized value</td>
<td>C_SE_NA_1</td>
</tr>
<tr>
<td>&lt;49&gt;</td>
<td>Set point command, scaled value</td>
<td>C_SE_NB_1</td>
</tr>
<tr>
<td>&lt;50&gt;</td>
<td>Set point command, short floating point value</td>
<td>C_SE_NC_1</td>
</tr>
<tr>
<td>&lt;51&gt;</td>
<td>Bitstring of 32 bit</td>
<td>C_BO_NA_1</td>
</tr>
<tr>
<td>&lt;58&gt;</td>
<td>Single command with time tag</td>
<td>C_SC_NA_1</td>
</tr>
<tr>
<td>&lt;59&gt;</td>
<td>Double command with time tag</td>
<td>C_DC_NA_1</td>
</tr>
<tr>
<td>&lt;60&gt;</td>
<td>Regulating step command with time tag</td>
<td>C_RC_NA_1</td>
</tr>
<tr>
<td>&lt;61&gt;</td>
<td>Set point command, normalized value with time tag</td>
<td>C_SE_NA_1</td>
</tr>
<tr>
<td>&lt;62&gt;</td>
<td>Set point command, scaled value with time tag</td>
<td>C_SE_NB_1</td>
</tr>
<tr>
<td>&lt;63&gt;</td>
<td>Set point command, short floating point value with time tag</td>
<td>C_SE_NC_1</td>
</tr>
<tr>
<td>&lt;64&gt;</td>
<td>Bitstring of 32 bit with time tag</td>
<td>C_BO_NA_1</td>
</tr>
</tbody>
</table>

**System information in monitor direction**  
(station-specific parameter)

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;70&gt;</td>
<td>End of initialization</td>
<td>M_EI_NA_1</td>
</tr>
</tbody>
</table>
System information in control direction
(station-specific parameter)

- <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  C_CS_NA_1
- <104> := Test command  C_TS_NB_1
- <105> := Reset process command (slave mode only)  C_RP_NC_1
- <106> := Delay acquisition command  C_CD_NA_1

Parameter in control direction
(station-specific parameter)

Contact us if you need this
- <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)
This is unlikely to be implemented, however contact us if you need this

- <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  F_DR_TA_1
8.5 Basic application functions

Station initialization
(station-specific parameter)

Remote initialization

General Interrogation
(system- or station-specific parameter)

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

Addresses per group have to be defined

Clock synchronization
(station-specific parameter)

Clock synchronization

Command transmission
(object-specific parameter)

- Direct command transmission
- Direct set point command transmission command
- Select and execute command
- Select and execute set point
- 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

*Note this IO driver allows direct access to all bits of the IEC definition, to implement many of the above requires application layer interaction with different addresses, this is however simple scripting with most SCADA systems.
Transmission of Integrated totals
(station- or object-specific parameter)

- Counter request
- Counter freeze without reset
- Counter freeze with reset
- Counter reset
- General request counter
- Request counter group 1
- Request counter group 2
- Request counter group 3
- Request counter group 4

Addresses per group have to be defined
Parameter loading
(object-specific parameter)

☐ Threshold value
☐ Smoothing factor
☐ Low limit for transmission of measured value
☐ High limit for transmission of measured value

Parameter activation
(object-specific parameter)

☐ Act/deact of persistent cyclic or periodic transmission of the addressed object

File transfer
(station-specific parameter)

☐ File transfer in monitor direction
☐ File transfer in control direction
Appendix A : Change log

V 7.10.27
1. Added support for IEC870-5-104, TCP/IP master & slave

V 7.10.26
2. Several changes to slave mode to perfectly simulate an RTU including select execute

V 7.9.24
1. Increased number of channels from 16 – 32
2. added functionality of new datatypes to slave mode better support for status bits in slave mode. STP, IT etc
3. OPC server now sets status bad if the polling program fails

Bug fixes:
1. fixed text file import

V 7.9.23
1. Added Step position datatype to slave mode
2. Allow typing of addresses with text instead of bit numbers eg. ...:VALUE,:INVALID
3. fixed master mode bug where it was only sending commands every 2nd time the OPC client writes
4. Buffering of events so client does not loose events in the case of multiple change of state of single address in one IEC message