The Beautiful Simplicity of the Integration of Modbus, DNP3, IEC 60870-5-104, and IEC 61850 into a powerful WEB-PLC operating on an Embedded Controller

Dipl.-Ing. Karlheinz Schwarz
karlheinz.schwarz@nettedautomation.com
NettedAutomation GmbH, Karlsruhe

The experience has shown that manufacturers are still shying away from the high costs and long time required for the development of new products based on standards like IEC 61850 and IEC 61400-25 (Wind Turbines) because the implementations and applications are quite complex. For these reasons, a team at NettedAutomation developed a web-based integration tool based on Beck IPC's com.tom WEB-PLC[1] that significantly streamlines the application of these and other standards and the implementation of simple logic functions that consume and generate data communicated with a variety of protocols. The solution can be used to build various kinds of IEDs[2] for monitoring, control, data concentrators, data aggregators, and gateways.

Key words: *Modbus, IEC 60870-5-104, IEC 61850, IEC 61400-25, gateway, PLC, monitoring, control, programming*

1. Introduction

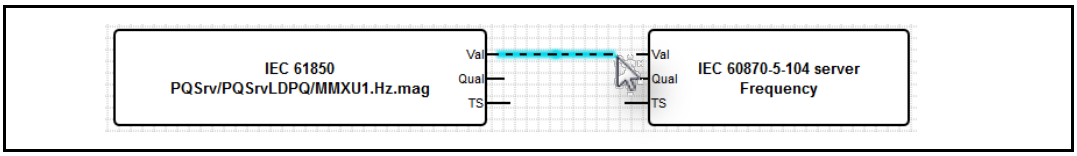
Beck IPC, NettedAutomation and SystemCorp offer products and services for all aspects in advanced control technologies and communication for any industrial applications and energy delivery domains. Key products are the wide range of WEB-PLC based Beck IPC's com.tom. These devices provide connectivity with protocols like IEC 61850, IEC 61400-25, and IEC 60870-5-104, and DNP3. The solutions allow for a very short-time-to-market implementation of these standards. The com.tom solution is a powerful real-time operated and secure platform for monitoring and controlling of power system components like transformers, power quality monitors, wind power, photo voltaic, CHP, batteries to name just a few.

The various modules allow building simple devices that just support field communication with Modbus, M-Bus or simple I/Os. Further options are applications with integrated servers providing IEC 60870-5-104 or IEC 61850 connectivity to the process level. The information of the process level can easily be aggregated into gateways and proxy servers to allow secure information exchange with control centers, condition monitoring systems, maintenance personnel or other applications.

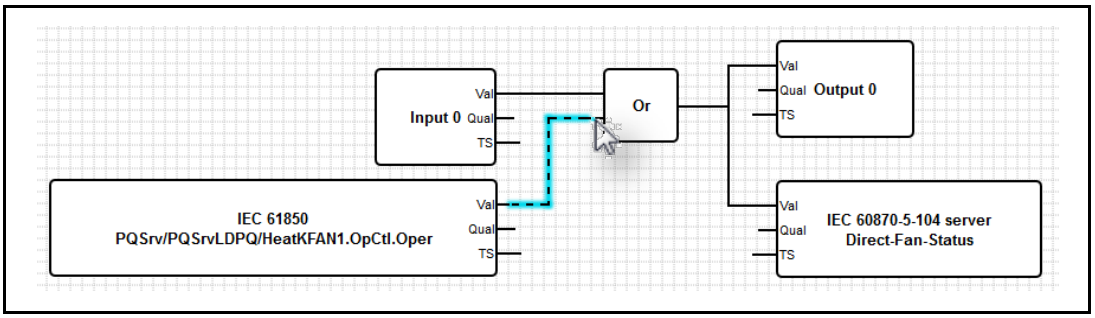
[1] com.tom = **com**munication **to m**achine; PLC = programmable logic controller
2 IED = Intelligent Electronic Device

The crucial benefit comes with the application of the WEB-PLC that uses since 2005 a powerful real-time processor platform integrated into an embedded controller. All functions and applications of, e.g., Ethernet, TCP/IP, MMS, openVPN, NAT, Modbus, logic functions, function blocks, IEC 60870-5-104, and IEC 61850 are embedded and can be used right away – without writing a single line of program code. The applications are configured just by drawing lines between input objects, logic functions, and output objects.

The input signals (frequency received from an IEC 61850 server) as shown in the following figure can easily be marshalled in a gateway to an IEC 60870-5-104 signal – just by drawing a line between the two WEB-PLC objects. The notation of the WEB-PLC objects relative to the signals modelled in IEC 60870-5-104 and IEC 61850 is explained in Annex 1.

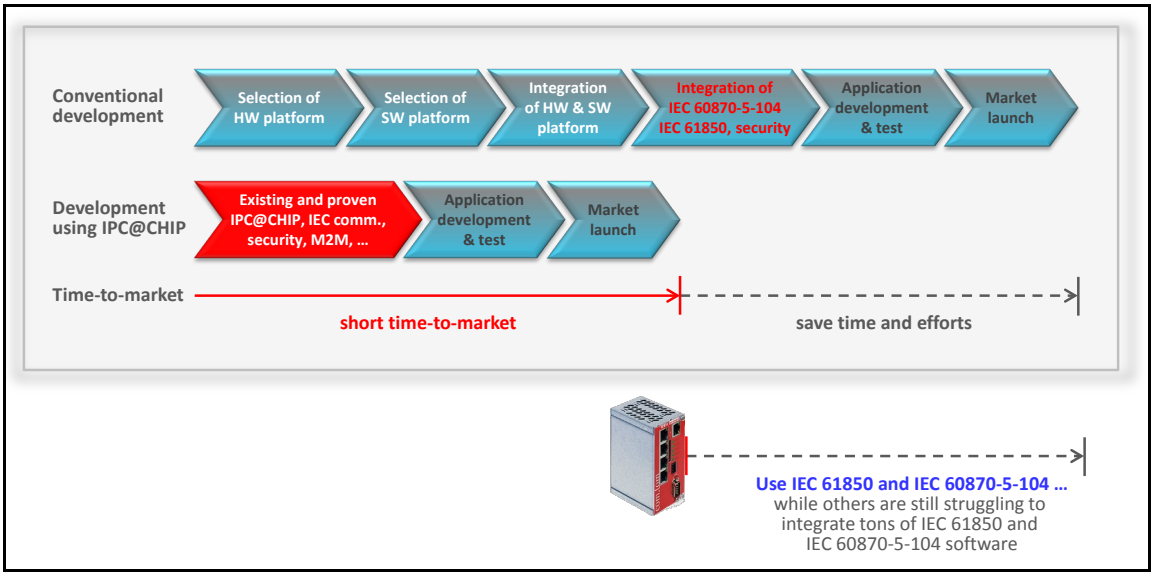


Input signals from a local terminal (Input 0) or a signal received from an IEC 61850 server (operate command) may be used as input for logic functions (e.g., Or, And) as exposed in the following logic diagram. The output of an Or function could be connected to an output function (local output 0 at first physical terminal). In addition the signal is also used as an output signal communicated through IEC 60870-5-104 (object on the bottom right).



Very little configuration information, e.g., for fire walls and openVPNs, needs to be entered in special web-based forms as shown in the following figure.

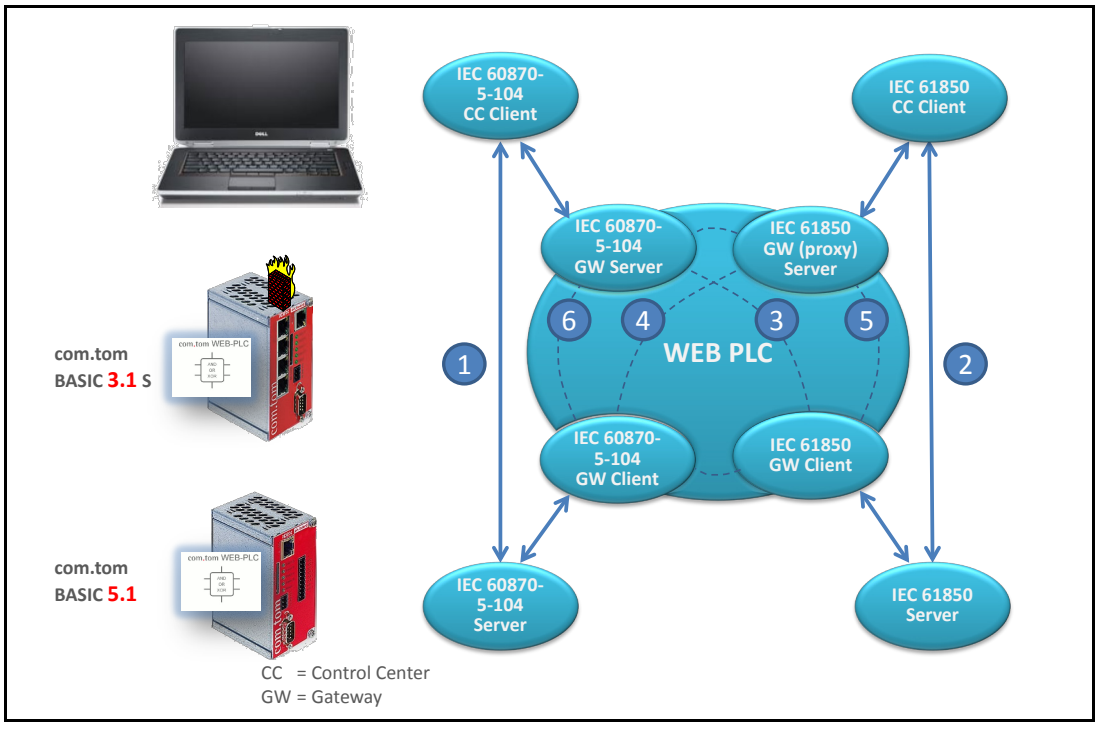
The IEC 60870-5-104 and IEC 61850 integrated into the WEB-PLC streamlines the development process as shown in the next figure. The crucial benefit of the solution described in this document is the short time-to-market development for monitoring and automation functions that need to exchange signals with many other devices – over a variety of standard protocols without a special tool. The WEB-PLC is a high level web-based tool for controlling and monitoring of a variety of processes in the electric power domain and many other domains. The com.tom devices support in addition to the WEB-PLC also IEC 61131-3 (CoDeSys) and C/C++ programming. The core component of the com.tom (the IPC@CHIP controller SC 143) can, too, be integrated into any other device – offering the same functionality.



The next clauses describe the steps to build various applications and gateways using standardized and secure communication and SCL[3] configuration mechanisms. The description requires basic knowledge about PLCs and standards like IEC 60870-5-104 and IEC 61850.

2. Topologies of IEDs implemented

The following figure shows the many options available for the painless and quick realization of systems that let any signal cross protocol and device boundaries. The WEB-PLC enabled com.tom is a very powerful and easy to use device allowing uncomplicated and elegant solutions to frequently encountered automation problems.



[3] SCL = System Configuration Language, IEC 61850-6

The web-based solution of the WEB-PLC incorporated in the Beck IPC com.tom significantly streamlines the direct application of the standards:

(1) IEC 60870-5-104 (DNP3 in preparation) – for details see clause 5
(2) the direct application of the standards IEC 61850 and IEC 61400-25 – see clause 5

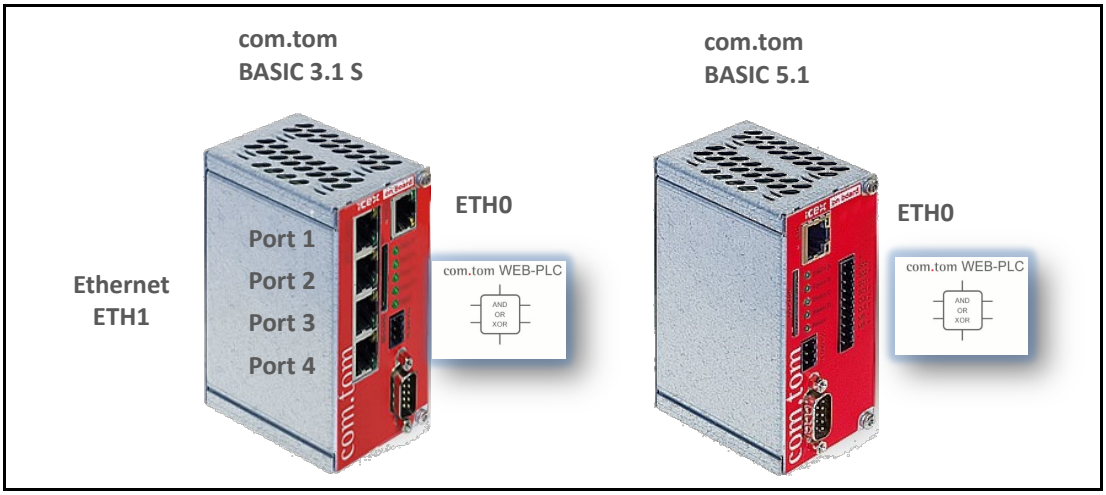
and the web-based configuration of gateways between:

(3) IEC 61850 server and IEC 60870-5-104 client – for details see clause 6
(4) IEC 60870-5-104 (DNP3) server and IEC 61850 client
(5) IEC 61850 server and IEC 61850 client – for details see clause 7
(6) IEC 60870-5-104 (DNP3) server and IEC 60870-5-104 (DNP3) client

The “stream” of signals is configured with a standard web-browser like Firefox – no additional vendor-specific or third-party tool is required to let signals “travel” between any two devices.

3. com.tom devices applied in this report

The two com.tom devices BASIC 3.1 S and BASIC 5.1 are used for the demonstration of the beautiful simplicity of building applications. The BASIC 5.1 (right in the following figure) is used as an interface to the process to monitor and control it. The BASIC 3.1 S (left) is used as a gateway, switch, and router; it comes with an Ethernet switch that can be used to build a sub-network for the process monitoring and control and to separate the process interface from a higher level system.



The com.tom BASIC 5.1 provides

one Ethernet Port, one serial Port RS232/RS485 (used for Modbus), SD-Card Slot, 4 digital Input, 4 digital Output, WEB-PLC Programming

http://www.com-tom.de/products.php?device=com.tom BASIC 5.1

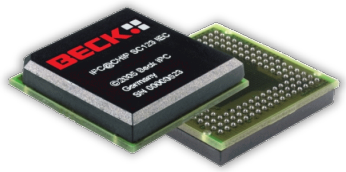
The powerful com.tom BASIC 3.1 S provides

one Ethernet Port, one serial Port RS232/RS485, SD-Card Slot, **4-port Ethernet Switch**, WEB-PLC Programming

http://www.com-tom.de/products.php?device=com.tom BASIC 3.1 S

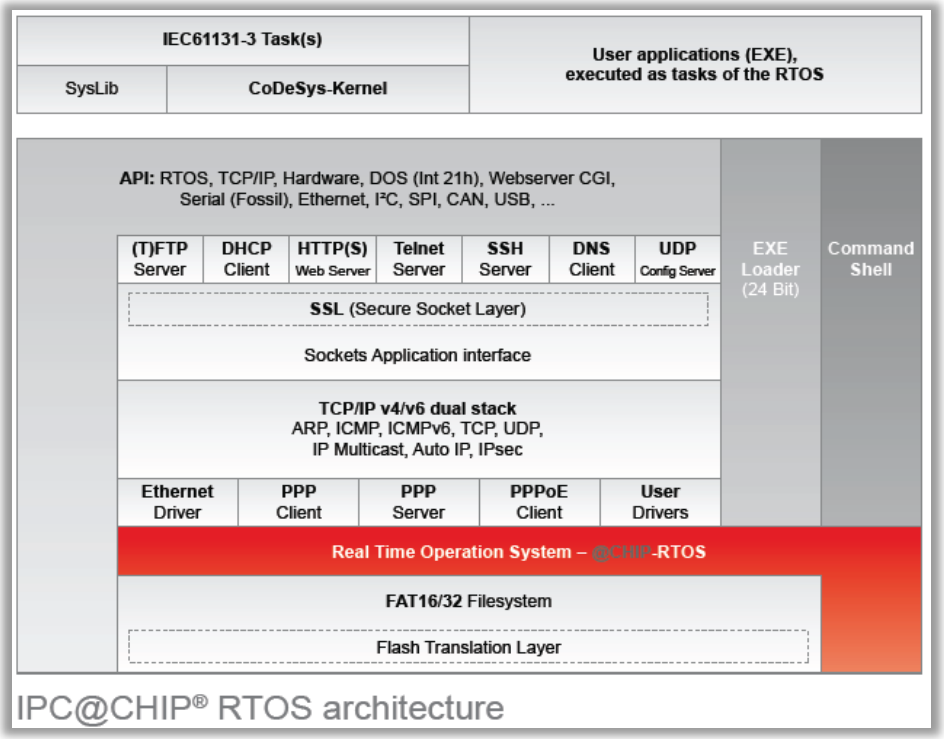
Other com.tom devices support wireless communication, mobile connectivity, fieldbus and many more possibilities.

The “heart” of the com.tom is the so-called Beck IPC@Chip embedded controller SC143 running the RTOS real-time operating system.



http://www.beck-ipc.com/en/products/sc1x3/sc143.asp

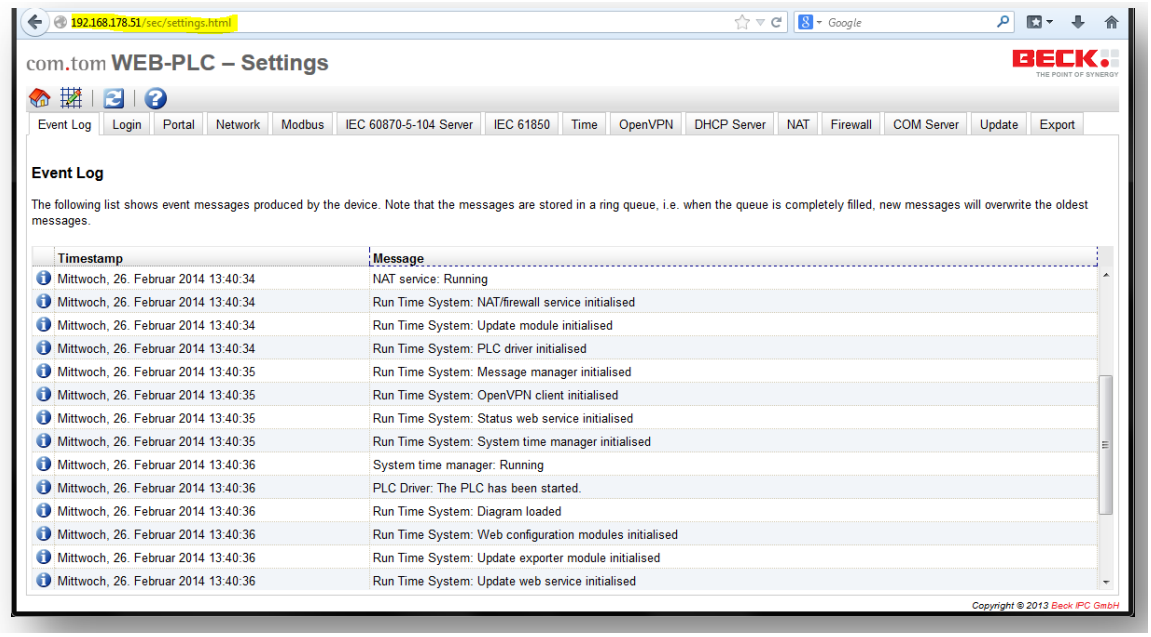
The Software architecture of the RTOS (real-time operation system) is very comprehensive as shown below:



The embedded controller is an industry proven component that is on the market in industrial automation systems for some 10 years. It is a modular controller chip (IPC@CHIP). The substantial advantage of the embedded controller based solution is its high efficiency, performance, and the minimum expenditure needed for the implementation of IEC 60870-5-104 and IEC 61850-based interfaces for application functions. This platform is very economical. More powerful embedded controllers are available.

From a programming point of view the controller is a PC and a PLC – it can be programmed in C/C++ as well as in IEC 61131-3 (CoDeSys), finally the WEB-PLC provides a very easy

approach to graphically design applications and gateways. The WEB-PLC is the basic tool to configure the application, the information, and the information flow with the process, functions, and IEDs. The overview of the WEB-PLC is depicted in the following figure.



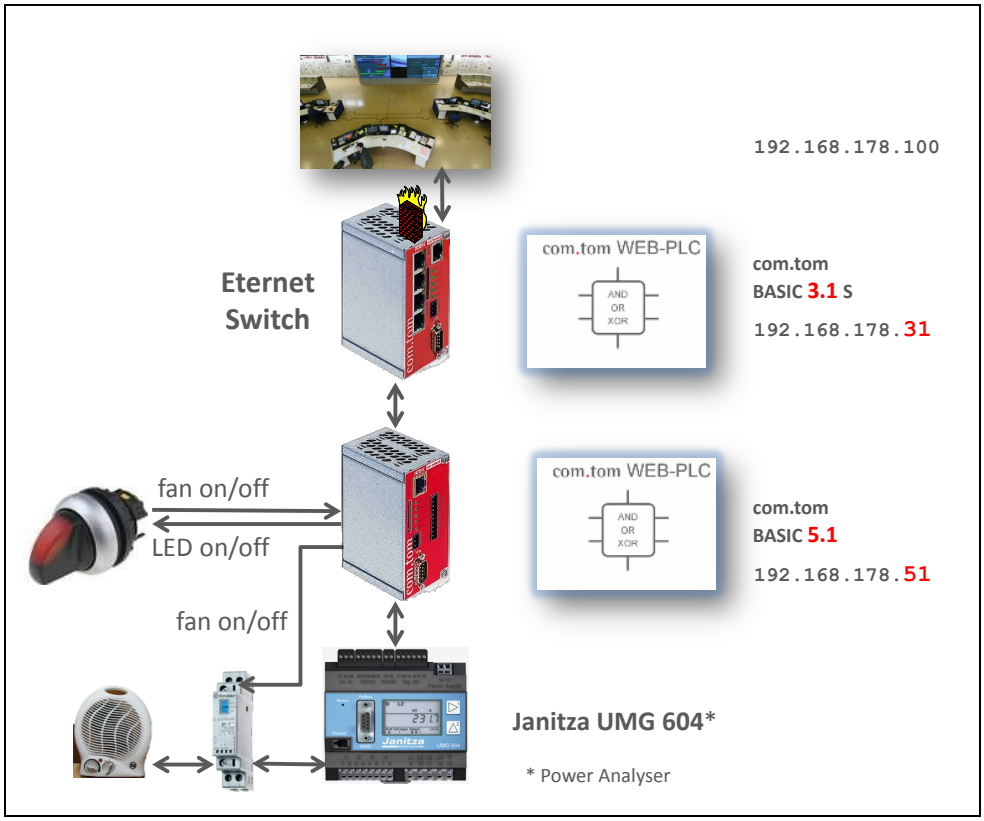
4. Application topology from process to control center

According to the figure below there is a process level with the Janitza power quality analyzer UMG 604 that provides measurements and calculated values of the electrical system like voltage, current, frequency, phase angle, and harmonics. In addition a fan heater can be controlled by an application implemented at the WEB-PLC. The WEB-PLC controls the heater and the LED in the switch at the left side. The heater can be operated locally by that switch or remotely by communication commands coming from the com.tom BASIC 3.1 S or even directly from the control center. The latter case requires to route from the control center directly through to the com.tom BASIC 5.1.

The measured values are communicated through a serial Modbus protocol to the com.tom BASIC 5.1. The fan heater is used as a controllable load. The control and monitoring of the process is implemented as a logic running at the WEB-PLC of the com.tom BASIC 5.1.

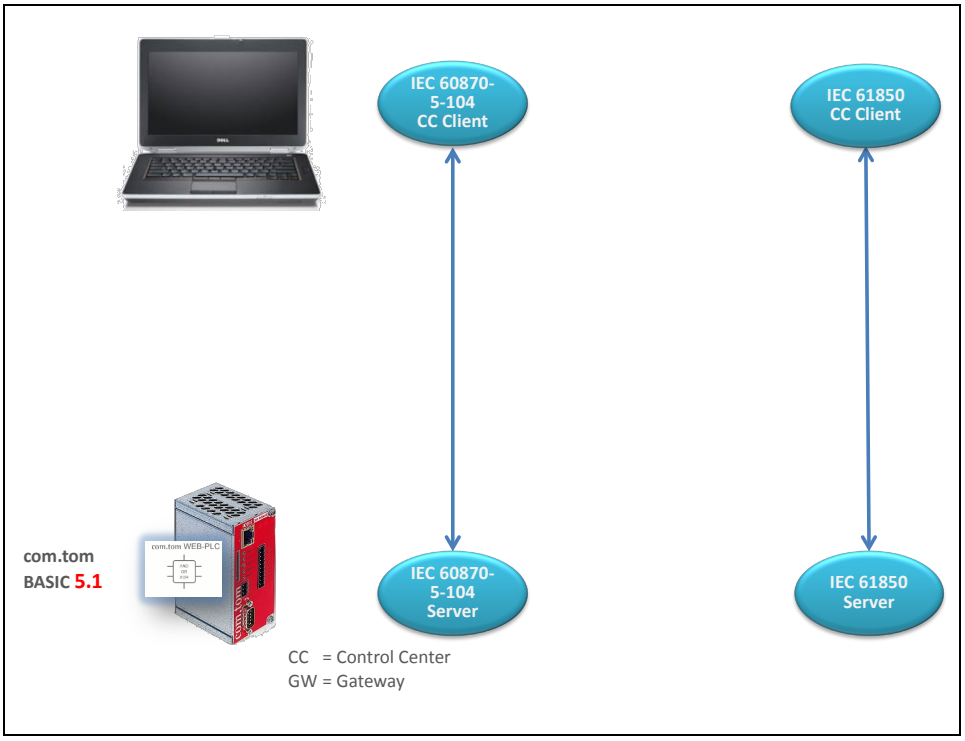
The com.tom BASIC 5.1 can run an IEC 60870-5-104 server (slave) and an IEC 61850 server. All signals to be exchanged with the com.tom BASIC 5.1 can be communicated through either of the two servers. The top com.tom BASIC 3.1 S is used as a gateway, e.g., between an underlying IEC 61850 server and a control center that uses the IEC 60870-5-104 protocol or DNP3.

The BASIC 3.1 comes with a 5-port Ethernet switch and NAT router incorporated. The gateway may additionally act as an IEC 61850 proxy server that aggregates the signals of multiple underlying IEC 61850 servers. All applications and gateway functions are implemented with the WEB-PLC.

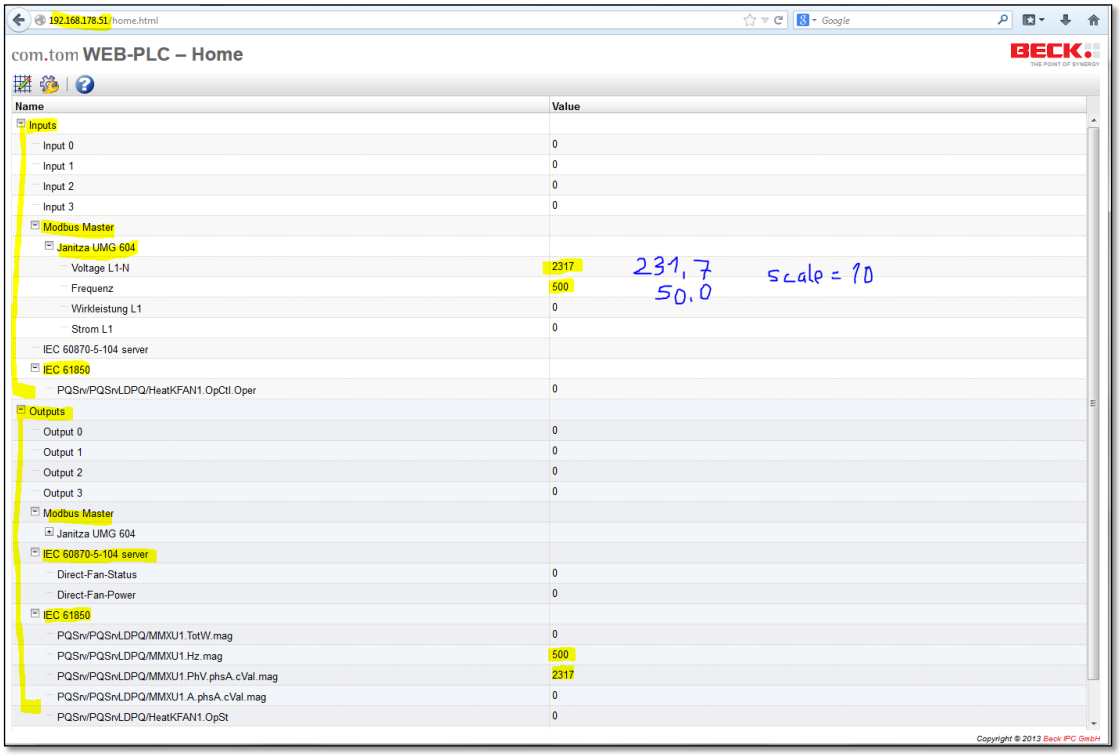


5. Process level applications and communication

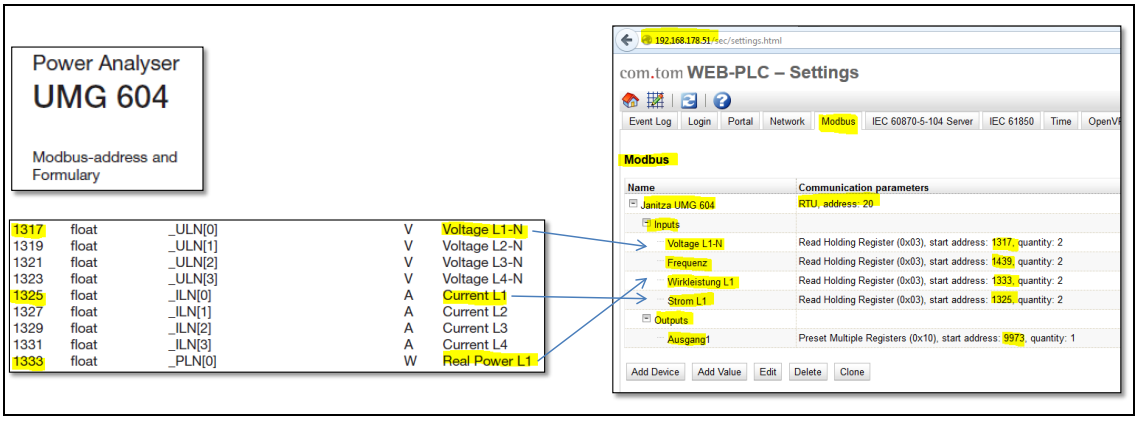
The process interface is implemented at the com.tom BASIC 5.1 with IEC 60870-5-104 or IEC 61850 connectivity. The two standards can directly be used as sketched in the figure below.



The input and output signals of the process are communicated via Modbus and by local I/Os of the com.tom BASIC 5.1. All signals are available at the WEB-PLC for processing or communication. A standard web browser is used to connect to the com.tom WBE-PLC. The complete list of signals that can be used at the WEB-PLC is shown in the next figure. The inputs are on the top and the outputs in the second half. The current values of the signals are exposed as well. The values are scaled by a fixed factor of 10 (2317 means 231,7).



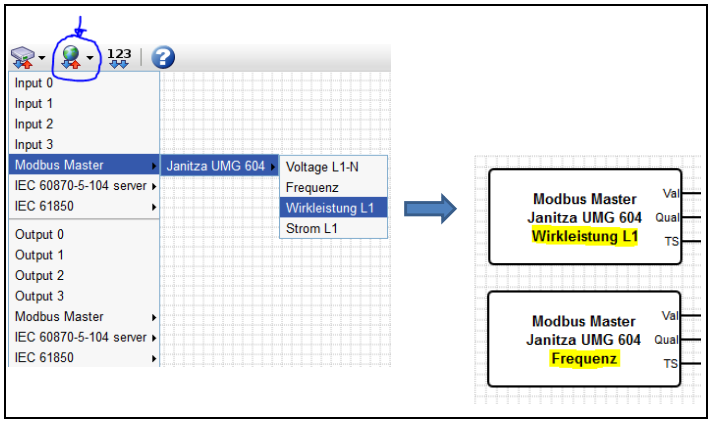
One task is to configure these signals and the signal flow. The local I/Os are inherently available at the com.tom BASIC 5.1. The other signals need to be configured. The configuration of the Modbus and IEC 60870-5-104 signals is done through web-based forms. The indexes of the Modbus signals are usually documented in a table by the vendor of the Modbus server. In the case of the Janitza UMG 604 the needed signals and their mapping to the WEB-PLC are as shown in the next figure.



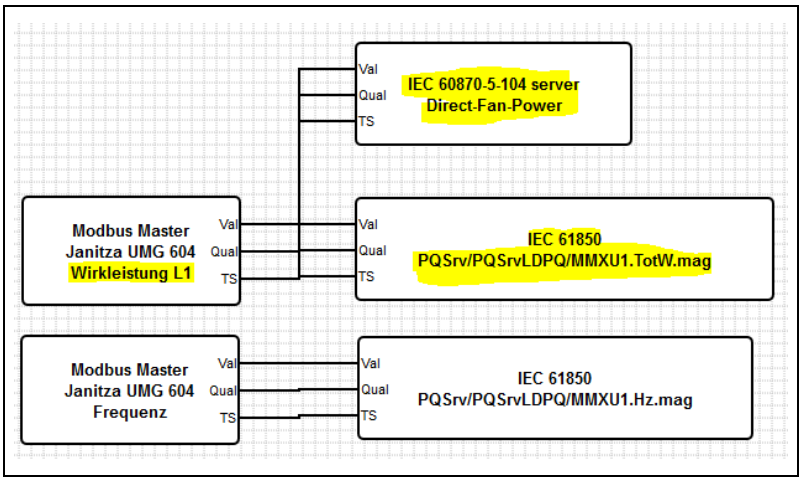
The names of the WEB-PLC objects (“Strom L1” for the index 1325) can be configured freely.

The signals available at the WEB-PLC are listed in a drop-down menu for immediate use in a logic diagram (see next figure). Any object can be placed as graphical object on the WEB-

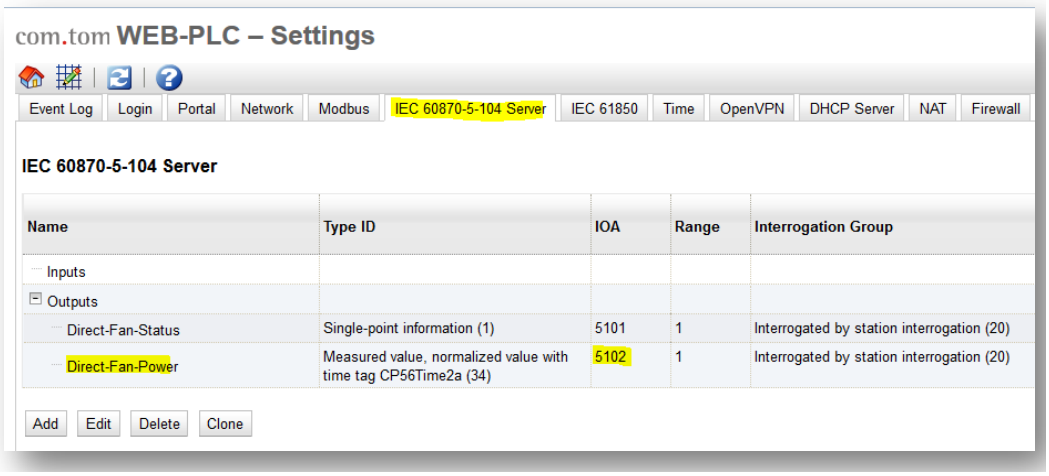
PLC working space of the web browser. The measurement “Wirkleistung L1” (from Modbus signal 1333) is used as input to the WEB-PLC. The measurement can be used for any reasonable function at the WEB-PLC.



The incoming signal (from the Janitza PQ Analyzer) can be communicated through an IEC 60870-5-104 server or an IEC 61850 server as depicted below. The same signal may be communicated for different use-cases simultaneously.

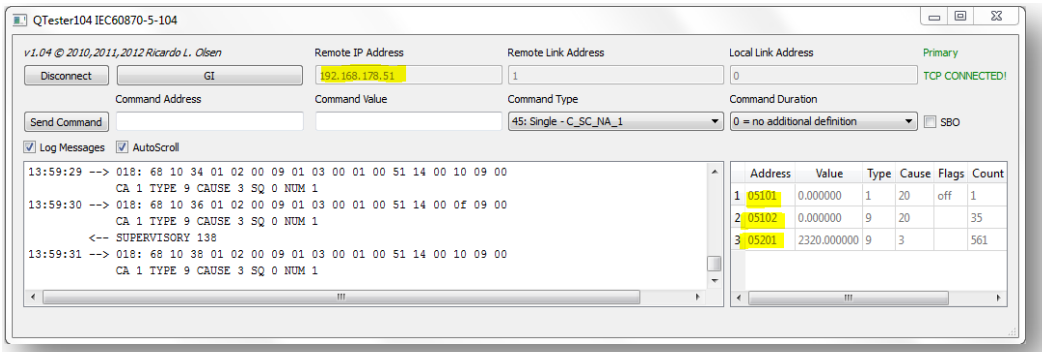


The signal list for the IEC 60870-5-104 server has also to be configured manually by filing out a form at the web browser. The WEB-PLC object “Direct-Fan-Power” (configured for the WEB-PLC) is communicated as a measurement value with IEC 60870-5-104 message type identifier 34 and information object address 5102:



Other objects can be added by pushing the bottom “Add”.

The WEB-PLC objects for IEC 60870-5-104 can be accessed by an IEC 60870-5-104 client, e.g., the QTester104 as shown in the next figure.



One crucial question remains: How are the signals configured that are intended to be communicated with IEC 61850? The WEB-PLC incorporates an XML and SCL parser that can analyze a given CID[4] file and automatically generate the IEC 61850 related input and output objects of the WEB-PLC. The names of the WEB-PLC objects are derived from the object references according to the functional constraints ST, MS, CO, and SP of the CID. The retrieved information model is shown as a tree (see next figure). The only decision to be made is: Which Data Objects and Data Attributes should become WEB-PLC objects. Any subset could be selected.

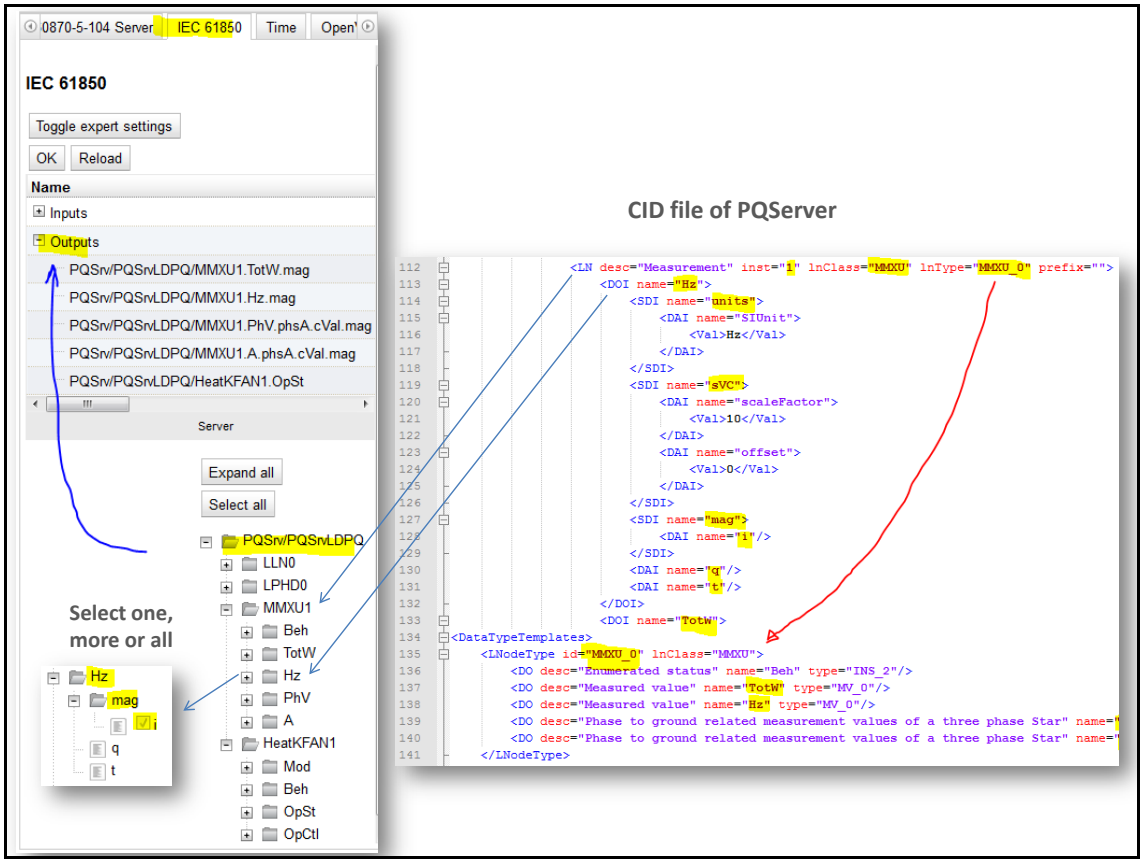
At the left bottom side the frequency “Hz” has been selected (check box) for use at the WEB-PLC. “Hz” belongs to the Logical Node MMXU1 (3-phase measurements of an AC electrical system).

The frequency “Hz.mag.i” has been selected to become a WEB-PLC object – the quality attribute “q” and timestamp “t” are automatically selected with the “mag”. The name of the WEB-PLC object as shown in the output list is derived from the object reference of the signals in the SCL file (“PQSrv/PQSrvLDPQ/MMXU1.Hz.mag”) where “PQSrv” represents the IED, “PQSrvLDPQ” the Logical Device name and “MMXU1” the Logical Node instance name, “Hz” the Data Object name and “mag” the Data Attribute name.

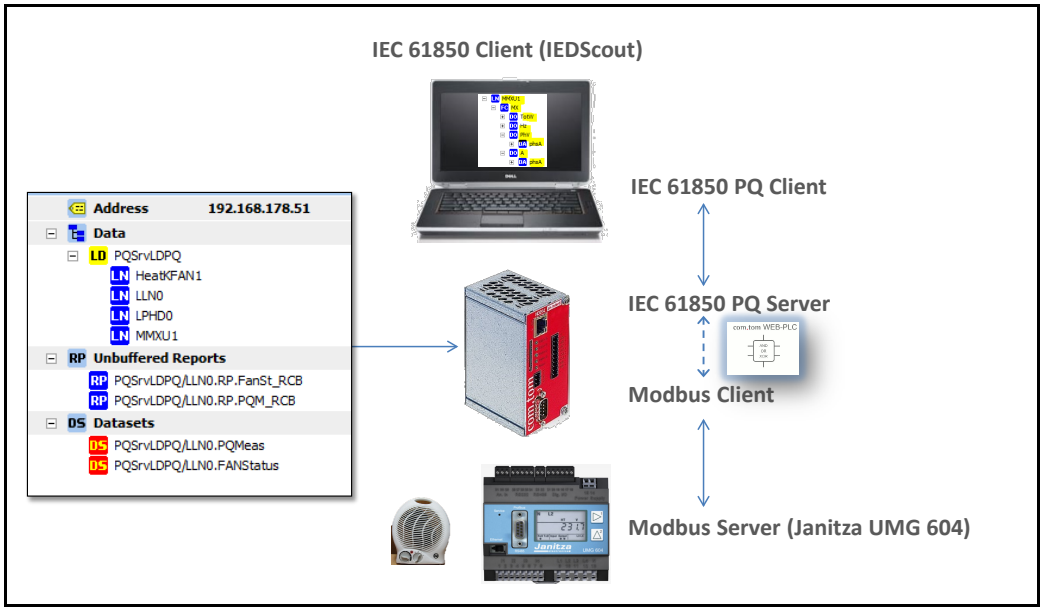
The Signals selected from the CID file are now available for further processing at the WEB-PLC. The frequency model “MMXU1.Hz.mag” is just an instantiated model of the logical node class MMXU. The instance is numbered with the extension “1”. At the WEB-PLC level there is an easy way to link the frequency in that instance to a real frequency measurement provided by the Janitza device. As can be seen three figures above the frequency value from the Janitza UMG 604 is connected with the “PQSrvLDPQ/MMXU1.Hz.mag”.

An IEC 61850 client can read out this frequency value or can receive reports with that value.

[4] Configured IED Description; this is a configuration file according to IEC 61850-6 (SCL – system configuration language).



The signal “Wirkleistung L1” can be communicated by IEC 60870-5-104 or by IEC 61850. There is no need to write a single line of program code. Any client for IEC 60870-5-104 (e.g., the QTester104) or for IEC 61850 (e.g., IEDScout as shown in the figure below) can be used to receive the total active power provided by the power quality monitoring device Janitza UMG 604. Any other underlying monitoring device would end up exposing the same standardized signals – there is no need to understand proprietary signal lists.

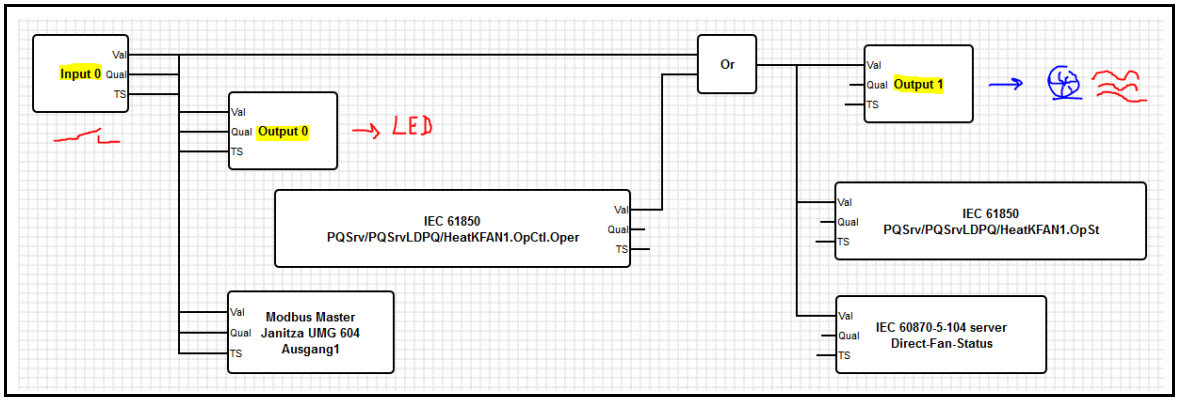


The signals for the most known measurements in the power systems are standardized in IEC 61850 as logical nodes (e.g., MMXU) that contain data objects (e.g., TotW and Hz). Most of

the signals provided by the Janitza UMG 604 can be exposed by Logical Node classes defined in IEC 61850-7-4 Edition 2 like:

- Environmental information: MENV
- Flicker measurement: MFLK
- Harmonics or interharmonics: MHAI
- Non-phase-related harmonics or interharmonics: MHAN
- Metering: MMTR
- Non-phase-related measurement: MMXN
- Measurement: MMXU
- Sequence and imbalance: MSQI
- Metering statistics: MSTA

The control logic and the corresponding signals are shown in the following figure. In this application the fan heater is controlled either locally by the switch (input 0) or by an operate message to “PQSrv/PQSrvLDPQ/HeatKFAN1.OperCtl.Oper” coming in through an IEC 61850 object. The status of the heater is communicated through IEC 60870-5-104 and IEC 61850.

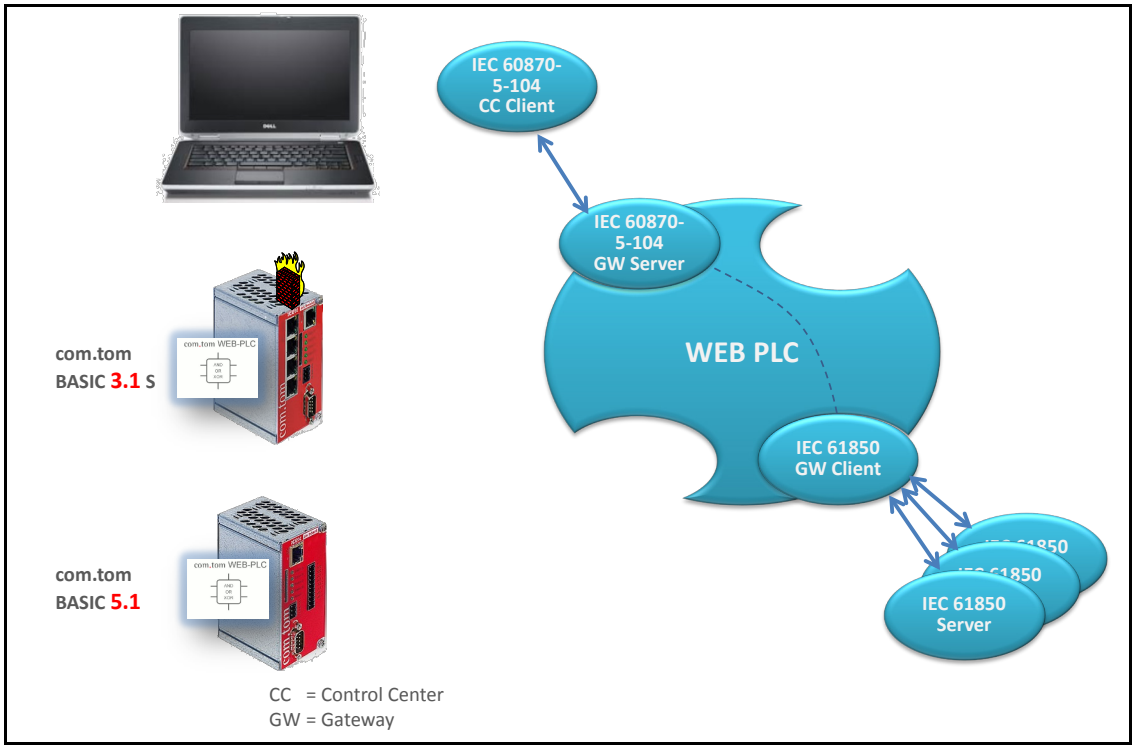


Any other reasonable application can be configured graphically by placing signals on the work space and connecting them with functions (e.g, an OR gate) and other signals.

6. Building gateways from IEC 61850 IEDs to IEC 60870-5-104 IEDs

The very same web-based approach as introduced above can be applied to build hierarchical monitoring and control systems and Gateways. The gateway between aggregations of IEC 61850 IEDs (e.g., transformer condition monitoring devices) to IEC 60870-5-104 is shown in the next figure. The com.tom 5.1 at the bottom is used as an example of an IEC 61850 IED. Further IEDs from any other vendor that is conformant to IEC 61850 could be applied as well.

The signals of the IEC 60870-5-104 server need to be configured as described above. The WEB-PLC for the gateway has to interpret the CID file provided for the IEC 61850 client. That CID file is built by a subset of all ICD files of all IEC 61850 IEDs that need information being communicated to the WEB-PLC of the com.tom BASIC 3.1 S for applications running on that device or to pass through to the control center applying IEC 60870-5-104. Of course, this uplink could also be implemented by DNP3.

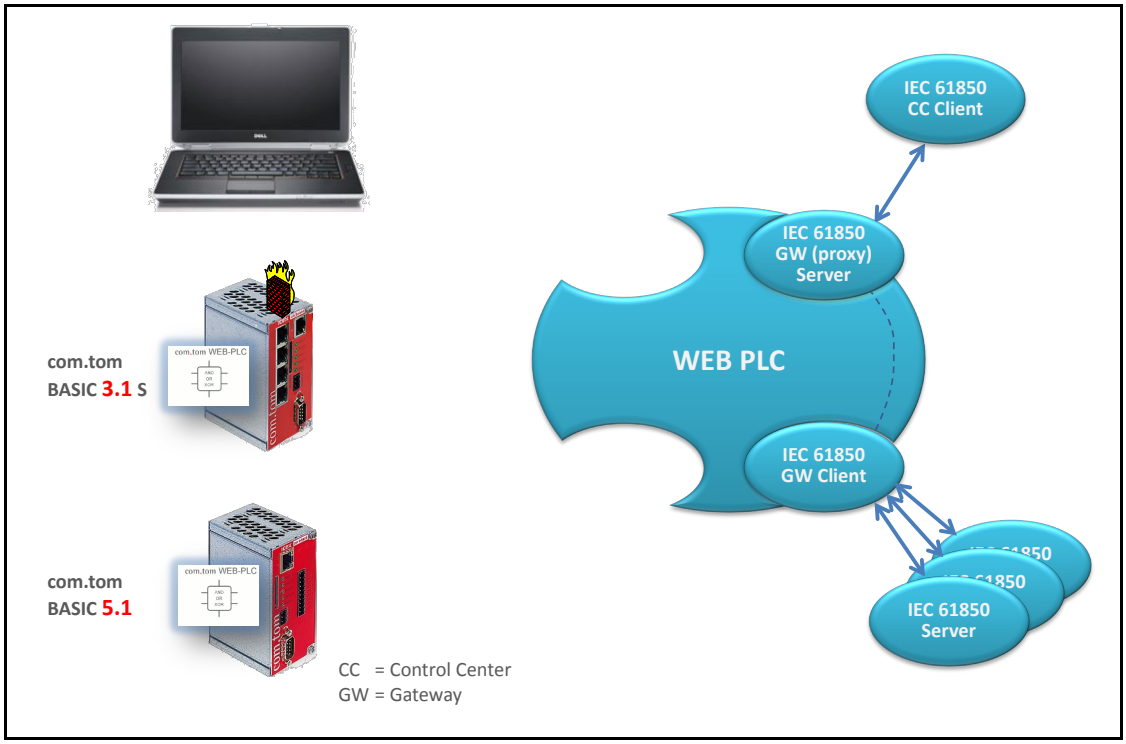


The application and marshalling of the signals at the WEB-PLC of the com.tom BASIC 3.1 S works in the same way as described above – it is the same WEB-PLC, just running on a separate com.tom: the BASIC 3.1 S. This com.tom has also an Ethernet switch and NAT integrated that could be used to build a separate sub-network for the process automation. The second Ethernet port (to the upper right corner) is part of a different sub-network – thus allowing a quite secure topology that separates the access from the control center from the access to the IEDs. Firewall and openVPN and other means could be applied as well. The BASIC 3.1 S even allows port mirroring at the switch to easily trace the Ethernet traffic of all ports – this is crucial for testing.

7. Building gateways from IEC 61850 IEDs to IEC 61850 IEDs

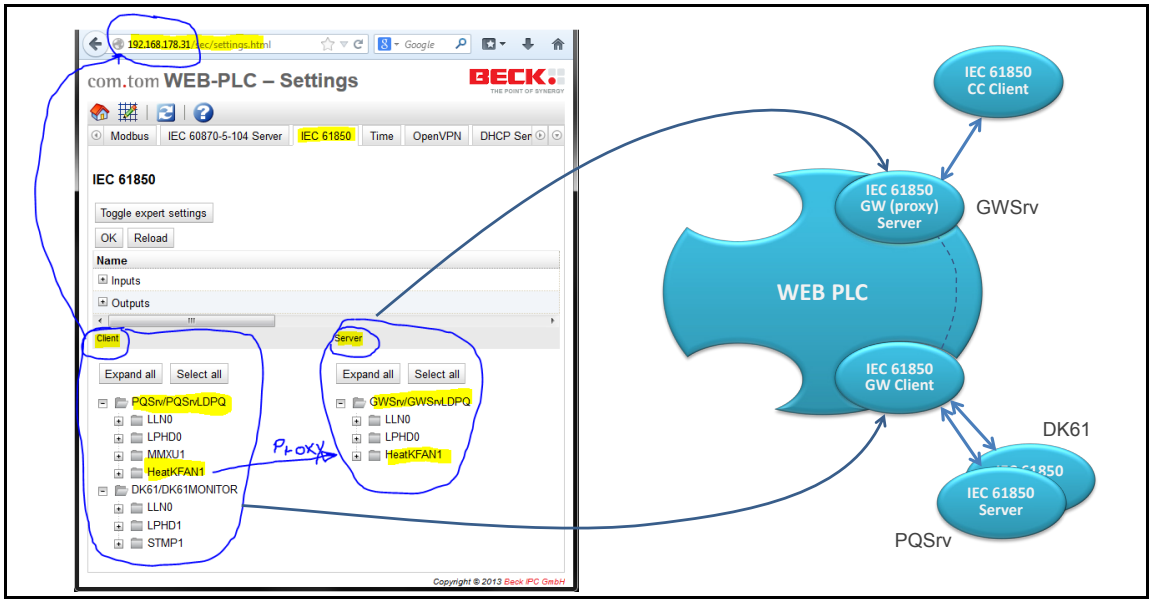
There are still two recesses in the ellipse of the gateway in the last figure. One is used for an IEC 61850 uplink and the second is for an IEC 60870-5-104 downlink. This allows building multiple gateways – according to the need of an application – in one and the same box running concurrently and configurable independently (see next figure). All signals at the WEB-PLC can be processed further; this allows getting more than just a gateway between protocols.

One application could be to aggregate the measurements or calculated values of the underlying IEDs. Let's say, 10 underlying IEDs provide the active power of 10 PV inverters. The 10 values are received by the client in the gateway. The sum of the 10 values can be calculated by a function of the WEB-PLC. Another application could be to build summary alarms out of any alarm that is reported by the underlying IEDs.



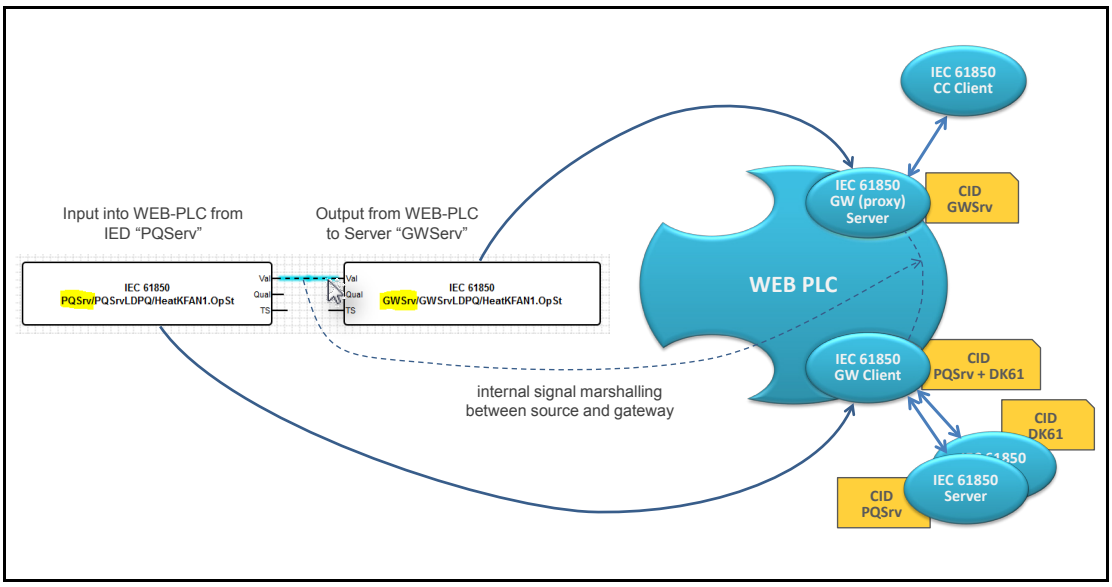
The example in the following figure models and creates an IEC 61850 proxy server that "mirrors" the underlying fan heater status (fan heater operational status). The com.tom BASIC 3.1 S acts as an IEC 61850 client to two IEC 61850 IEDs: com.tom BASIC 5.1 with the IED name "PQServ" and DK61 with IED name "DK61". These two IEDs implement each an IEC 61850 server.

The WEB-PLC of the com.tom BASIC 3.1 S has input signals from the two underlying IEDs and output signals to the server "GWServ" that is connected to the IEC 61850 client in the control center. The status of the fan heater "HeatKFAN1" is defined in the underlying IED and in the proxy gateway IED.



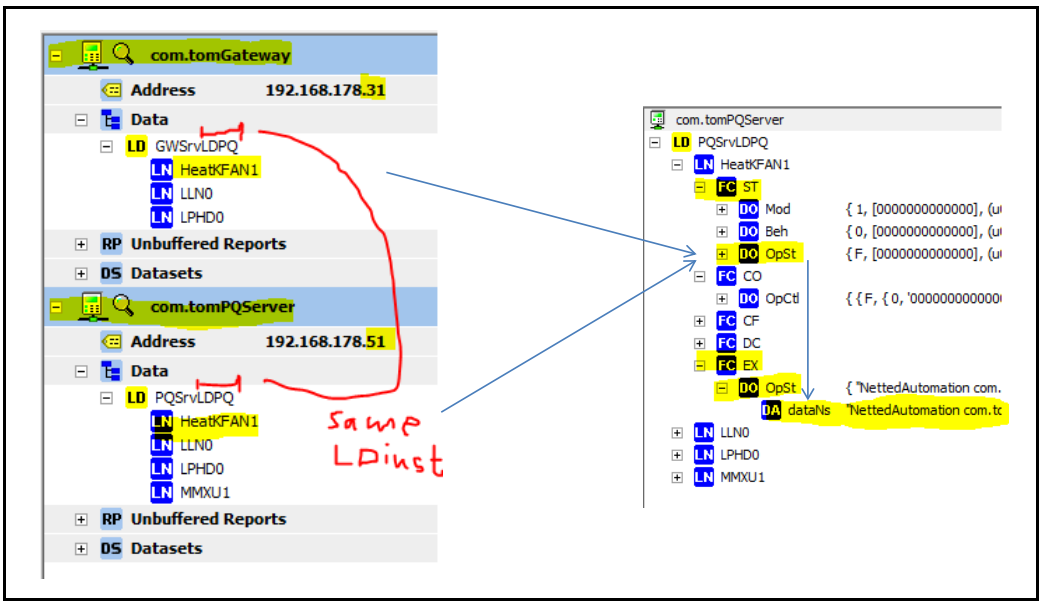
The internal "link" between the fan heater status coming from the underlying IED and the server for the uplink is configured by drawing a line between the input signal and the output

signal as depicted in the following figure. The required SCL files for the hierarchical system including a proxy server are shown to the right of the server and client icons.



The status data object "OpSt" (operation status) of the fan heater is an extended object in the standard logical node class "KFAN". This logical node class is used to operate the fan remotely by an IEC 61850 operate service. If the fan is locally switched on and off then there needs to be a separate status object that exposes the current status. The extension is specified by the attribute "dataNs" (data namespace). This namespace concept is defined for extended logical nodes and data objects. It makes sure that the standard models and the extended modes are clearly separated. The com.tom BASIC 3.1 S automatically connects to the BASIC 5.1, checks the report control blocks and enables them in a plug&play manner – this information is configured in the CID file and processed by the IEC 61850 software. No manual intervention is required to connect the gateway (GW Client) with the underlying IEDs (PQServ and DK61). The CID file for the client in the com.tom BASIC 3.1.S knows everything it needs to know about the two servers and about itself as a client talking to two servers.

The next figure shows the access from IEDScout to the two independent servers: "GWServ" and "PQServ".



The IDScout is a browser (client) and test tool to connect to servers. The connection has to be configured and initiated manually. The application of the hierarchical system of two levels of com.toms is different in the way that it has to run without human operators.

8. Resume

The high costs and long times required for the development of products based on standards like IEC 61850 and IEC 61400-25 (Wind Turbines) have been reduced dramatically. The web-based integration tool that is based on Beck IPC's com.tom WEB-PLC has significantly streamlined the application of these and other standards and the implementation of simple logic functions that consume and generate data communicated with a variety of protocols. The solution can be used to build various kinds of IEDs for monitoring, control, data concentrators, data aggregators, and gateways.

It has never been easier, faster, and more cost effective to get your application data communicated by IEC 60870-5-104, IEC 61850 and IEC 61400-25.

You are just minutes away to let your signals speak one of the standards.

For more information visit the following webpage:

http://www.blog.iec61850.com

or contact:

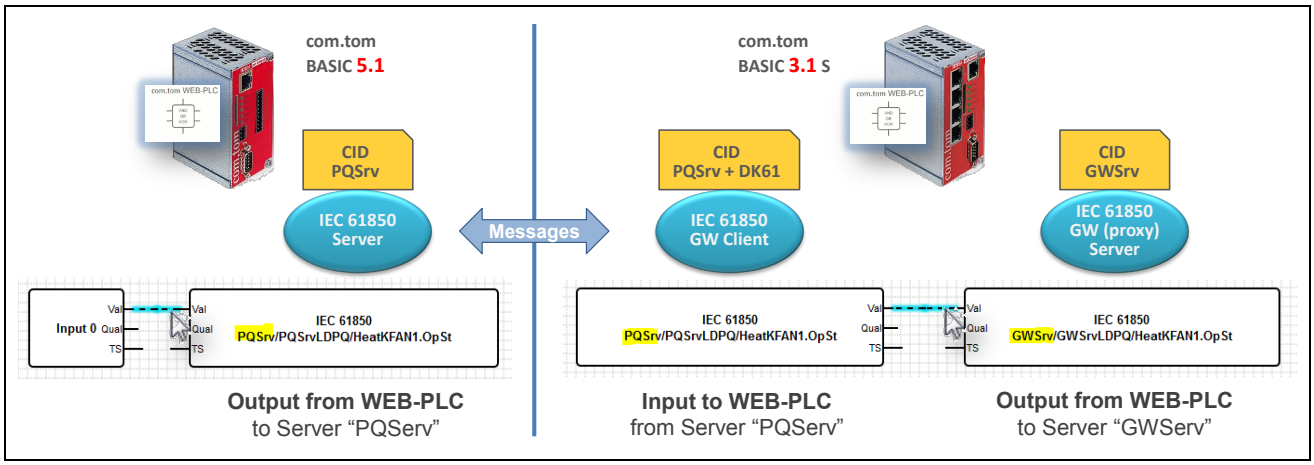
NettedAutomation GmbH
Im Eichbaeumle 108
D-76139 Karlsruhe
Germany
Phone +49-721-684844
Fax +49-721-679387
http://www.nettedautomation.com
info@nettedautomation.com

or

Beck IPC GmbH
Nauborner Straße 184
35578 Wetzlar
Phone +49-6441-3092-0
http://www.beck-ipc.com/en

Annex 1 WEB-PLC Object notation and signals in IEC 60870-5-104 and IEC 61850

The signal flow between the process (exposed by the “Input 0” object) and any hierarchical level uses the notation sketched in the following drawing.



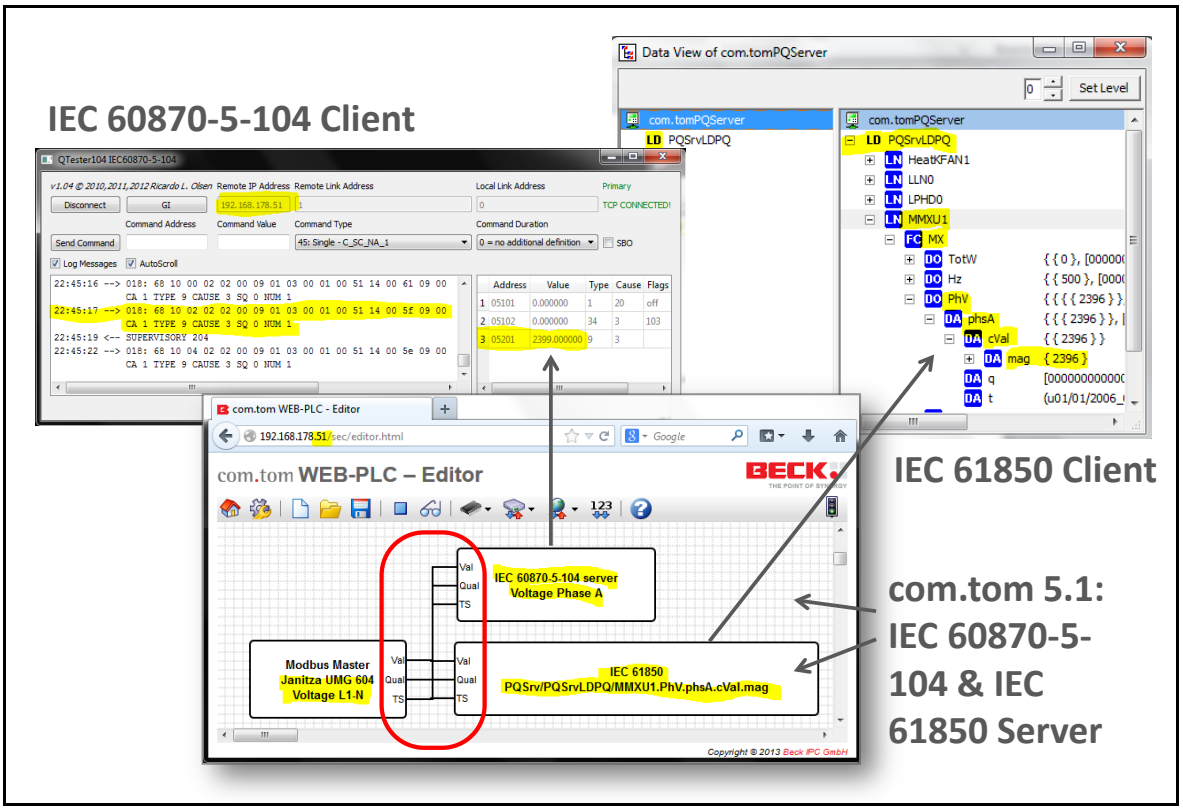
The heater fan status object at the WEB-PLC is an output object as shown on the left side (in the com.tom BASIC 5.1) and representing an IEC 61850 status object of the server “PQServ”. This status is reported by a message to an IEC 61850 client in com.tom BASIC 3.1 S and exposed as an input object at the WEB-PLC. This input object is finally marshalled to an output object (to the IEC 61850 proxy server “GWSrv”) in order to report the value to a higher level IEC 61850 client (not shown here).

Care has to be taken to differentiate the use-cases of incoming and outgoing signals defined for the WEB-PLC and used in conjunction with communication solutions like IEC 61850 and other standards. A status signal may be used as an output (IEC 61850 server) or as an input (IEC 61850 client).

Note that at the WEB-PLC level the signals flow from left to right.

Annex 2 WEB-PLC to build two mappings in parallel: IEC 60870-5-104 and IEC 61850

The signals from the Janitza Power Quality Analyser can flow from the incoming process (exposed by the “Voltage L1-N” object) to any output signal as shown in the following drawing.



The same value can be mapped to two standard mappings:

1. MMS according to IEC 61850-8-1 and IEC 61400-25-4 Annex C
2. IEC 61400-25-4 Annex D (mapping to IEC 60870-5-104)

The two mappings may be used in parallel to communicate some operational data to a control center by IEC 60870-5-104 and non-operational data to the owner’s monitoring system by IEC 61850-8-1.

The solution is very flexible. The decision which signal goes where is made during the design of the application with the WEB-PLC Editor.

END of Document