21, rue d'Artois, F-75008 PARIS
http : //www.cigre.org

B5_105

CIGRE 2010

Future developments in protection, control and monitoring from a manufacturer perspective

N. SCHUSTER , Siemens AG Germany

H-J. HERRMANN Siemens AG Germany

T. JACHMANN Siemens AG Germany

SUMMARY

The future of protection, control and monitoring is controlled by external influences, such as changes in the infrastructure of power systems, developments in the area of decentralized energy resources (DER), high-voltage direct current (HVDC), the process bus with electronics in close proximity to the switchgear and/or super conducting short circuit current limiters. All of these are promoted by the manufacturers and require additional protection and monitoring functions as well as new conceptional solutions. Global manufacturers are faced with a heterogeneous environment, which equally demands both decentralized as well as centralized solutions for the utility network.

On a worldwide scale, manufacturers must respond to extremely diverse regulations, imposed by various governments. Standardization, which is actively supported by the manufacturers, must also be viewed in this context. World-wide standards such as e.g. IEC 61850 will be established in more products. Increased environmental demands have a direct influence on the hardware design of the devices. Additional functions must be provided by increased flexibility of the software design. In the context of standardization the devices and systems become increasingly similar in terms of functionality, thereby satisfying the customer expectation with regard to interoperability. The intelligent system with Human Machine Interface distinguishes the suppliers.

This paper addresses some aspects of developments which will upcoming in the near future in the field of protection, control and monitoring.

KEYWORDS

Energy system, renewable energy, protection, functional integration, communication, communication topologies, Cyber security, new intelligence via communication, engineering, engineering tools, holistic workflow

Norbert.Schuster@siemens.com

THE ELECTRIC-ENERGY-SYSTEM IN FLUX

The expected shortage of energy resources and the increasing environmental burden are a booster for a global change of thought in the field of energy politics. This changes of thought toward renewable energy resources and new modes of usage such as for example the electrically powered car (E-Car offensive of the automotive industry) has a deciding impact on the electrical-power-system. Electrical energy is developing into a deciding energy resource for the user.
Therefore a change is taking place in the naturally grown power system of the last decades, where energy production took place in close proximity to the user as well as according to user requirements, thereafter fed into the transmission network, and was then distributed. A structure of this kind is typical for Central Europe.
The intention to effect a change is shown by the SMART GRID Initiative [1], [2], which deals with the new challenges regarding the individual voltage levels. The electrical power system is developing into a network, comparable to the Internet. The main difference to the Internet is the transmission of electrical energy instead of information. This constitutes an entirely different quality, as the balance between production and use has to be maintained. An imbalance necessarily leads to reduction in the reliability of supply, which may result in local blackouts or supply shortages. Figure 1 of [1] visualises the changes in the electrical power system.

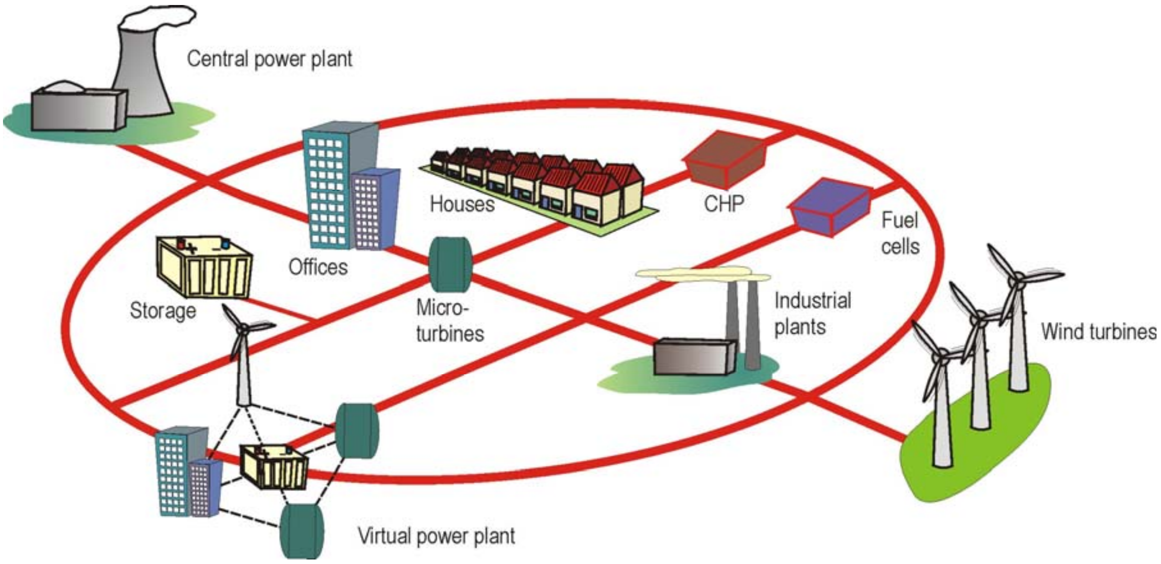


Figure 1: Illustration of changing in the electric energy system

Alongside conventional power plants, renewable energy sources play a deciding role. They can however only be used where they are available. Considering the resource wind, it is available with certain constancy only close to shores and in the ocean. In the case of Off-Shore Windparks, the energy has to be transported on-shore and to the consumer. This makes a network expansion with combined transmission via cable and overhead line necessary, and possibly leads to an increase in DC current transmission, which requires intelligent energy management. Driven by the deregulation and the trade with the commodity “electricity” results in the most diverse power flows, which the systems have to control. Furthermore Figure 1 clearly shows the future diversity of power producers. Producers may be found at all voltage levels, so that each network quasi assumes transmission tasks. In order for everything to work properly, intelligent control and monitoring solutions are essential. The protection and control technology makes a deciding contribution to this.

The future requirements regarding the protection and control technology and essential changes will be discussed, using three theses:

THESIS 1: INTELLIGENT AND MULTIFUNCTIONAL BAY UNITS ARE THE FUTURE

Microprocessor technology will also in future continue to be the defining technology at bay level. The necessities for real time processing as well as severe environmental requirements (e.g. EMC) will in future lead to embedded devices. Further development of technology toward higher processor performance (several 100 MHz), larger memory size and higher memory density, high resolution and fast anlog/digital converters (e.g. 24-bit resolution) as well as the utilisation of customer specific circuit technologies (e.g. FPGAs) are undisputed. A further motivation for the device technology is the rapidly developing communication technology (see theses 2).

Due to the current as well as the new structures, the electrical power system will become even more heterogeneous, so that the classic interfaces such as binary in-and outputs as well as measurement transducers will still be required especially for refurbishments. In the case of new plants, the advantages of technology, especially the consistent communication from the bay to the substation level will be implemented. The diversity of requests requires flexible hard-and software design from the device manufacturers, to optimally respond to the changing conditions.

With the introduction of the communication standard IEC61850, the object oriented approach for the selection of protection and control technology has begun. Depending on the requirements, the desired functionality is selected and assigned to the relevant device. This leads to a further functional integration. Figure 2 shows a possible functional scope. One can no longer refer to this as classic protection and control devices. Future devices will be referred to as IED (intelligent electronic device), a name introduced by IEC61850.

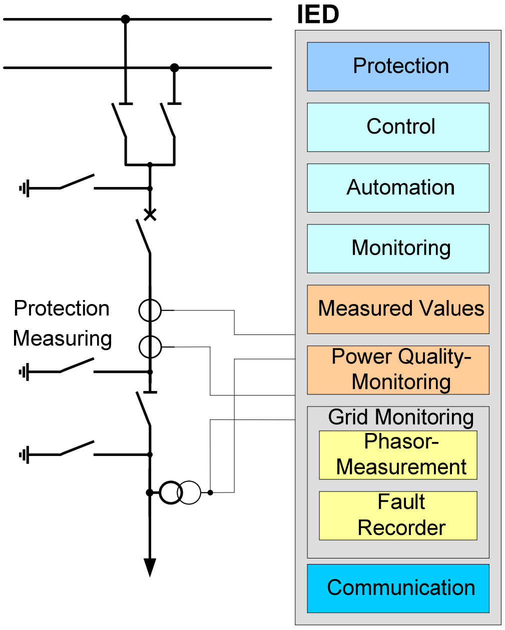


Figure 2: Overview functional integration

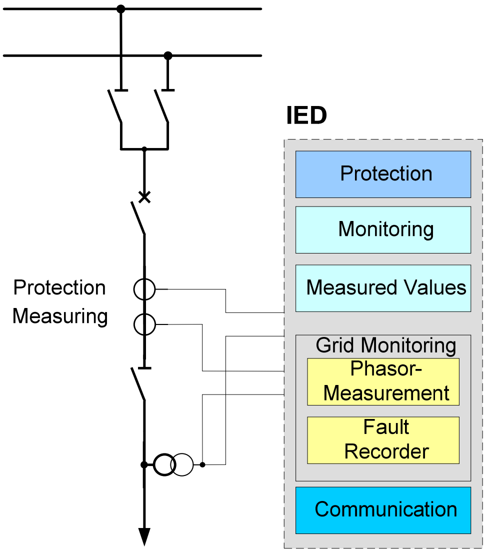


Figure 3: IED-Protection with functional integration

Functional Integration does however not mean that all the functions shown in Figure 2 have to always be contained in one device. Depending on the application and the requirements, functionalities can be combined in different ways. When selecting a device, the classic design criteria apply, such as the adherence to the n-1 principle. For protection applications in the transmission networks, a main protection 1 and a main protection 2 with different functional principals is required.

In practice, functional integration can mean that one IED protection contains additional functions, such as monitoring (monitoring of the plant, such as circuit breakers, line, GIS plant), highly accurate measurement (classic measured values and operational metering) and detection of phasors, as well as fault detection (see Figure 3). An efficient communication to a control system, between the devices or with a PDC (phasor data concentrator) will be state of the art. The highly accurate measurement guarantees the connection to the measurement transformers. In the case of process bus applications the sampled values (protection and measurement transformer signals) are made available via the Merging Unit (MU) over an Ethernet connection.

As a result of the design of functions and the possibility of using additional information, future IEDs will gain in intelligence (intelligence definition: "ability to understand, to abstract, to solve a problem, to apply knowledge ..."). Especially the communication with other devices offers an increase in information, which can be used to make a decision. When viewing Figure 1, it becomes obvious that the changed network requires an intelligent supervision and control. In the case of abnormal operation conditions, correct decisions have to be made. As a result of the changes in the network (e.g. diverse producers at all voltage levels, increase in power electronic control) current protection concepts have to be re-thought. Intelligent solutions are also sought for here. Figure 4 shows an example of this by using electronic fault current limiters (EFCL.) [3]. In the case of a short- circuit, these interrupt the current flow in a few milliseconds. The IED feeder is able to capture the "transient" fault current and to assess it. Depending on the fault situation it trips the switch (e.g. switch-disconnector or circuit breaker if available) in the corresponding feeder, and gives the release for the auto-reclosure. To keep the duration of the interruption as short as possible, fast communication is essential. In the example, the protection closest to the fault trips the switch-disconnector, and gives the release for auto-reclosure. State of the art devices must now not only monitor the transient measured values to ensure selectivity, but must also facilitate communication between the devices. Comparable solutions are being developed in the scope of Smart Grid, which is "a new form of intelligence".

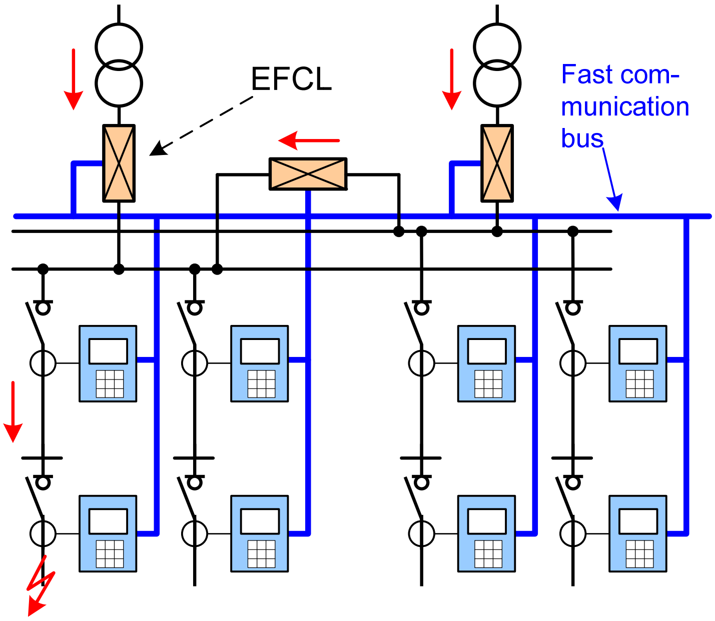


Figure 4: New protection concept based on fast communication

THESIS 2: FLEXIBILE COMMUNICATATION IS THE KEY FEATURE OF FUTURE IEDs

In future almost all devices will provide fast Ethernet communication interfaces. This also applies to less expensive devices, which are used in the distribution network. The previous serial communication to a Master unit is replaced by IP-based communication so that in a few years the serial method will only be relevant for maintenance/repair/refurbishment of devices. In an IP – infrastructure, the device acts as server that transfers its data to one or more clients. Via fast Ethernet interfaces a number of protocols and services can be transferred in parallel. In this manner, the server executes various tasks in the network with regard to its functionality as data provider for superceding systems. It can autonomously execute protection and monitoring functions and then provide the results to various superceding systems.

Benefits of the advantages of IEC 61850

IEC 61850 is more than a substation control protocol. It comprehensively defines functions, data and the communication systems for communication in networks of the power supply industry. Edition 2 extends the influence of the standard to further branches of the power supply industry, so that a consistently homogenous communication and technical data description of objects is available. Where the standard is at present still mostly being used as a classic substation control protocol, the new processes will in future be used at the communication and engineering level.

The dynamic reporting will establish itself in communication between Client and Server. Using a configuration file (ICD or SCD – file) or online, by establishing a connection to the server, the client is able to read all data points, which the server can potentially provide. The Client selects the information from the Server that he wants to subscribe to. The extent of this data can be altered during the lifecycle of the system, without re-configuring the Server. In this way the Client can read specific monitoring data, alarms or measured values of a Server for a certain period of time. Where it is today still customary to establish and transmit data records via fixed communication links, this will in future be replaced by dynamic processes. This facilitates a clearly increased flexibility during operation, as only immediately required data is read. Setting values of functions can also be changed via the protocol. The switching of fixed parameter settings is no longer necessary, if a threshold in the device can simply be changed during operation. With superceding systems, setting values can be checked and adapted to the condition in the Smart Grid.

With the GOOSE – Message the IEC 61850 defines the interoperable communication between Servers in the network. In this way wiring between devices can be replaced with communication links. However not only binary values can be exchanged. Measured values can also be transmitted. GOOSE – Messages are also exchanged between substations. New protection procedures (see Figure 4), which will require peer to peer communication will prevail. With Edition 2 of IEC 61850 a possibility will be created, using a Substation Exchange Description (SED – File), to describe this exchanged data interoperably. The GOOSE – Message will replace proprietary point to point connections for signal comparison or directional comparison, and facilitates the data exchange between devices of different manufacturers, including between substations.

Developments in Network technology

Network components with a very high availability are a prerequisite for IP based protocols both within a substation and outside the substation. Today different forms of ring or star shaped network topologies and well as various methods to achieve redundancy are applied. These methods lack interoperability and a short interruption in the range between 30 ms – 2 s is possible in the event of failure of a component. For critical applications such as the transfer of trip commands via GOOSE or the transfer of sampled measured values according to IEC 61850 9-2 for process bus applications these interruption intervals are not acceptable. In the IEC 62439 a High availability Seamless Redundancy Protocol (HSR) is described. It allows for interruption free switching in the network with ring or star configuration. Pilot projects will be presented by manufacturers at Cigre 2010. This technology will become established as standard for substation networks and process bus applications.

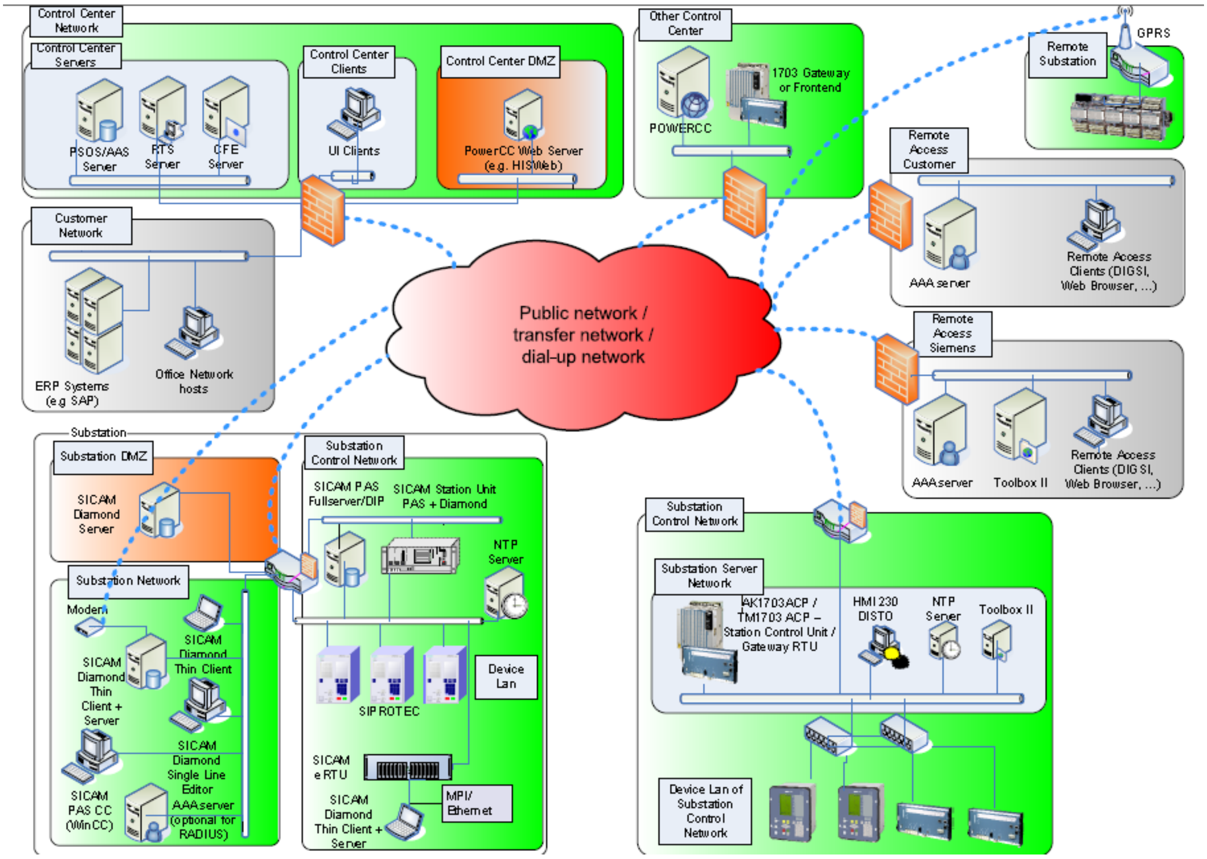
Furthermore there is a trend to higher bandwidths. At present station networks are operated at 100 MBit/s. The trend is towards 1 GBit/s, if the applications such as e.g. process bus require this. Cost effective components for this are already available in the market place so that 1 GBit/s technology will become available in the bay devices.

Cyber Security as Basis for secure operation of Networks

Because of the application of network technology the security within the network becomes a critical task. Security against internal threats and security against external attacks must be considered. Also in private networks it is possible that as a result of an accidental mal-operation the functioning of the network is placed at risk. The BDEW – Whitepaper [4] and Nerc – CIP [5] address these topics. With

IEC 62351 a standard is made available that describes methods for the end to end encryption as well as authentication between participants on the network in substation automation systems. Parts of these standards will be implemented by the manufacturers in their devices and substation automation protocols will be extended with security features.

Figure 5 shows a energy automation system with secure access to the devices in the substation. For remote access the user must be authenticated at the gateway as well as at the device. This Client Server Authentication ensures that only authorized persons or clients have access to specific services in the devices. Remote access operates then via encrypted connections. The operators and manufacturers must focus on the security of the networks as the Smart Grid will be of strategic importance. The degree to which encryption will also be applied to fast services e.g. GOOSE or SMV (sampled measured values) depends on the degradation of performance as a result of these procedures or the developments of special encryption hardware. One solution would be to provide the time critical services on segregated network segments on bay level and dedicated communication links.



Control Center Network
Control Center Servers
PSOS/AAS Server
RTS Server
CFE Server
Control Center Clients
UI Clients
Control Center DMZ
PowerCC Web Server (e.g. HISWeb)
Other Control Center
POWERCC
1703 Gateway or Frontend
GPRS
Remote Substation
Remote Access Customer
AAA server
Remote Access Clients (DIGSI, Web Browser, ...)
Customer Network
ERP Systems (e.g SAP)
Office Network hosts
Public network / transfer network / dial-up network
Remote Access Siemens
AAAserver
Toolbox II
Remote Access Clients (DIGSI, Web Browser, ...)
Substation
Substation DMZ
SICAM Diamond Server
Substation Network
Modem
SICAM Diamond Thin Client
SICAM Diamond Thin Client + Server
SICAM Diamond Single Line Editor
SICAM PAS CC (WinCC)
AAAserver (optional for RADIUS)
Substation Control Network
SICAM PAS Fullserver/DIP
SICAM Station Unit PAS + Diamond
NTP Server
SIPROTEC
Device Lan
SICAM eRTU
SICAM Diamond Thin Client + Server
MPI/ Ethernet
Substation Control Network
Substation Server Network
AK1703ACP / TM1703 ACP – Station Control Unit / Gateway RTU
HMI 230 DISTO
NTP Server
Toolbox II
Device Lan of Substation Control Network

Figure 5: Secure operation in energy automation systems through network segmentation

Synchronism and matching real time in the network

Different methods are applied to obtain time synchronism. Local long wave real time receivers achieve an accuracy of 5-10 ms. Via GPS and the derived IRIG-B protocol accuracies of < 1 ms are achieved. The highly accurate impulse per second (PPS) from the GPS – system provides an accuracy of 1 µs. This technology is already applied today with the differential protection e.g. 7SD5 [6], when the channel delay times in the communication system are not constant. The µs accuracy is also required for synchro-phasors according to IEEE C37.118 and the process bus.

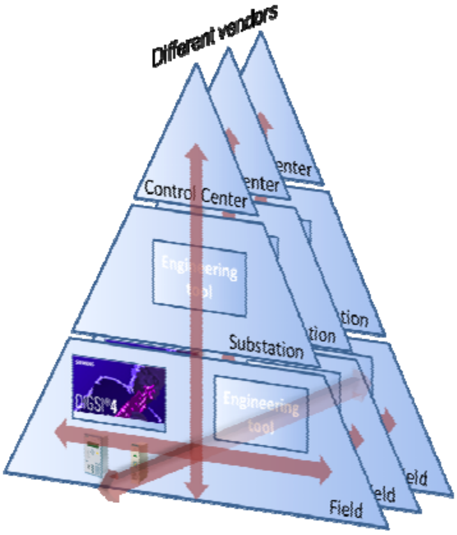
In future, the time synchronisation will be done via the Ethernet network. Within the IEC61850, SNTP (simple network time protocol) is applied and can achieve an accuracy of less than 1ms. Redundant clocks can be can easily be applied in the network and the channel delay times of the telegrams between Client and Server can be measured and compensated in the devices. Devices with an Ethernet interface can therefore be easily provided with time synchronisation so that their event records and measured values may be evaluated with millisecond resolution.

With IEEE 1588 Edition 2 procedures are described, which can achieve < 1 µs accuracy within a local Ethernet network. This accuracy must be supported by measures taken in the hardware of the Ethernet interfaces e.g. in switches and other network devices [7]. Activities to make IEEE 1588 with highly accurate time synchronisation available are in preparation at the manufacturers. Suitable switches and time receivers are already available. In future, time synchronisation via Ethernet will replace the classic methods via dedicated interfaces and all equipment works with the same time.

THESIS 3: HOLISTIC WORKFLOW WITH AN UNIVERSAL ENGINEERING

Looking at global trends, the following is obvious: The systems in energy transmission and distribution are getting larger and increasingly connected. To recognize the trend even better one just need to look back some years to find protection and communication schemes neatly separated. Not only are both sides gaining flexibility and complexity but new standards like IEC 61850 Edition 2 are fusing this world together.

More and more devices are connected via intelligent communication protocols. The standard IEC 61850 describes not only the communication between devices but also heavily influences - especially with the upcoming edition 2 - the structure of each protection device. Previously each device acted as a black box and was communicating through defined protocols with the outside world. But those devices are not that "black" anymore, since the IEC 61850 Edition 2 also proclamates for the unification of protection application interfaces and therefore moves the boundary from the communication interface right into the heart of the devices.



Also make improvements in speed and predictability of communication channels based on redundant network-topologies possible what was unthinkable in the past: Passing vital real-time information (like trip and blocking signals) not via cable but via logical communication busses.

IEC 61850 is bringing the different levels closer together. Connecting device information not only to the substation automation, but up to the control centre is an increasingly common requirement. This increases not only the reach but also the amount of transmitted data tremendously.

Mapping these changes to the engineering systems brings up manifold and even contradictory requirements. Some customer statements:

- "Provide me with mechanisms that allow the quick and easy configuration of large sets of protection devices."
- "Give me the full flexibility of the IEC 61850 standard."
- "I only want to configure and commission one or just a few devices. Don't make me learn the language of IEC 61850."

Even those three very usual scenarios put an immense pressure on engineering workflows and tools. Engineering tools are the key lever in the future to cover the growing complexity of highly integrated and more complicated protection solutions.

Engineering tools must speak the "language" of the user

Since the common data engineers using those tools are not experts in IEC 61850 at present, they have to use engineering tools, with a language and view that is task and workflow oriented, without requiring knowledge of the standard. An example: In the past it was sufficient to provide an easy solution within one's device configuration to connect for example a binary input or measured value with the logic (CFC), display etc. In the future it must be just as simple to connect signals from other devices received via GOOSE - and that even for data engineers who see GOOSE as a tool similar to a screwdriver, which must be usable without having to read or understand the instruction manual first.

However on the other hand the number of IEC 61850 experts is constantly growing and they desire full flexibility and functionality of the standard at their fingertips. They also need to recognise in the engineering tools the wording used in the standard. Engineering tools of the future will have the challenging task to provide a productive answer to both groups.

For engineering tools data must be sacrosanct

The growing number of devices applied in solutions, implies an increase in engineering data that needs to be managed. Engineering tools must ensure that this data can be provided in the most efficient way and that once entered data can also be used wherever it is needed. If we look at the workflow of the user this means that engineering of a system need to have an open interface to enable reuse of already existing data from other systems. At the culmination of the engineering workflow the same flexibility is required, to provide the engineering data to other processes such as documentation, testing, asset management etc.

During the engineering process within the engineering tool the key factor is re-use to decrease effort and the risk of errors. This can be done e.g. by copy/paste, mass data handling/manipulation or the usage of templates, but only a combination of all of them provides the highest efficiency in all scenarios:

- Reuse existing expertise by starting with "almost-done"-template solutions that reduces the effort to adopt these to the specific needs, e.g. selecting templates based on the required protection scheme.
- Copy adapted parts to all places where they are needed, e.g. for deriving the main 2 protection from the main 1 protection settings or protecting multiple lines.
- Mass-data handling/manipulation is needed for changes to the data, e.g. if protection settings of all main 1 protection devices for all lines need to be changed.

Engineering systems must be a lot more intelligent in the future to cover the growing requirements for future energy automation systems. The need to move from data input tools to data management and validation tools to ensure the stability of the systems is essential.

BIBLIOGRAPHY

[1] www.smartgrids.eu, see folder documents of interests.

[2] Electric Transmission and Distribution Program. Five year program plan (2008 – 2012) US Department of Energy, August 2006

[3] Kunde, K. and others: Integration of fast acting electronic fault current limiters (EFCL) in medium voltage system. CIRED 2003, Barcelona, 12-15 May 2003

[4] BDEW – Bundesverband für Energie und Wasserwirtschaft: White Paper – Requirements for Secure Control and Telecommunication Systems. Version 1, Berlin, 10 Juni 2008

[5] North American Electric Reliability Council (NERC): Critical Infrastructure Protection (CIP) Cyber Security Standards CIP–002–1 through CIP–009–1. June 1, 2006

[6] Siemens AG: Manual - Line Differential Protection with Distance Protection 7SD52/53. V4.6, Release date 11.2009

[7] Prof. Hans Weibel: Technology Update on IEEE 1588 - The Second Edition of the High Precision Clock Synchronization Protocol. 2009, Zurich University of Applied Sciences Institute of Embedded Systems (InES)