6

Power System and Substation Automation

Edward Chikuni
Cape Peninsula University of Technology
South Africa

1. Introduction

Automation is "the application of machines to tasks once performed by human beings, or increasingly, to tasks that would otherwise be impossible", Encyclopaedia Britannica [1]. The term automation itself was coined in the 1940s at the Ford Motor Company. The idea of automating processes and systems started many years earlier than this as part of the agricultural and industrial revolutions of the late 18th and early 19th centuries. There is little disputing that England was a major contributor to the Industrial Revolution and indeed was the birth place of some prominent inventors, for example. in the area of textiles:

- James Hargreaves: Spinning Jenny
- Sir Richard Arkwright: Mechanical Spinning Machine
- Edmund Cartwright: Power Loom

Cartwright's power loom was powered by a steam engine. At these early stages we see the symbiotic relationships between automation, energy and power. The early forms of automation can only largely be described as mechanisation, but the emergence of electrical power systems in the late 19th century and the entry of electronic valves in the early 20th century heralded the humble beginnings of modern automation. With electronic valves came computers. One of the earliest computers was the ENIAC (Electronic Numerical Integrator and Automatic Computer) built over two years between 1943 and 1946. It occupied an area of 1000 square feet (about 93 square metres), had 18000 valves and consumed 230 kW [2].

Before the deployment of computers in industrial automation, relays and RELAY LOGIC, the wiring of circuits with relays to achieve automation tasks, was in common use. Today, however, relay logic is far less used than computer-based, PROGRAMMABLE LOGIC, which has followed the invention of the transistor, integrated circuits and microprocessors.

2. Automation in the automobile (car / truck) industry

The motor assembly line pioneered by Ransom Olds and Henry Ford, the maturity of computer technology and the structured nature of the car assembly process led early entrepreneurs in the motor industry to view automation as key to business success. Indeed there was all to be gained in automation and today automation is viewed to have, among many other attributes, the following [3]:

a. relieves humans from monotony and drudgery
b. relieves humans from arduous and dangerous tasks
c. increases productivity and speeds up work rates
d. improves product quality
e. reduces costs and prices
f. increases energy and material savings
g. improves safety
h. provides better data capture and product tracking.

The automotive industry was very competitive right from the early days and automation soon came to be seen as key to commercial success. General Motors embraced it and so did many other auto manufacturing corporations in the US, Europe and Japan. The computer system used was designed for the usually harsh industrial environments. Programmable Logic Controllers (PLC) as such computers are known typically to have many inputs and outputs; the inputs receiving sensor signals, the outputs being for displaying information or driving actuators (Figure 1).

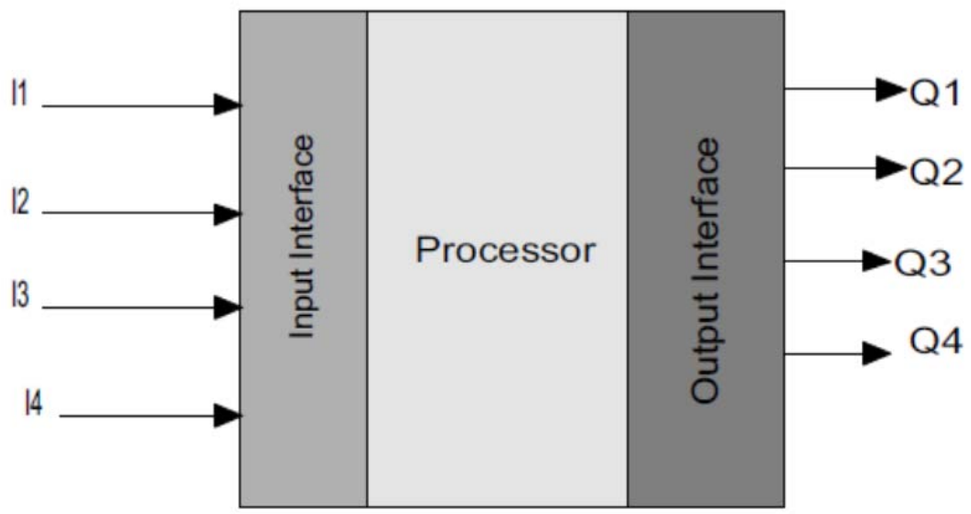


Fig. 1.

The need for standardization was realized early, especially when many PLCs are required to achieve the automation task. The standards generating body IEEE has been a driving force in computer communication standards over the years. One of its standards, the token ring 802.4 was implemented in modified form by General Motors in its Manufacturing Automation Protocol (MAP).

3. Power system automation

The early power plants had a modest number of sensor and action variables, of the order of several hundreds. Modern large power stations have in excess of hundreds of thousands, even tens of million variables [3]. It is therefore easy to see that automation took root in

power and generating stations earlier than in transmission and distribution. One of the useful applications of automation is in the railway industry where remote control of power is often vital. This manifests itself in systems to control and manage power supplies to electric locomotives. The deprivation of power to any locomotives in a section could seriously disrupt schedules, inconvenience customers and in the end have serious adverse financial implications. Consider Figure 2

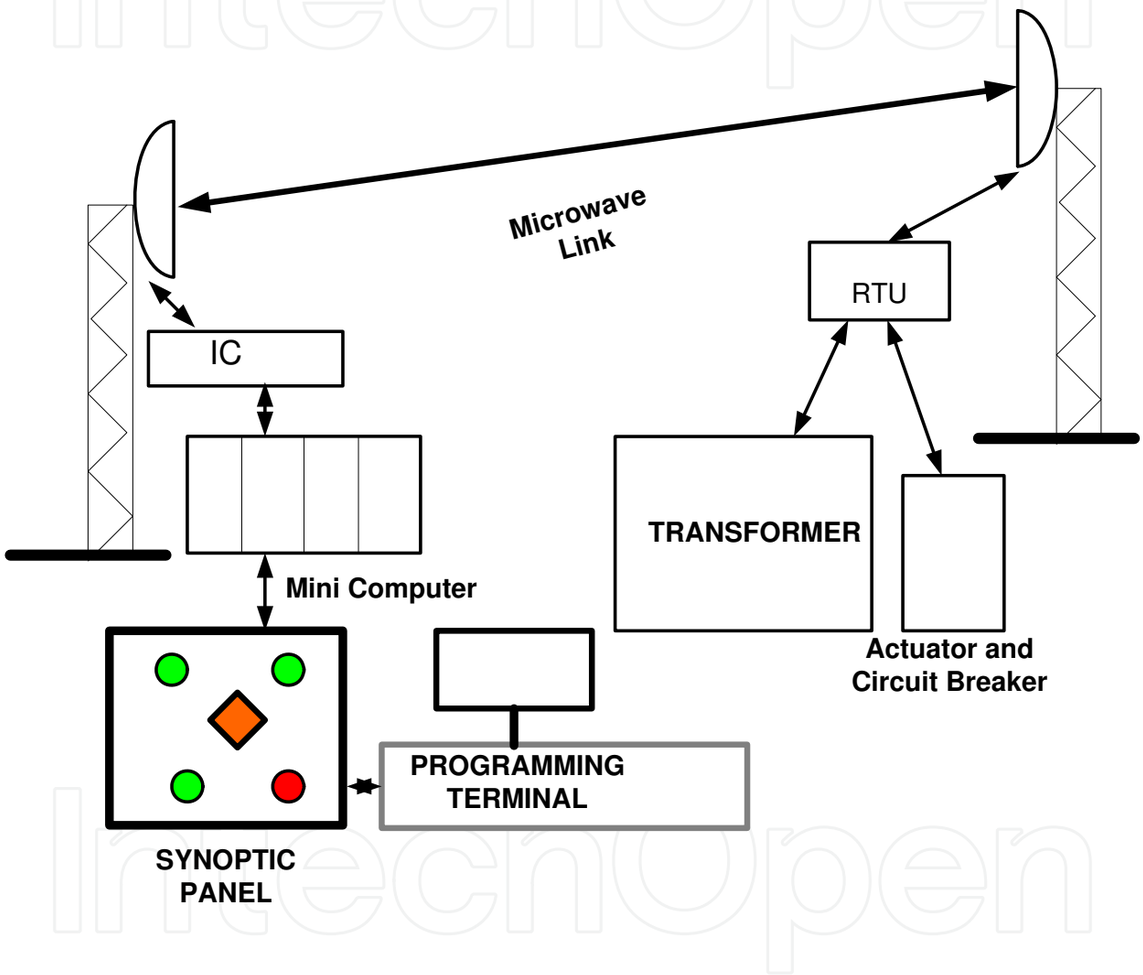


Fig. 2.

In earlier systems, the "mini computer" would have been sourced from specialised computer companies such as IBM, Perkin Elmer, Digital Equipment Corporation. The operating systems would have belonged to the same equipment provider (e.g., VMS VAX, in the case of Digital Equipment Corporation). The microwave link would have been part of the infrastructure costs for the project. The synoptic panel, allowed visual representation of the system states to the operator (and also some capabilities for remote switching). For Figure 1, the operator at the control centre is able switch a circuit breaker ON or OFF

through the microwave link. Interface cards (IC) provide the necessary I/O capabilities. The remote terminal unit (RTU) is able to send a switching signal to the circuit breaker through a suitably designed actuator. The circuit breaker is also able to send its position (ON or OFF) through the RTU and the same microwave link to the operator's panel. The older type of hardwired panel is largely being replaced by electronic displays and the controller is able to receive and view system status through touch panel capabilities or through networked computers in the control room.

The proprietary nature of the old "legacy systems meant that embarking on the path to automation was not a trivial matter. The cost of ownership, (infrastructure, hardware and software costs) was very high. Also very high were the costs of maintaining and upgrading this hardware and software. The cost of software licences was often prohibitive. On the other hand cyber threats and virus attacks were unheard of. The systems themselves were broadly secure, but not necessarily reliable. Communication link (microwave failure) meant that there was at the time, as there is even in this generation, a need for "manual back-ups". This usually meant sending a technician to do manual switching operations.

4. Modern grid and substation automation

Power system automation happens in segments of the power system (Northcote-Green, Wilson) [4] which can serve different functions. One segment is bulk transmission of power which traditionally was handled by the power producer, but increasingly (in de-regulated environments), is handled by an independent transmission system operator (TSO). Bulk transmission is usually associated with outdoor switchyards and high voltage operating voltage levels (in excess of 132 kV). Bulk transmission substations play a critical role in energy trading and power exchanges. Wholesale electricity is sold through the transmission system to distributors. Figure 3 shows a portion of the 400 kV outdoor substation at AUAS near Windhoek, the capital of Namibia. Namibia is a net importer of electrical power most of it from neighbouring South Africa and this substation is of vital importance. The substation with which it connects in South Africa is over 800 km away at Aries near Kenhardt. Figure 4 shows the Namibian electrical power transmission network. The complex interconnections between equipment, such as transformers, reactors, lines and bus-bars, is such that manual operation is not a practical proposition. In the case of the AUAS substation, effective control is in the hands of Namibia Power Corporation's (Nampower) headquarter-based National Control Centre in Windhoek.

The other segment of automation is at distribution level. Large distributors are typically municipal undertakings or in countries in which electrical power is de-regulated, the so called "DISCOS". Automation has existed at the distribution level for many years, but has been restricted to situations involving either large numbers of customers or critical loads. As a result of this the quality of service given has been very good, while the rural consumers have been at a disadvantage. For power distributors, automating rural supplies was not cost-effective due to the dispersed nature of the lines and loads (Alsthom Network Protection and Application Guide) [5]. Technology changes in recent years, national power quality directives as well as increased consciousness by consumers themselves has led to radical changes in our Power System Control infrastructure and ways of operation with serious implications for those organisations that lag behind [NPAG].

Fig. 3. A group of Polytechnic of Namibia students visit the AUAS 400 kV substation

4.1 Distribution systems automation

From experience, faults at transmission levels are less frequent than at distribution levels [6]. At the same time distribution networks are not only complex, but the consequences of failure are quite severe. For this reason investment in distribution automation will increase. The elements that characterise distribution automation systems are given the definition by the IEEE. According to the IEEE, a Distribution Automation System (DAS) is "a system that enables an electric utility to remotely monitor, coordinate and operate distribution components, in a real-time mode from remote locations [7]". In this chapter we shall deal in more detail with the components involved and how they are coordinated within a DAS. In countries or situations where there are large networks, the network (primary distribution) itself is subdivided into more segments, namely, one for large consumers (no transformation provided) and for the rest at a lower HV voltage (secondary distribution) (Figure 6).

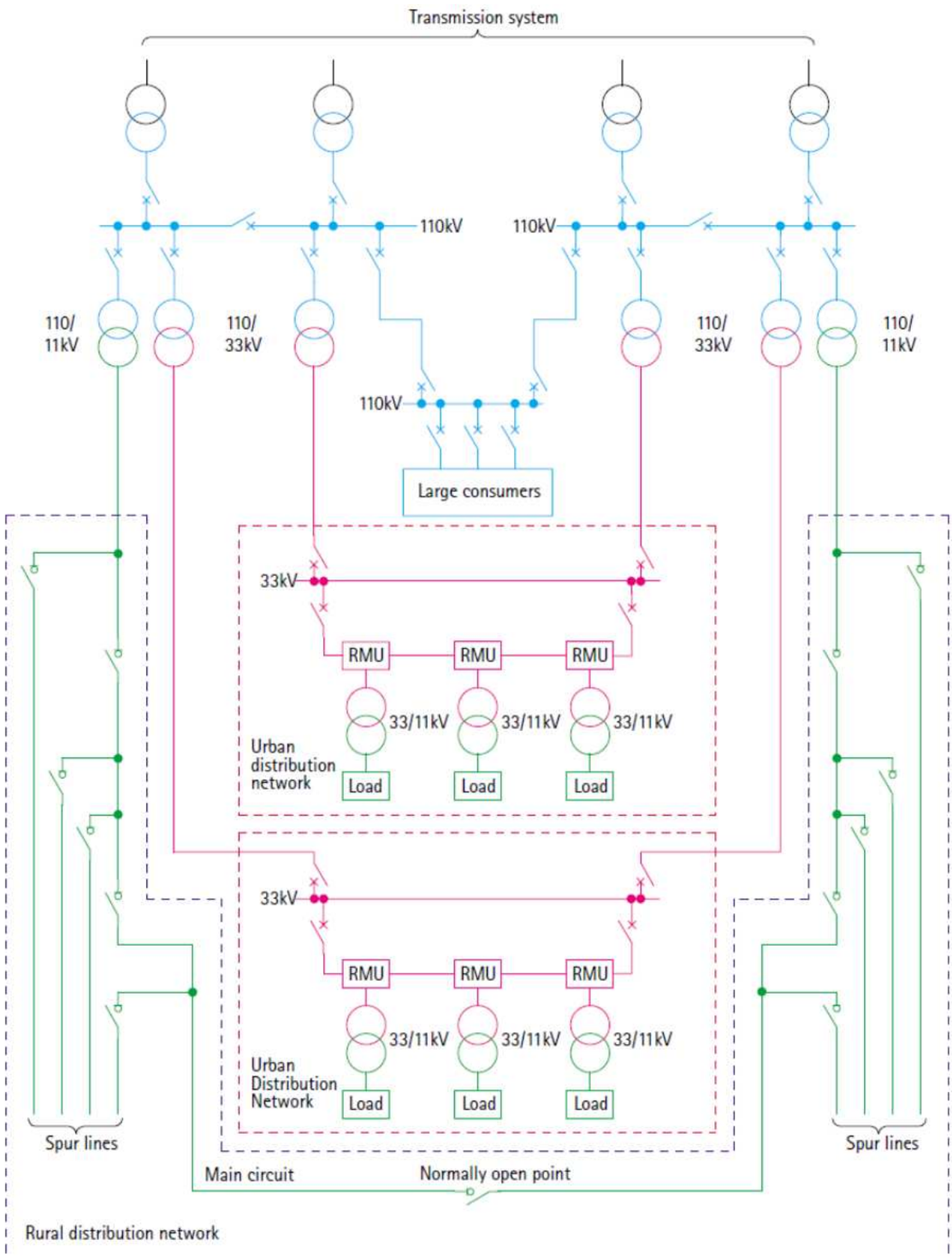


Fig. 4. (courtesy AREVA, NPAG)

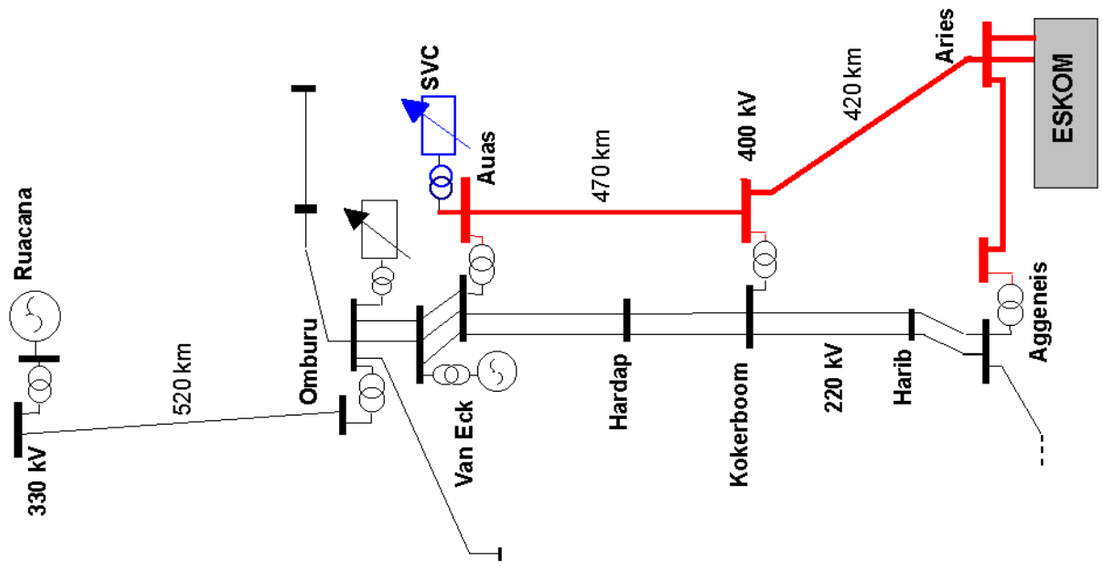


Fig. 5. (courtesy, Namibian Power Corporation)

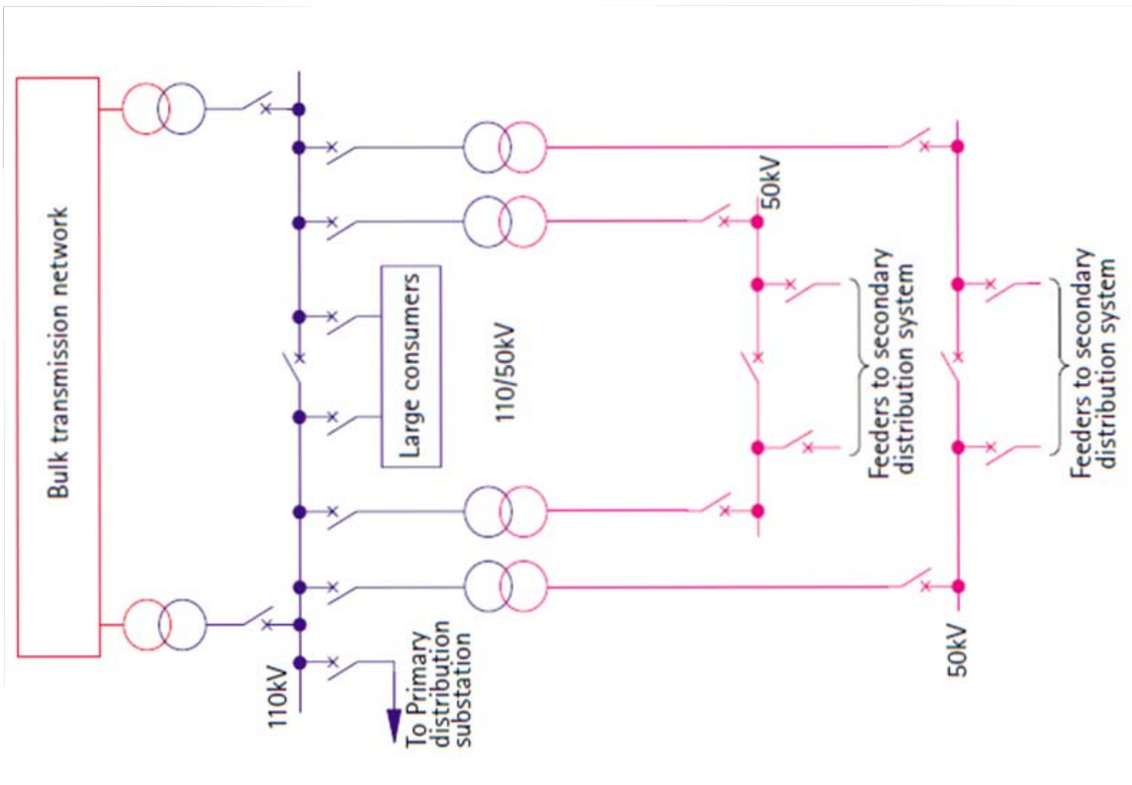


Fig. 6. (courtesy AREVA, NPAG)

5. Power system automation components

Power system automation components may be classified according to their function:

- Sensors
- Interface Equipment
- Controllers
- Actuators

Thus we see that Figure 1 is still a good representation of what is needed to effect automation, whether it is for EHV transmission, sub-transmission or distribution. Figure 7 depicts the control philosophy of a power system automation scheme.

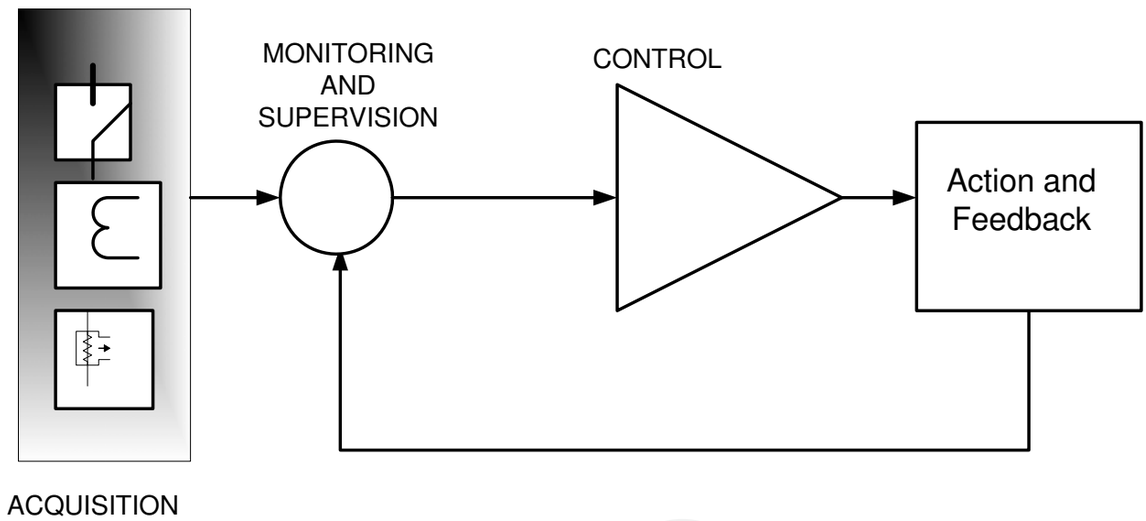


Fig. 7.

5.1 Overview of power system components

5.1.1 Sensors

5.1.1.1 Current and voltage transformers

Individually or in combination current and voltage transformers (also called instrument transformers) are used in protective schemes such as overcurrent, distance and carrier protection. Also in combination current and voltage transformers are also used for power measurements. In general custom specified voltage and current transformers are used for power metering, because of the increased accuracy requirements. Figure 8 shows instrument transformers in one of the substation areas (called bays).

Fig. 8.

5.1.1.2 Other sensors

For reliable electrical power system performance the states, stress conditions and the environmental conditions associated with the components have to be monitored. A very costly component in a substation is a transformer. For a transformer, monitoring is done, for example, for pressure inside the tank, winding temperature and oil level. For circuit breakers, sensing signals may need to be obtained from it such as gas pressure and number of operations.

5.1.2 Switches, isolators, circuit breakers

A most important function of a substation is the enabling of circuit configuration changes occasioned by, for example, planned maintenance, faults feeders or other electrical equipment. This function is of course in addition to the other important function of circuit protection which may also necessitate configuration changes. Modern switches and circuit breakers will have contacts or sensors to indicate their state or position. Figure 9 shows the ABB HH circuit breaker mechanism. The plant required to achieve the desired operation is usually quite elaborate and includes controls and protection to ensure that it operates reliably.

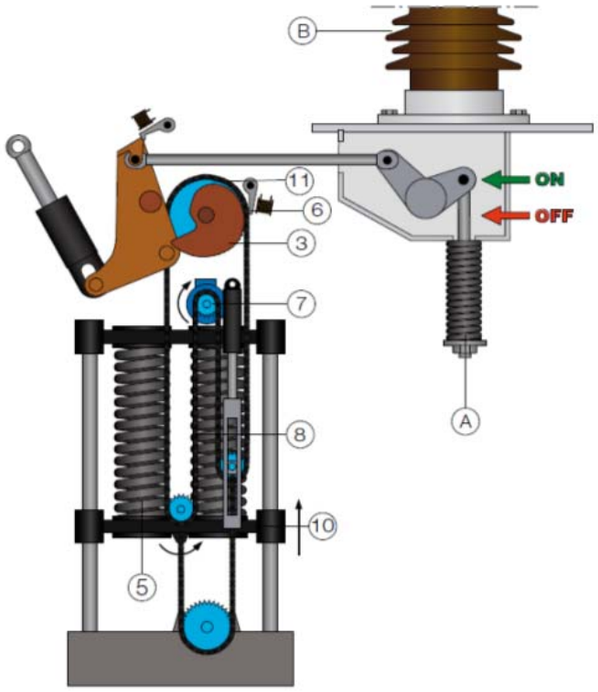


Fig. 9. Portion of HH ABB circuit breaker mechanism

6. IEC 61850 substation automation: Origin and philosophy

The International Electrotechnical Commission is one of the most recognisable standard generating bodies for the electrical power industry. Its standard the IEC 61850 "Communication Networks and Systems in Substations" is a global standard governing communications in substations. The scope of the standards is very broad and its ramifications very profound. So profound in fact that it is hard to imagine any new modern substation that would not at least incorporate parts of this standard. In addition, the standard is almost sure to be adopted albeit in customised / modified form in Generation, Distributed Energy Resources (DER) and in manufacturing. The standard has its origins in the Utility Communications Architecture (UCA), a 1988 initiative by the Electrical Power Research Institute (EPRI) and IEEE with the initial aim of achieving inter-operability between control centres and between substations and control centres. In the end it was found to be more prudent to join efforts with similar work being done by the Working Group 10 of Number 57 (TC57). The emerged document IEC 61850 used work already done by the UCA as a basis for further development.

6.1 IEC 61850 substation architecture

6.1.1 Substation bays

In an IEC 61850 compliant substation, equipment is organized into areas or zones called bays. In these areas we find switching devices (e.g., isolators and circuit breakers) that connect, for example, lines or transformers to bus-bars.

Examples of the bays would be:

- Incomer bay
- Bus-coupler bay
- Transformer bay

Figure 8 above, for example, could depict a transformer bay.

6.1.2 Merging units

Merging units are signal conditioners and processors. For example, they accept, merge and synchronise sampled current and voltage signals (all three phases' quantities of the CT/VT) from current and voltage transformers (conventional and non-conventional) and then transfer them to intelligent electronic devices (see IEDs, in the next section). So called electronic VTs and CTs are being manufactured by some companies which use new ways of sensing with the overall size being reduced. With electronic sensing, the sensing and merging are combined. Figure 10 gives an overview of the functions and associated inputs of a merging unit.

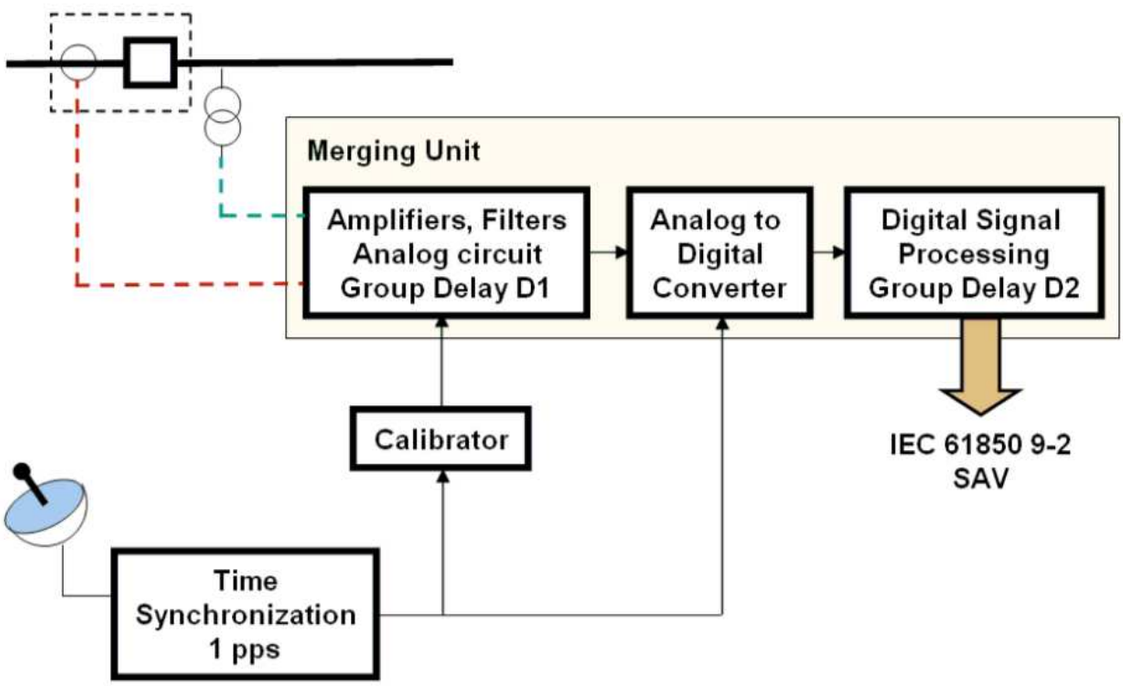
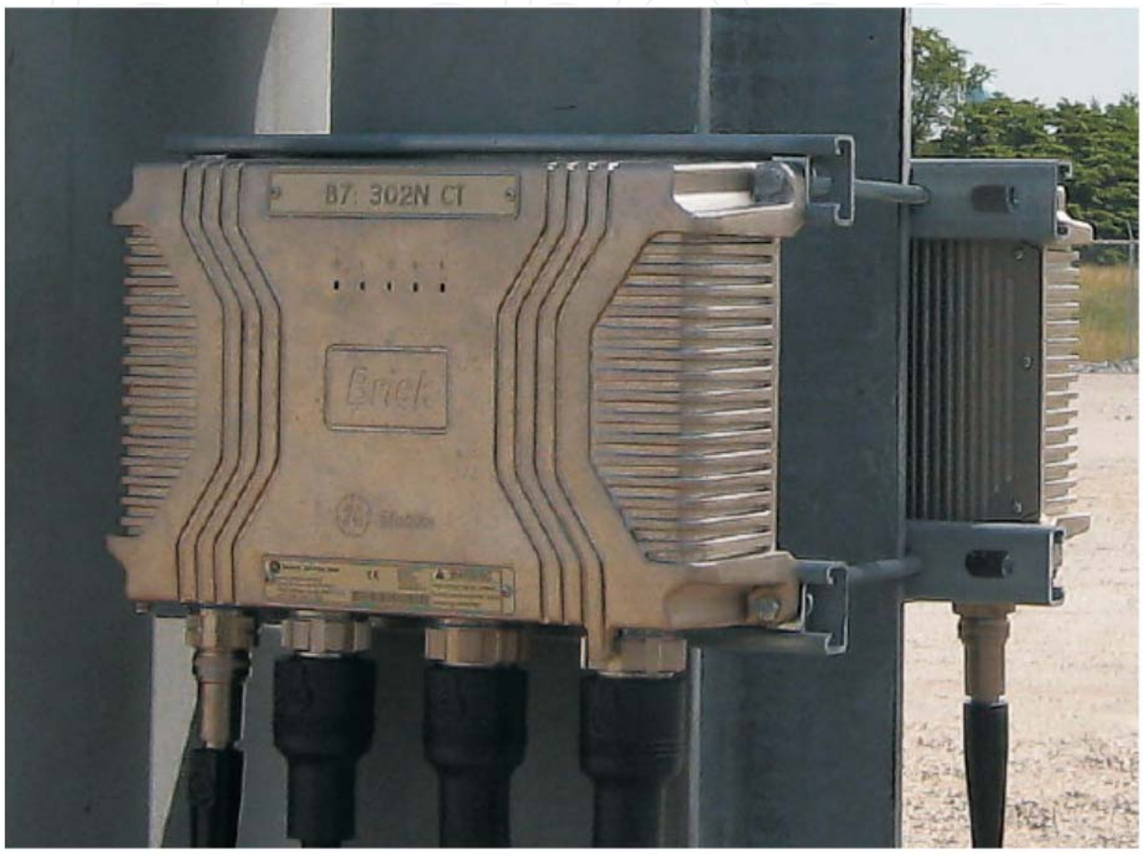


Fig. 10. (Jansen & Apostolov)

As technology progresses it is believed that there will be a move away from copper connections from field devices to the substation control room in favour of fibre. Figure 11 shows a merging unit (Brick) by vendor GE.



6.1.3 Intelligent Electronic Devices (IEDs)

An IED is any substation device which has a communications port to electronically transfer analog, status or control data via a proprietary or standard transmission format (BPL Global IEC 61850 Guide) [8]. Examples of IEDs are:

- Modern IEC 61850 protection relays (distance, over-current, etc.)
- Equipment-specific IED (e.g., for transformer bay protection and control, with tripping logic, disturbance monitoring, voltage, current, real and reactive power, energy, frequency, etc.).
- Bay controllers

Figure 11 shows some IEDs from various vendors with multiple functionality.

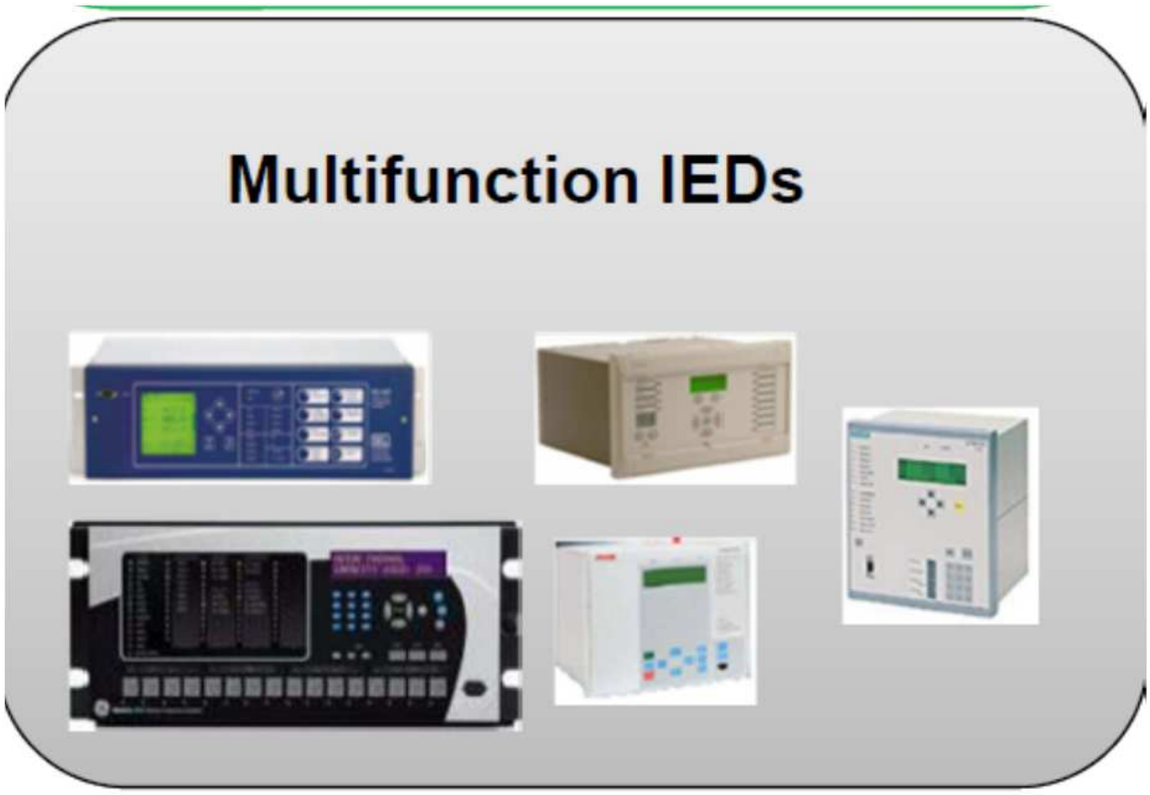


Fig. 11.

In reality today's IEDs have "mutated" to the form of programmable logical controllers (PLCs) of another kind with multiple capabilities.

6.1.4 Device/system integration: Substation functional hierarchy

An IEC 61850-designed substation has the following hierarchical zones:

- Process
- Bay
- Station

Diagrammatically this is illustrated in Figure 12 (Jansen & Apostolov) [9]. A complete representation that includes aspects, such as links to remote control centres and GIS, is given in Figure 13.

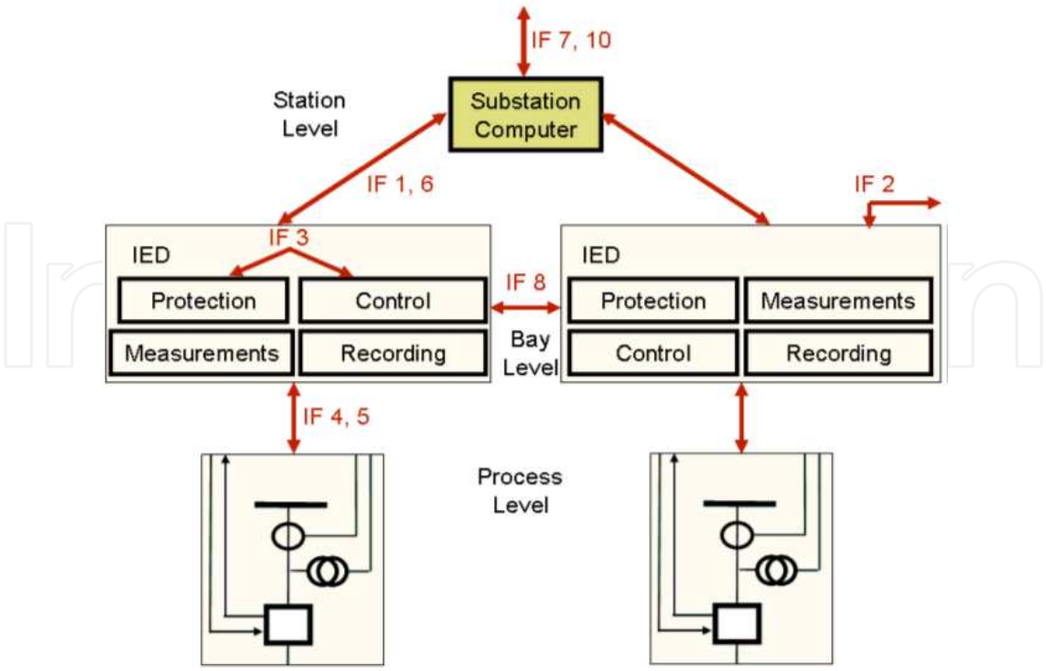


Fig. 12.

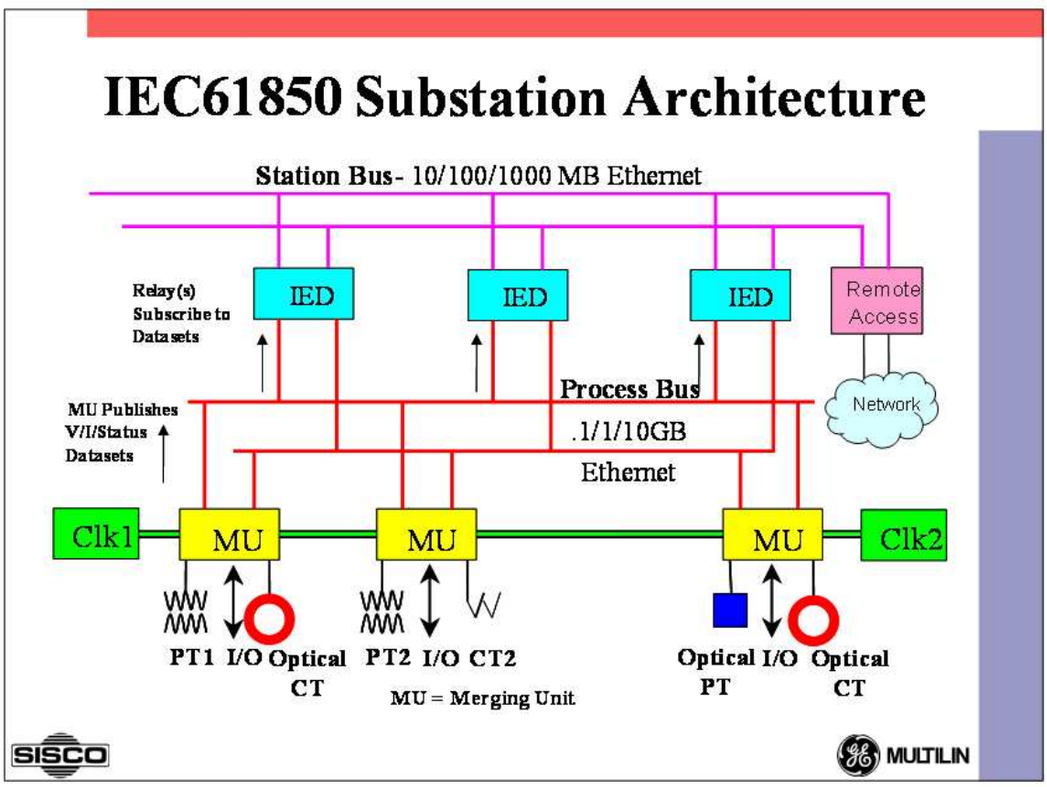
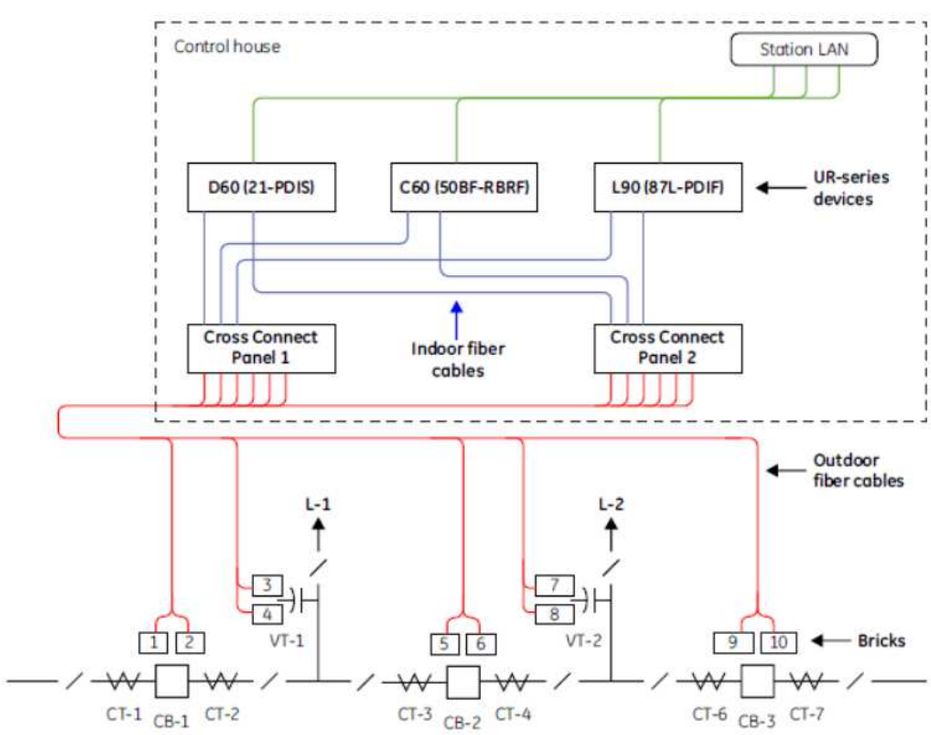


Fig. 13. (courtesy SISCO & GE)



[O1]

Fig. 14. Fibre-based

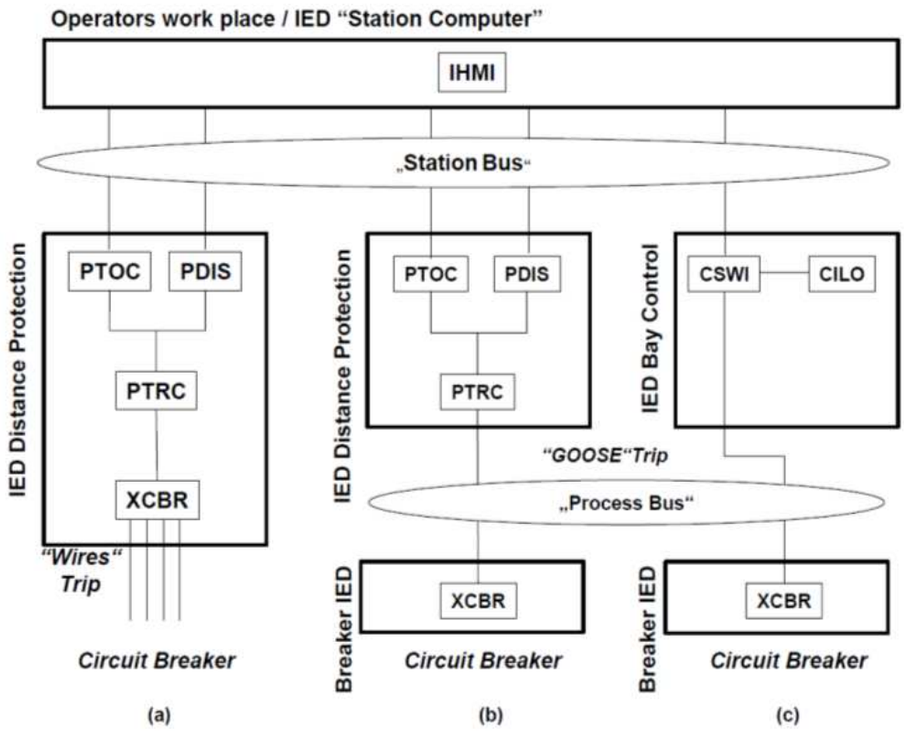


Fig. 15.

STRUCTURE OF THE IEC 61850 STANDARD

Part #	*Title*
1	Introduction and Overview
2	Glossary of terms
3	General Requirements
4	System and Project Management
5	Communication Requirements for Functions and Device Models
6	Configuration Description Language for Communication in Electrical Substations Related to IEDs
7	Basic Communication Structure for Substation and Feeder Equipment
7.1	- Principles and Models
7.2	- Abstract Communication Service Interface (ACSI)
7.3	- Common Data Classes (CDC)
7.4	- Compatible logical node classes and data classes
8	Specific Communication Service Mapping (SCSM)
8.1	- Mappings to MMS(ISO/IEC 9506 – Part 1 and Part 2) and to ISO/IEC 8802-3
9	Specific Communication Service Mapping (SCSM)
9.1	- Sampled Values over Serial Unidirectional Multidrop Point-to-Point Link
9.2	- Sampled Values over ISO/IEC 8802-3
10	Conformance Testing

7. Substation communications and protocols

With the IEC 61850 technology and with all the components and systems described in previous sections functioning normally, we have in fact a virtual substation. The remote terminal units (RTU) increasingly with IED functionality, pass on analog and digital data through either copper or fibre to IEDs in the substation control room in the form of relays or bay controllers. The process of transferring data and communicating it to various devices has been greatly simplified with the aid of the standard. The data arriving at the IEDs comes already formatted / standardized. The situation is similar to the "plug and play" philosophy applied to computer peripherals of today.

7.1 Virtualisation

With the IEC 61850 a real substation is transformed into a virtual substation, i.e., real devices transformed into objects with unique standardized codes. In Figure 16, a real device, a transformer bay is transformed into a virtual, logical device with descriptive name, e.g., Relay1. Inside the device are logical nodes (LN) named strictly in accordance with the IEC standard. For example, a circuit breaker inside this logical device is given XCBR1 [10]. In turn the breaker has other objects associated with it, e.g., status (open / closed) and health. The

services associated with this data model are defined in the Abstract Communications System Interface (ACSI). The following ACSI functions are listed by Karlheinz Schwartz [11]:

- Logical Nodes are used as containers of any information (data objects) to be monitored
- Data objects are used to designate useful information to be monitored
- Retrieval (polling) of the values of data objects (GetDataObjectValues)
- Send events from a server device to a client (spontaneous reporting)
- Store historical values of data objects (logging)
- Exchange sampled values (current, voltages and vibration values)
- Exchange simple status information (GOOSE)
- Recording functions with COMTRADE files as output

7.2 Mapping

IEC 61850 is a communications standard, a main aim of which is interoperability. A good definition is:

"Interoperability is the ability of two or more IEDs (Intelligent Electronic Devices) from the same vendor, or different vendors to exchange information and uses that information for correct co-operation" [12]. Although ACSI models enable all IEDs to behave identically from a general network behaviour perspective, they still need to be made to work with practical networks in the power industry, (Baigent, Adamiak and Mackiewicz) [10]. This universal compatibility is achieved through mapping of the abstract services to universal, industry-recognised protocols. Presently the protocol most supported is the Manufacturing Message Specification (MMS). MMS was chosen because it has an established track record in industrial automation and can support the complex and service models of IEC 61850.

Table 1 gives an idea of the naming process:

IEC61850 TO MMS OBJECT MAPPING

IEC61850 Objects	MMS Object
SERVER class	Virtual Manufacturing Device (VMD)
LOGICAL DEVICE class	Domain
LOGICAL NODE class	Named Variable
DATA class	Named Variable
DATA-SET class	Named Variable List
SETTING-GROUP-CONTROL-BLOCK class	Named Variable
REPORT-CONTROL-BLOCK class	Named Variable
LOG class	Journal
LOG-CONTROL-BLOCK class	Named Variable
GOOSE-CONTROL-BLOCK class	Named Variable
GSSE-CONTROL-BLOCK class	Named Variable
CONTROL class	Named Variable
Files	Files

IEC61850 SERVICES MAPPING (PARTIAL)

IEC61850 Services	MMS Services
LogicalDeviceDirectory	GetNameList
GetAllDataValues	Read
GetDataValues	Read
SetDataValues	Write
GetDataDirectory	GetNameList
GetDataDefinition	GetVariableAccessAttributes
GetDataSetValues	Read
SetDataSetValues	Write
CreateDataSet	CreateNamedVariableList
DeleteDataSet	DeleteNamedVariableList
GetDataSetDirectory	GetNameList
Report (Buffered and Unbuffered)	InformationReport
GetBRCBValues/GetURCBValues	Read
SetBRCBValues/SetURCBValues	Write
GetLCBValues	Read
SetLCBValues	Write
QueryLogByTime	ReadJournal
QueryLogAfter	ReadJournal
GetLogStatusValues	GetJournalStatus
Select	Read/Write
SelectWithValue	Read/Write
Cancel	Write
Operate	Write
Command-Termination	Write

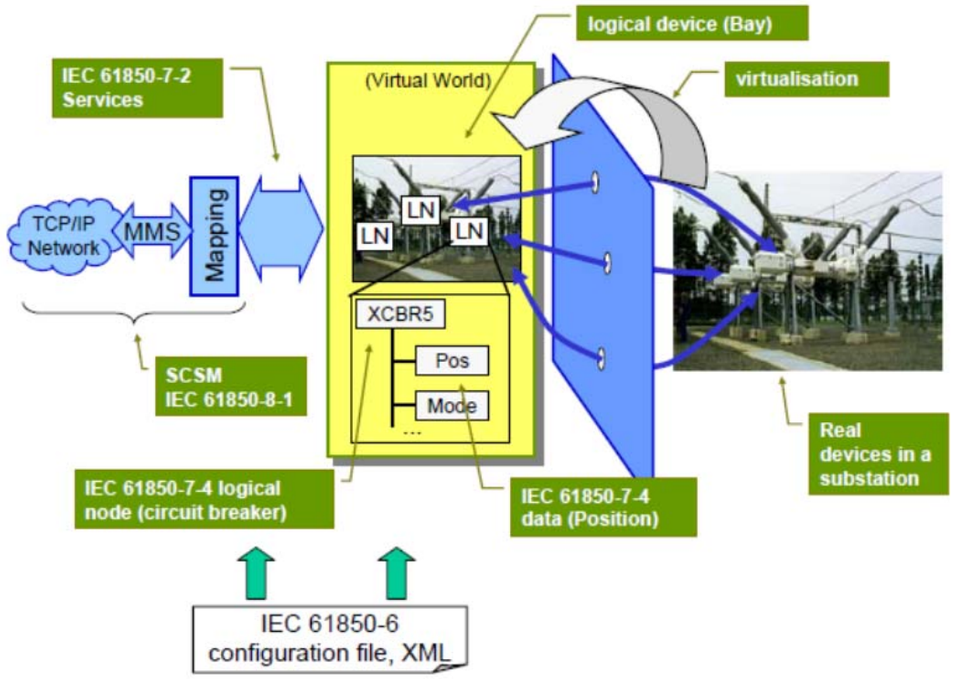


Fig. 16. Karlheinz Schwartz

8. Communication of events in an IEC 61850 substation

In his IEC 61850 Primer, Herrera states that "IEC 61850 provides a standardized framework for substation integration that specifies the communications requirements, the functional characteristics, the structure of data in devices, the naming conventions for the data, how applications interact and control the devices, and how conformity to the standard should be tested. In simpler terms, IEC 61850 it is an open standard protocol created to facilitate communications in electric substations."

8.1 The communication structure of the substation

The IEC 61850 architecture there are two busses:

- Process bus
- Station bus

IEC 61850 **station bus** interconnects all bays with the station supervisory level and carries control information such as measurement, interlocking and operations [13].

IEC 61850 **process bus** interconnects the IEDs within a bay that carries real-time measurements for protection called sampled values or sampled measured values [13].

Figure 17 shows the basic architecture.

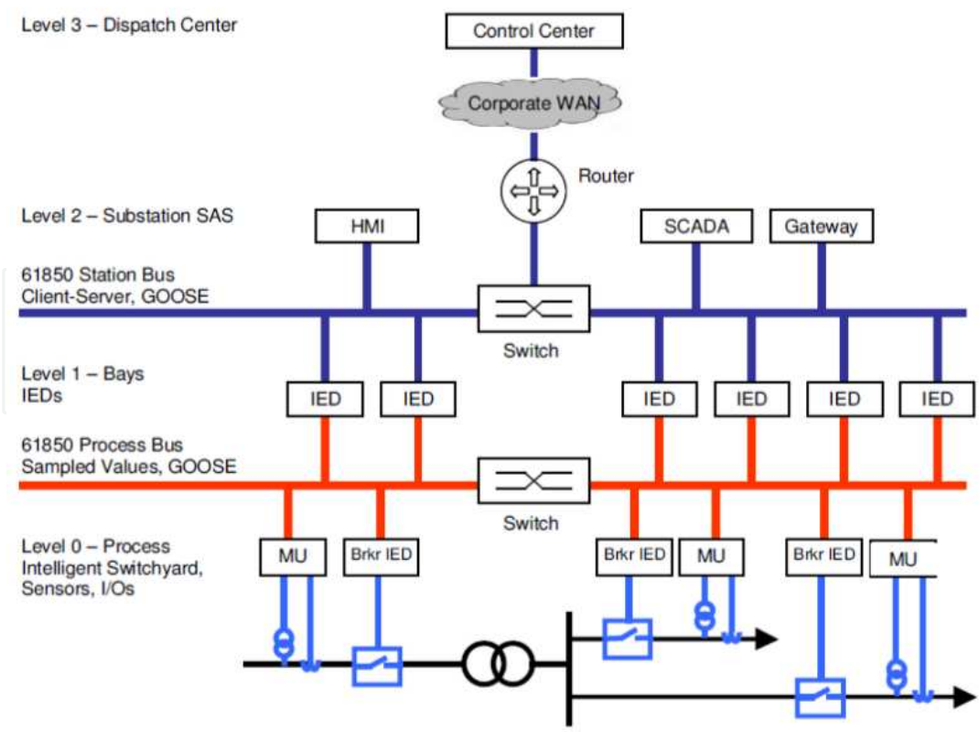


Fig. 17.

The process bus is designed to be fast since it must carry crucial I/O between IEDs and sensors/actuators.

The requirements for the process bus cited in various literature sources are as follows:

- High environmental requirements for the terminal equipment (electromagnetic compatibility, temperature, shock, where applicable) in the area of the primary system
- Adequate bandwidth for several SV data streams
- Highly prioritized trip signals for transmitting from the protection device to the CBC
- Permeability of data to the station bus/data filtering at the coupling point
- Simultaneous TCP/IP traffic for normal control and status signal traffic as well as reports on the process bus
- Download/upload channel for setting or parameterizing functions
- Highly precise time synchronization
- Redundancy
- For reasons of speed, the process bus is based on optical fibre with high data throughput of about 10Gbits/s. Because of its enhanced data capacity it is capable of carrying both GOOSE (Generic Object Oriented Substation Event) and SMV (Sampled Measured Values). The station bus is used for inter-IED communications. Only GOOSE messaging occurs in the station bus.

9. Substation control and configuration

Although the strengths of the IEC 61850 in the capturing, virtualisation, mapping and communication of substation information are undoubted, it will still be necessary to link everything together and to design a control strategy. This strategy must utilize the experience and expertise of the asset owner. The substation must also respond in accordance with the operational and safety criteria set by the organization.

9.1 Substation configuration

Automation of the substation will require in the first instance the capture of its configuration. This requires the capture of the information on all the IEDs in the substation. In some cases the IEDs could be from different vendors. The information has to be in a standardized IED Capability Description (ICD). Then, using a system configuration tool, a substation description file is created (Figure 18). The SCD (Substation Configuration Description) is then used by relay vendors to configure individual relays [14].

10. Wider implications of the IEC 61850: The Smart Grid

“Smart Grid” is a term used to describe the information driven power systems of the future. This will involve introducing new electronic, information and computer technology into the whole value chain of electrical energy systems from generation, transmission and distribution down to the consumer level. Figure 19 shows the linkages between the technology of electricity production and commerce.

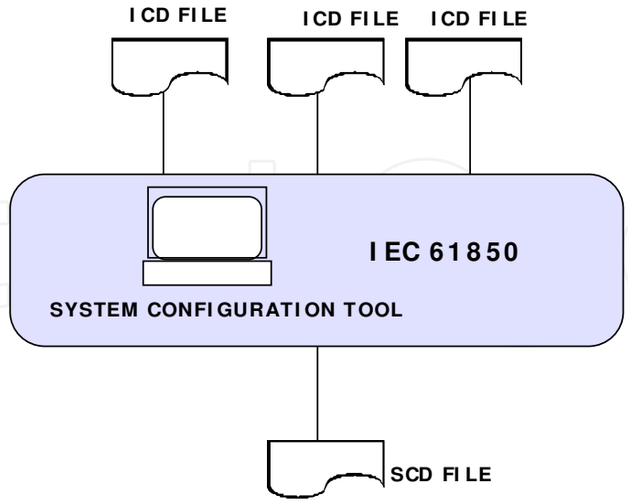


Fig. 18.

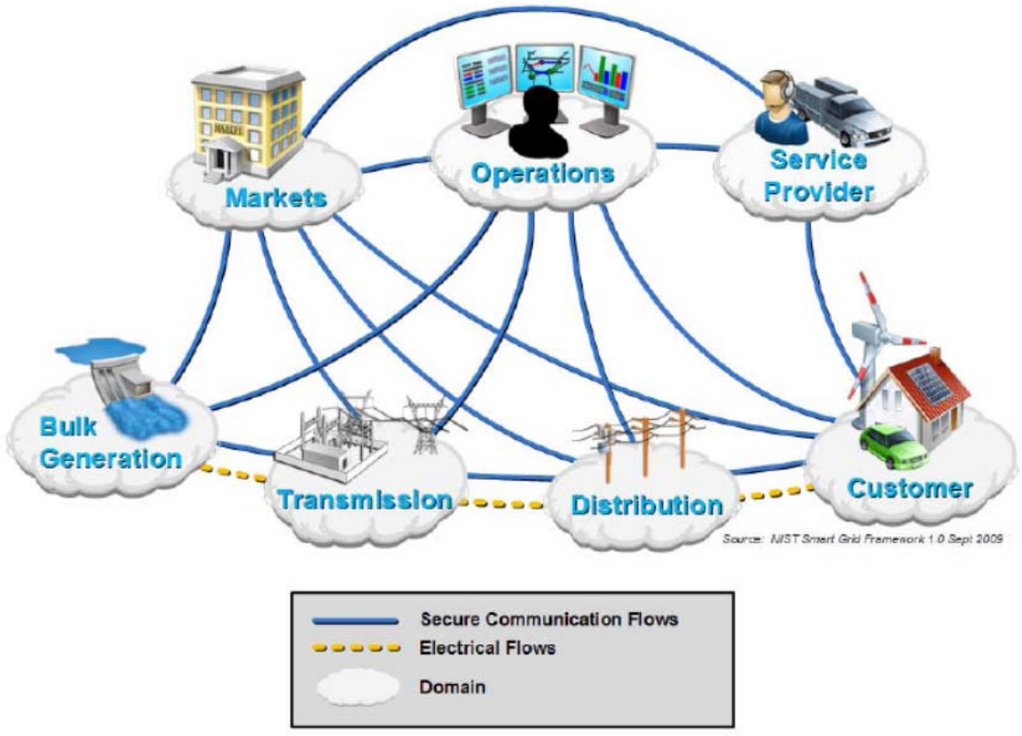


Fig. 19. Source NIST Smart Grid Framework

We have seen that automation started on the factory floor and some of the IEC 61850 functions use manufacturing protocols such as MMS. We already start to see the trend

towards extending the IEC 61850 to generating stations. It is therefore not hard to imagine IEC 61850 like protocols encompassing every facet of engineering, including manufacture.

10.1 Smart Grid benefits

Among the benefits of Smart Grid are:

- Increased grid efficiency - the use of control systems to achieve optimum power flow through, for example, centrally controlled FACTS devices which can increase efficiency of the transmission system
- Better demand control - a Smart Grid would incorporate an energy management system to manage demand (e.g., managing the peaks and valleys)
- Asset optimization - the IEC 61850 information model already has the capability to store not only the status of a logical device / node, but also condition / health
- Management of renewable energy sources - renewable energy sources, such as wind and solar, tend to be unpredictable, therefore, the Smart Grid system can enable predictions on the availability of these resources at any moment and ensure proper energy scheduling decisions are taken
- Management of plug in electric vehicles - the Smart Grid can inform electric vehicle motorists of the nearest charging stations
- Smart metering - with smart metering, power usage and tariffs can be administered remotely to the advantage of both the supplier and the consumer

11. Security threats in automated power systems

In this chapter we have seen the central role computer hardware and software in the control and management of the power system bring tremendous benefits. However, investing in these high technology, information technology reliant assets also brings threats. The threats are quite serious especially when it is realized that every critical component of the substation becomes a virtual computer. The IED mentioned numerous times in this chapter is itself a computer. What are the threats?

11.1 SCADA vulnerabilities Chikuni, Dondo [15]

- Computing vulnerabilities

Hardware: RTUs, IEDs and SCADA Masters belong to the class of computer hardware and suffer from the same vulnerabilities of regular computer systems such as interruption (denial of services [DoS]) and eavesdropping

Communication links: the vulnerabilities are also similar to those in regular computer networks - if messages are not encrypted, data or passwords can be intercepted. Radiation emissions from equipment can be read by unauthorized people

- **SCADA software:** the most common attacks come in the form of interruption, interception and modification. Software bugs, if not fixed in time, can attract hobbyist hackers to attack unpatched SCADA [15]

- **Data:** SCADA data has more value to the attacker than hardware and software. Data may be stolen by competitors of saboteurs. To safe guard the data, encryption needs to be included

11.2 Other vulnerabilities

- **Equipment location**: we have seen that some IEDs and RTUs are located in usually unmanned remote locations; where this applies these must be housed or mounted securely
- **Remote access**: access to relays, controllers, IEDs and RTUs should be password protected; encryption modems are available for secure dial-up communications
- **Human element**: the employee could be the most vulnerable part of the automated power system, therefore, no unauthorized persons should have access to the control terminals. Strong authentication and smart card access are recommended
- **Integrity and confidentiality**: software and hardware should have at least the US National Computer Security Centre (NCSC) class 2 rating. In Europe criteria similar to that of NCSC is managed through the European Information Technology Security Evaluation Criteria (ITSEC)

11.3 Attack examples

Nadel et al. [16] list what they describe as generic attack categories to which all network-based threats to substation automation systems can be reduced, namely:

- Message modification
- Message injection
- Message suppression

They demonstrate the various paths that an attacker can take in a given attack. An example of circuit breaker attack scenario is shown in Figure 20. In this case an attacker may take one of the paths in the graph to prevent a circuit breaker from opening when it is supposed to.

11.4 Countermeasures

Nadel et al. [16] list some of the important assumptions / precautions necessary before any meaningful countermeasures can be instituted. These include static configuration of the SAS and the number and types of devices in the bay level are known; configuration changes only to occur during major maintenance or modification work; also that the SAS is not used for billing and no general purpose PCs are allowed at bay level.

Message modification

In this attack parts of a valid, existing message are modified in transit. Detection is facilitated through encryption and digital signatures, with the receiver having a record of all authorized senders.

Message injection and replay

The attacker sends messages which are not intended to be sent by any authorized sender. These may be entirely new messages from the attacker or original untampered with replayed messages. Digital signatures are a way of combating message injection. To mitigate against replay, a digital signature and message sequence number are required.

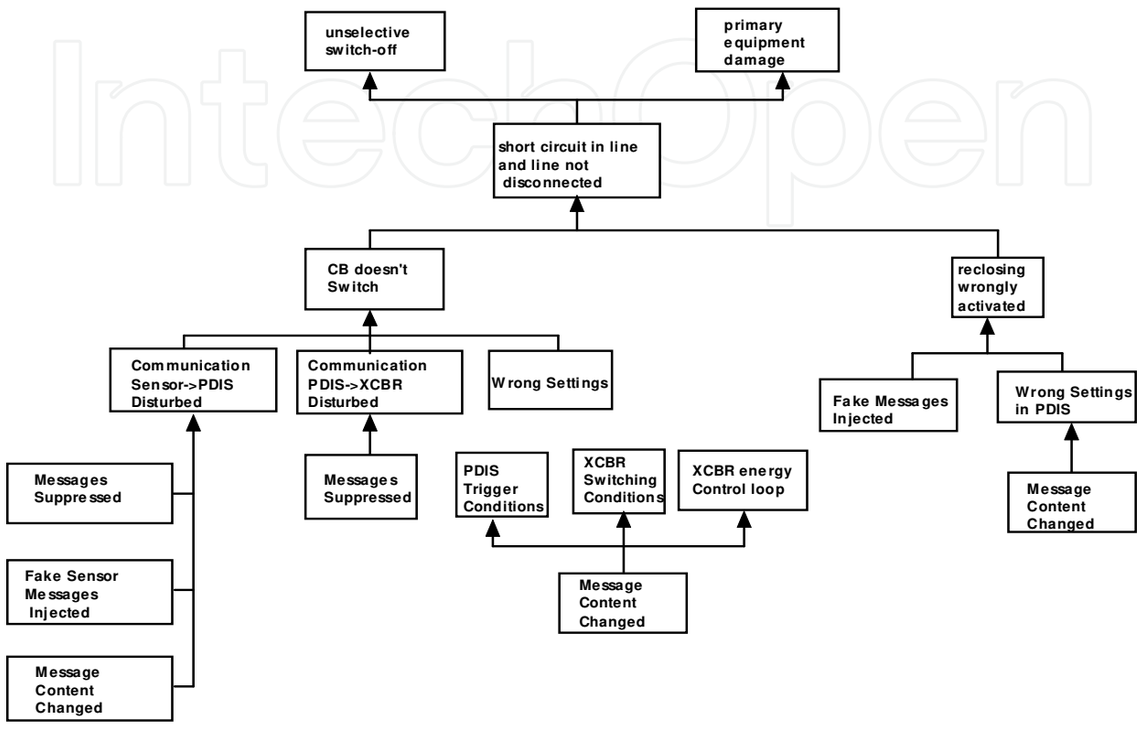


Fig. 20. Example of attack graph for a circuit breaker

Message suppression

In this attack certain messages between SAS devices are prevented from reaching the receiver, e.g., circuit breaker control devices are isolated from protection devices. Message suppression can involve several other types of attack, e.g., re-configuration of routers or switches, cutting wires or congesting the network so that genuine messages cannot get through (denial of service attack).

Security protocols

The multiplicity and varied nature of SAS attacks makes it imperative to institute robust security protocols capable of handling all eventualities. Such protocols include the use of private keys (only known to the sender), encryption and sequence numbers (initial number known between sender and receiver at the start).

Markets	
Subsystem Communication	
Intra-Markets	See Clause Markets
Intersystem Communication	
Operation	For scheduling and trading purposes, information about the availability of power (transfer power, operating reserve) or order information is transmitted to or from the operation system
Bulk Generation	For scheduling and trading purposes, information about the availability of power (transfer power, operating reserve) is transmitted from the bulk generation system
Service	Support functions for markets (e.g. forecasting for renewable generation)
Prosumer	For scheduling and trading purposes information about the availability of power or order information is transmitted to or from the markets system

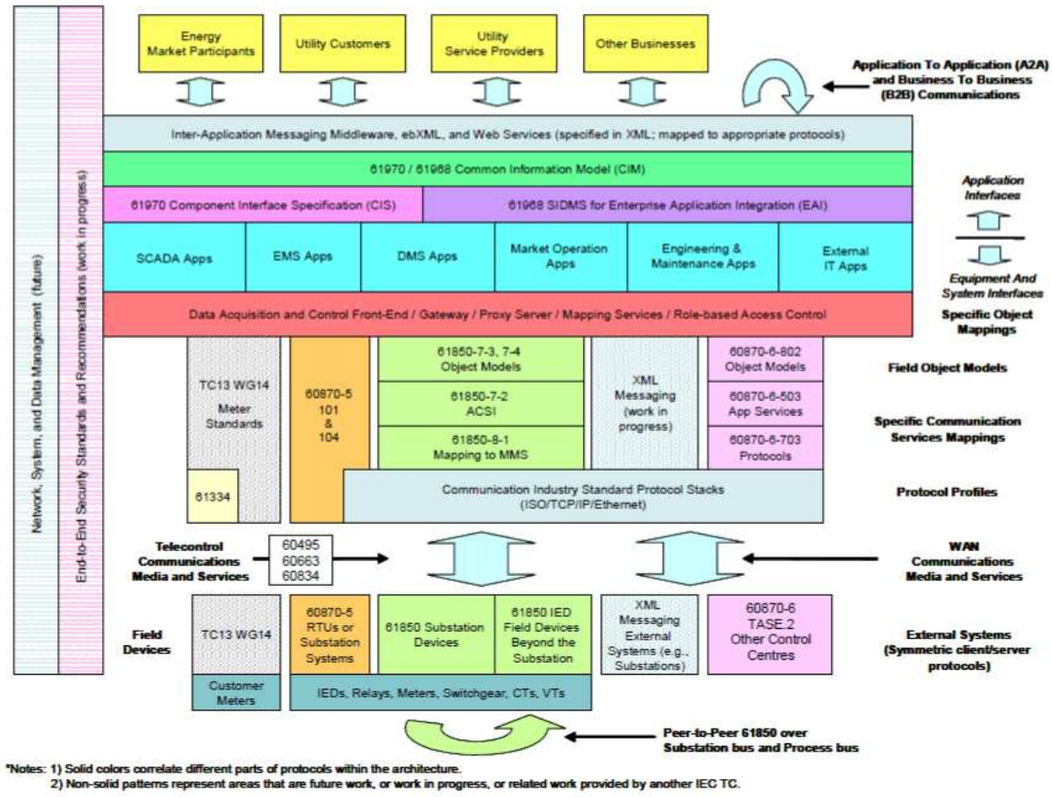
System: Service

The service system offers potential for a wide range of new service developments. New business models may emerge due to the opportunities of the future Smart Grid. Therefore the service system will have and depend on various interfaces to other systems.

Service	
Subsystem Communication	
The new service application shall follow a standardized way of software development in order to seamlessly fit into an overall system. The relevant standards are not within the scope of the IEC	
Intersystem Communication	
Operation	Support functions for operation (e.g. forecasting for renewable generation)
Market	Support functions for markets (e.g. forecasting for renewable generation)
Prosumers	Customer services (Installation, Maintenance, Billing, Home & Building Management) are quite conceivable

System: Prosumer
Description

Prosumer	
Subsystem Communication	
See Clause HBES/BACS	
Process Automation	In many industries (e.g. chemical, manufacturing) process automation is applied to control and supervise not only the manufacturing process but also the energy consumption or generation
Intersystem Communication	
Service	Support functions for operation (e.g. forecasting for renewable generation)
Operation	See Clause AMI, DER
Markets	For scheduling and trading purposes information about the availability of power or order information is transmitted to or from the markets system
Distribution	Typically the distribution system infrastructure is used for the communication to DMS



*Notes: 1) Solid colors correlate different parts of protocols within the architecture.
2) Non-solid patterns represent areas that are future work, or work in progress, or related work provided by another IEC TC.

12. Effects on educational curricula

To give an idea of the profound changes the power system will have on our education systems and also to give some suggestions on how to mitigate some of the challenges, we reproduce the following excerpts from a paper by Chikuni, Engelbrecht and Dongo [17] at the PowerCon 2010 conference:

"When we analyse a modern substation incorporating the new substation technology based on IEC 61850, it would seem that the role of an electrical engineer is notable by its absence. Certainly some of the responsibilities of both engineers and technicians have shifted and there needs to be new breed of electrical engineers altogether. Some questions need to be answered:

- Should we retrain the power engineer in networks or
- Should we train network engineers so that they acquire power engineering knowledge or
- Should we work with a completely new curriculum which merges power systems, electronics and networks into one programme?

We first need to acknowledge that there are already a lot of good power engineers out there trained in the traditional manner, i.e., starting off with physics, circuits and systems, electrical machines and power systems (including electrical protection). For these engineers, one needs to identify those who can benefit both themselves and their organizations by

going through this additional training. The process of training engineers has been quite formal, especially if they wish to attain professional status. One typically needs four to five years of formal training and a further two years of guided industrial training before attaining the status of chartered (CEng) or professional (PrEng) engineer. A great debate will ensue, therefore, when a computer network engineer is designated the 'responsible person' in an electrical substation, notwithstanding the obviously immense power this individual will have in making sure that the substation operates correctly, safely and efficiently.

The other route is to include networking as part of any electrical engineering curriculum. A few programmes today include industrial automation and a few even include computer networking. In the University of Zimbabwe model all electrical engineering students have a chance to complete at least the first semesters of a CISCO network academy programme. Indeed some complete the CCNA (four semesters). Whatever solution is arrived at, it is clear that electrical engineering training curricula inevitably have to include more and more electronics, sensors, automation and networking, not as peripheral subjects, but as part of the core.

13. Summary and conclusions

In this chapter we have seen the extremely rapid development of automation, starting from the years of mechanisation, production lines and the taking root of computer-based automation in the car manufacturing industry. Then we noticed rapid increases in computer power in both hardware and software forms. There has also been tremendous moves in standardization in North America and Europe. We have seen too IEC 61850 international cooperation in standards development and the benefits that are already being reaped from this. Interoperability brings some relief to customers, giving them the ability to choose hardware from an increasing variety of vendors. Quite striking is the increasing dominance of ICT in power system control and massive changes in power system operation and practice. The power systems have become more complex - more interlinked. The complexity presents new challenges. The traditionally trained power systems engineer lacks the know how to understand or tackle faults that could arise in these systems. On the other hand the network engineer may lack the underlying principles of power and energy systems. A new type of multi-discipline power systems engineer has to be trained. The Smart Grid will soon be a reality. Generation, transmission, distribution consumption and commerce will be information driven. Finally, when automation is combined with mechatronics and robotics, our lives are poised to be drastically changed.

14. References

[1] Mikel P. Groover, Britannica Online Encyclopedia
[2] Benjamin F. Shearer,. "*Home front heroes: a biographical dictionary of Americans during wartime*", Volume 1, Greenwood Publishing Group 2007
[3] Edward Chikuni, "*Concise Higher Electrical Engineering*", Juta Academic Publishers, 2008
[4] James Northcote-Green, Robert Wilson, "*Control and Automation of Electrical Power Distribution Systems*", Taylor& Francis, 2006
[5] AREVA, ALSTOM, Network Protection and Application Guide, 2011 Edition

[6] Su Sheng; Duan Xianzhong; W.L. Chan, "*Probability Distribution of Fault in Distribution System* , Power Systems, IEEE Transactions on, Aug. 2008"

[7] D. Bassett, K. Clinard, J. Grainger, S. Purucker, and D.Ward, "*Tutorial course: distribution automation,"* IEEE Tutorial Publ. 88EH0280-8-PWR, 1988

[8] IEC 61850 Guide Serveron® TM8TM and TM3TM On-line Transformer Monitors 810-1885-00 Rev A August 2011

[9] M.C. Janssen,, A. Apostolov "*IEC 61850 Impact on Substation Design"*

[10] Drew Baigent, Mark Adamiak, Ralph Mackiewicz, GE and SISCO "*Communication Networks and Systems In Substations, An Overview for Users*",.

[11] Karlheinz Schwarz, SCC, "*Monitoring and Control of Power Systems and Communication Infrastructures based on IEC 61850 and IEC 61400".*

[12] Dipl.-Ing. H. Dawidczak, Dr.-Ing. H. Englert Siemens AG, Energy Automation Nuremberg, Germany "*IEC 61850 interoperability and use of flexible object modeling and naming"*

[13] R. Moore, IEEE Member, R. Midence, IEEE, M. Goraj, "*Practical Experience with IEEE 1588 High Precision Time Synchronization in Electrical Substation based on IEC 61850 Process Bus"*

[14] J. Holbach, J. Rodriguez, C. Wester, D. Baigent, L. Frisk, S. Kunsman, L. Hossenlop, "*First IEC 61850 Multivendor Project in the USA, Protection, Automation and Control World, August 2007*"

[15] Edward Chikuni, Maxwell Dondo, "*Investigating the Security of Electrical Power Systems*" SCADA, IEEE Africon 2007, Windhoek

[16] Martin Naedele , Dacfey Dzung , Michael Stanimirov, "*Network Security for Substation Automation Systems*", Proceedings of the 20th International Conference on Computer Safety, Reliability and Security, p.25-34,September 26-28, 2001

[17] E Chikuni, F Engelbrecht, and M Dondo, "The emergence of substation automation in Southern Africa, opportunities, challenges and threats", IEEE Africon Conference, Windhoek, September, 2007

IntechOpen