Centralized Substation Protection and Control

IEEE PES

Power System Relaying Committee

Report of Working Group K15

of the

Substation Protection Subcommittee

Members of the Working Group

Ratan Das, Chair
Bethlehem, PA USA
ratan.das@us.abb.com

Mital Kanabar, Vice Chair
Markham, ON Canada
mital.kanabar@ge.com

Members:

M. Adamiak
A. Apostolov
G. Antonova
S. Brahma
M. DadashZadeh
R. Hunt
J. Jester
M. Kezunovic
M. Kockott
L. Kojovic
R. Lascu
Y. Liao
Y. Luskind
V. Madani
A.P. Meliopoulos
R. Midence
P. Myrda
A. Oliveira
J. Park
C. Preuss
Q. Qiu
M. Sachdev
I. Voloh
J. Xavier

The following were the members of the Substation Protection Subcommittee of the Power System Relaying Committee when this report was submitted and approved.

Michael Thompson, Chair

Don Lukach, Vice Chair

Members:

Martin Best
Gustavo Brunello
Patrick Carroll
Arvind Chaudhary
Stephen Conrad
Randy Crellin
Paul Elkin
William English
Dominick Fontana
Stephen Grier
Randy Hamilton
Roger Hedding
Gene Henneberg
Charles Henville
Gerald Johnson
Vahid Madani
Dean Miller
George Moskos
Chuck Mozina
Adi Mulawarman
Pratap Mysore
Mukesh Nagpal
Bruce Pickett
Lubomir Sevov
Charles Sufana
Qun Qiu
Ilia Voloh
John Wang
Roger Whittaker
Rich Young

Table of Contents

1. INTRODUCTION

The power grid is now more dynamic than ever before and newer tools are increasingly developed to manage the grid better. Renewable energy sources are changing power system characteristics at a time when utilities are also focusing on improving customer service and resiliency of the grid, by using advanced monitoring and control technologies. Synchrophasor technologies are being rapidly deployed to provide high-speed, high-resolution measurements from phasor measurement units (PMUs) across the transmission systems as a tool for monitoring and post fault analysis which may lead to real-time control using PMU data in near future. In addition, communication technologies are advancing and related international standards are maturing to be deployed in substation environment. Renewed attention is required on protection and control strategies that build upon the available and emerging technologies backed by a cost analysis that can be used to support a long-term value proposition. To explore improved utilization of present technologies and chart the development of the next generation Protection and Control (P&C) technologies, the IEEE Power System Relaying Committee has formed a working group to prepare a report describing and analyzing the state-of-the-art technologies for centralized protection and control (CPC) within a substation.

This report starts by reviewing the advancements in substation protection and control technology. Next the report describes CPC and reviews its history. Then the report reviews some of the existing technologies that can support CPC. Following this discussion is a review of some emerging technologies supporting high-speed communication with high degree of reliability. The report then proposes possible CPC architectures using existing standardized communication technologies, and provides an example of such a system with a typical substation configuration. The report then discusses reliability and cost analysis for these CPC architectures; addresses testing and maintenance aspects and discusses advanced applications that are either not possible or difficult to implement without CPC.

The report reviews a pilot project demonstrating that existing technologies are mature enough to support CPC. The report then discusses some of the emerging and future applications for protection and control which will require a paradigm shift in the way we approach the engineering, operation and maintenance of the power system protection and control. Some of these applications can only be applied with a CPC approach while others will significantly benefit in having the high-performance computing platform at the substation which centralizes protection and control.

Finally the report concludes that CPC technology, when appropriately applied, significantly improves the reliability of protection and control systems and the power grid at an affordable cost - with enhanced applications capability and maintainability for both hardware replacement and software upgrade.

2. BRIEF HISTORY OF POWER SYSTEM PROTECTION AND CONTROL

The history of protection goes back to the end of the nineteenth century. The first protection device invented and used was the fuse. Fuses were originally introduced in the North American and European markets almost simultaneously in mid-1880 [1]. The objective was to protect lamps because, at that time, the cost of a lamp was approximately equal to two weeks' gross earnings of an average worker. Only about three years after their introduction in the market, fuses were applied to protect circuits.

The first protection relay was developed in the early 1900s and the first installation was made in 1905 [2].The first Supervisory Control and Data Acquisition (SCADA) systems, although not called SCADA at the time, likely developed in the power industry with remote sensing of operation status in Chicago around 1912. Westinghouse Electric Corporation prepared a System Requirements Specification for a "Substation Control and Protection System" for EPRI Research Project RP-1359-1 in April 1980 [3] and developed the WESPAC system based on this specification in 1980s. The 'Integrated Protection System for Rural Substations' or 'Sistema Integrado de Protección para Subestaciones Rurales' (SIPSUR) was developed by GE and the North West Utility in Spain, Union Electrica Fenosa in 1990 [4]. Ontario Hydro developed the Integrated Protection and Control System (IPACS), with the first system installed in 1992. A more recent example is the centralized protection and control system for the island of Gotland installed in 2000 by Vattenfalls Eldistribution of Sweden [5].

2.1 Protection (Relaying)

The evolution can be divided into three main stages; the first stage was the era of electromechanical relays, which started over 100 years ago. The next era was characterized by static or solid state relays, which were introduced in the 1960s. The present era with microprocessor based relays started in the beginning of the 1980s, where microprocessor performed the logics, but the filtering was analog. Although earlier prototype systems had been implemented, the first commercially available fully numerical relay was introduced in 1984.

In the history of electrical protection, the basic function of protection has not changed: to properly detect a disturbance in the system and to clear the faulted area. Different technologies have been applied to change the form of a protective relay as most of the relaying fundamentals are inherited from previous technologies [6, 7, 8, 9].

The original protection relay, the electromechanical relay, still has a large installed base. It is not uncommon to hear of electromechanical relays that have been in service for 50-60 years. In the early 1960s, advances in large-scale integration technology enabled the use of electronics in relays. Before solid state relays were largely accepted as an industry standard, research in applying computer technology to protective relaying had already begun by the late 1960s. Initial experiments were performed using computer-based systems. It was suggested in mid-1960's that computers could be used to protect components of power systems [10]. During the 1970s, great advances were made in hardware technology as well as in software techniques. These advances led to the first commercially available microprocessor-based relay in 1984. Continuous advances in electronics combined with extensive research in microprocessor-based systems reached a point where few applications could not be covered by a numerical/digital relay by the late 1980s.

Despite the great advantages offered, the new technology received stiff competition from well-established electromechanical and solid state devices. Multifunction relays, which appeared in the late 1980s, offered significant advantages by drastically reducing the product and installation costs. Since the mid-1990s, the use of microprocessors and digital technology in protective relaying has exploded into a thriving industry.

Modern protection and control technology is characterized by a few trends: common hardware platforms, software configuration to perform many different protection functions in one device, improved communication capabilities supporting protocols such as DNP3 (IEEE 1815) as well as MMS and GOOSE (IEC 61850), and synchrophasor (IEEE C37.118) combined with transitioning support from serial communications to Ethernet based communications. This led to the naming of new devices as Intelligent Electronic Devices (IEDs), to contrast with the traditional relay, as protection IEDs perform control, automation and communication functions in addition to their traditional protection functions.

Figure 1 captures the evolution of technologies applied for protection over the years. Block 1 shows electromechanical and solid state relays. Block 2 adds communications with an RTU or data concentrator (a station level device collecting all information from Bay level relays/IEDs), the start of a substation automation system. Block 3 shows communications using protocols like DNP3 (IEEE 1815) and Modbus; more recently, block 3 also represents peer-to-peer communications using GOOSE (IEC 61850). Block 4 shows the transfer of digitized analog values directly to IEDs from merging units using IEC 61850-9-2.

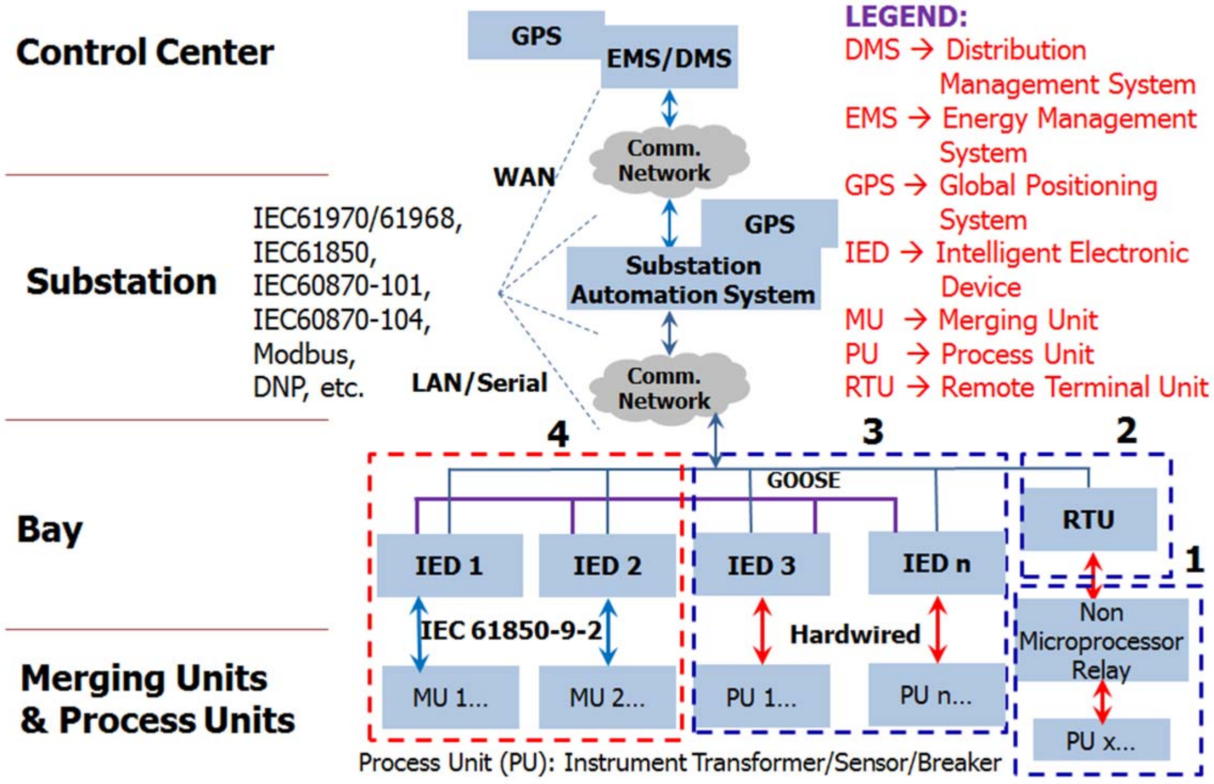


Figure 1. Evolution of protection system.

2.2 Control

While protection is associated with protecting the power system from abnormal operation, the control system is primarily concerned with supporting the operation of the substation equipment. Because the control system provides access to changing the state of substation equipment, it is leveraged by protection devices to remediate any abnormal operating conditions detected by the protection system. While the control system typically acts slowly, perhaps on the scale of seconds, the protection system typically acts at a much higher speed, i.e. ¼ -1cycle (~ 4 to 16 ms for 60 Hz).

There are two basic types of control operation, manual and automatic control. Manual control is performed by personnel using control switches to change the operating state of electrical equipment for some reason, such as equipment maintenance, load transfer, change transformer tap position, override automatic control, etc. Automatic control is used when the control system performs some task automatically, without human intervention, by measuring the parameter being controlled and all of the inputs and outputs that change the measured parameter. Automatic controls are most commonly found in transformer automatic load tap changers and capacitor bank controls.

Both automatic and manual control can be performed locally at the equipment level, at a control house, remotely from a centralized location such as a control center, or any combination of the three. Local control is typically performed at the control house or at the equipment, where all control circuits are actually hardwired from the switches to the equipment. Remote manual control is typically performed from a location considered remote, or far away, from the equipment's location, where today there is no hardwired connection all the way from the operator in the control center to the equipment being operated. Automated control can also take place locally at the substation (in the control house or at equipment) or remotely at the control center. This centralized automatic control is actually one approach to distribution automation, where automatic control is maximizing the performance of the distribution grid through reactive power and circuit configuration optimization using real-time load flow analysis based upon data being automatically reported from equipment on the distribution circuits and in distribution substations.

Just as the application of advanced control technology to distribution system is called distribution automation, similarly its application in substations is typically called substation automation. Both are somewhat ironic because the amount of actual automatic control being performed, ignoring protection as a form of automatic control that it is, may actually be quite small. Interestingly, the amount of automated data collection is quite high, which reflects the roots of substation automation in the first forms of SCADA technology.

The first SCADA systems, although not called SCADA at the time, likely started in the power industry with remote sensing of operation status in Chicago around 1912. At that time, telephone lines were used to transmit data from a number of electric power plants to a central office. It is likely this "supervisory" control was done to avoid having personnel stationed at the remote site to continuously monitor the equipment. By 1937, supervisory control, supervisory indication, and telemetering were defined in IEEE C37.2. By 1955, the term telemetering was officially defined by the AIEE as measuring with the aid of intermediate means which permit the measurement to be interpreted at a distance from the primary detector [11]. By the 1960s, the expression "Supervisory Control and Data Acquisition" was being used by the Bonneville Power Administration in planning studies [12]. In 1984, ISA-RP60.6 defines the SCADA acronym. In 1987, IEEE C37.1 contained the term "scada" for the first time, but interestingly it was not defined as an acronym, the longer term defined was a supervisory control data acquisition system. In 1992, IEEE 999 used the term SCADA in the title and the forward acknowledges that work on it began in the early 1980s because each SCADA vendor was producing a proprietary protocol to communicate between the master station and the RTUs. Today, there are Energy Management Systems, Generation Management Systems, Distribution Management Systems, and even advanced Distribution Management Systems. All of these still have at their core, SCADA. Over all these years, the fundamental architecture of these systems has remained the same, comprised of three main components:

1. The master station
2. The communications transport system
3. The remote station, or remote terminal unit (RTU)

What has significantly changed over the years is what makes up all three systems. For example, the remote station located at a substation used to be a dedicated device manufactured by a SCADA vendor communicating over slow serial communication channels and housed in one, two, or even three cabinets. Today, the RTU tends to be a data concentrator polling a variety of IEDs using protocols such as DNP3, IEC 61850 MMS, and Modbus over a high-speed local area network. All of these protocols provide the ability for a master station to communicate with a remote station, to automatically collect data and enable control, locally or remotely, manually or automatically.

2.3 Communications for Protection and Control

A visitor to any power system installation is hardly ever attracted to the underlying telecom infrastructure, and there was a time when power system communications were no more than, say, a SCADA or a substation subsystem. In today's T&D environment, it has become a consolidated activity as utilities increasingly invest in their own dedicated telecommunications infrastructure. Secure, reliable communications lie at the core of today's power delivery systems.

Through the years the need for reliable communications systems has become a mandatory consideration when designing protection and control systems. To date, communication is an important element for protection, control, energy management, and wide area monitoring.

Power system fault protection is the traditional VIP passenger of a dedicated telecommunications network with the most stringent performance requirements. To clear a network fault within 80 to 100 ms, the communications signal must propagate in just 5 to 10 ms. Moreover, the network's availability and integrity requirements are well beyond a mainstream telecom service—and are growing more demanding as differential protection and System Integrity Protection Schemes (SIPS) are used for more selective, precise, faster fault clearance. Inadequate communications can have drastic consequences.

With increasing demand for communications, digital communication technologies are being applied at an increasing rate. Electric utility applications are also increasing as the advantages and characteristics of the various digital communications technologies are better understood.

The telecommunications industry is one of the leaders in digital communications technology. They can drive the technology and the market. Electric utilities have a much smaller impact on the digital technology market.

Accordingly, electric utilities typically buy versions of telecommunications industry products with modifications made for this industry, such as surge withstand capability, wide temperature variations, abnormal vibrations, and immunity to electromagnetic, electrostatic and radio interference. This is the case for the digital communications systems applied in the typical environments found in power system substations.

In the new era of protection and control, it is very important that protection and control engineers understand digital telecommunication system architecture [13, 14]. However, as mentioned before, the environmental requirements for the application of digital communications for substation automation are more stringent to ensure an acceptable and reliable performance.

2.4 Centralized Protection and Control

There is no formal centralized protection and control (CPC) definition in the IEEE based upon the working group's survey of IEEE publications. This report defines a CPC system as a system comprised of a high-performance computing platform capable of providing protection, control, monitoring, communication and asset management functions by collecting the data those functions require using high-speed, time synchronized measurements within a substation.

The concept of CPC dates back almost to the beginning of the wide adoption of computers for business, starting with a first proposal published in 1969 [15], and a first installation as a field proof of concept in 1971 [16, 17]. The early experimental systems focused on computer relaying in general, and were limited by the technology available at the time. Projects in the late 1980s and early 1990s began to experiment with centralized protection and control specifically. This section is an overview of some of the projects and systems that have been installed.

2.4.1 Westinghouse Electric Corporation Project - USA

Westinghouse Electric Corporation prepared a System Requirements Specification for a "Substation Control and Protection System" for EPRI Research Project RP-1359-1 in April 1980 [3]. This specification is considered to be one of the earlier attempts to provide protection and control in an integrated system. The report includes Line, Transformer, Bus, Shunt Reactor, Out-of-step and Breaker Failure protections. The specification also includes control features such as local control of voltage, VAR flow, load shedding and automated switching sequence. Monitoring features including sequence of events records and oscillography are also considered in the specification. System restoration aid such as fault location estimation is also included in the specification. Revenue metering and SCADA interface were also considered. Based on this specification, WESPAC system shown in Figure 2, was developed and deployed in several substations starting in early 1980s [18,19]. American Electric Power (AEP) developed an Integrated Modular Protection and Control system (IMPACS) during this period while ASEA had developed a hybrid system in conjunction with the Swedish State Power Board [20].

2.4.2 SIPSUR – Spain

The SIPSUR system was developed by GE and the North West Utility in Spain, Union Electrica Fenosa in 1990 [4]. SIPSUR was a project to integrate in a single hardware package a complete protection system for a medium voltage (MV) distribution substation. The system comprised two incoming feeders, one transformer and five distribution feeders. The specialty of this system was the concept of “Back-up CPU ” as shown in Figure 3.

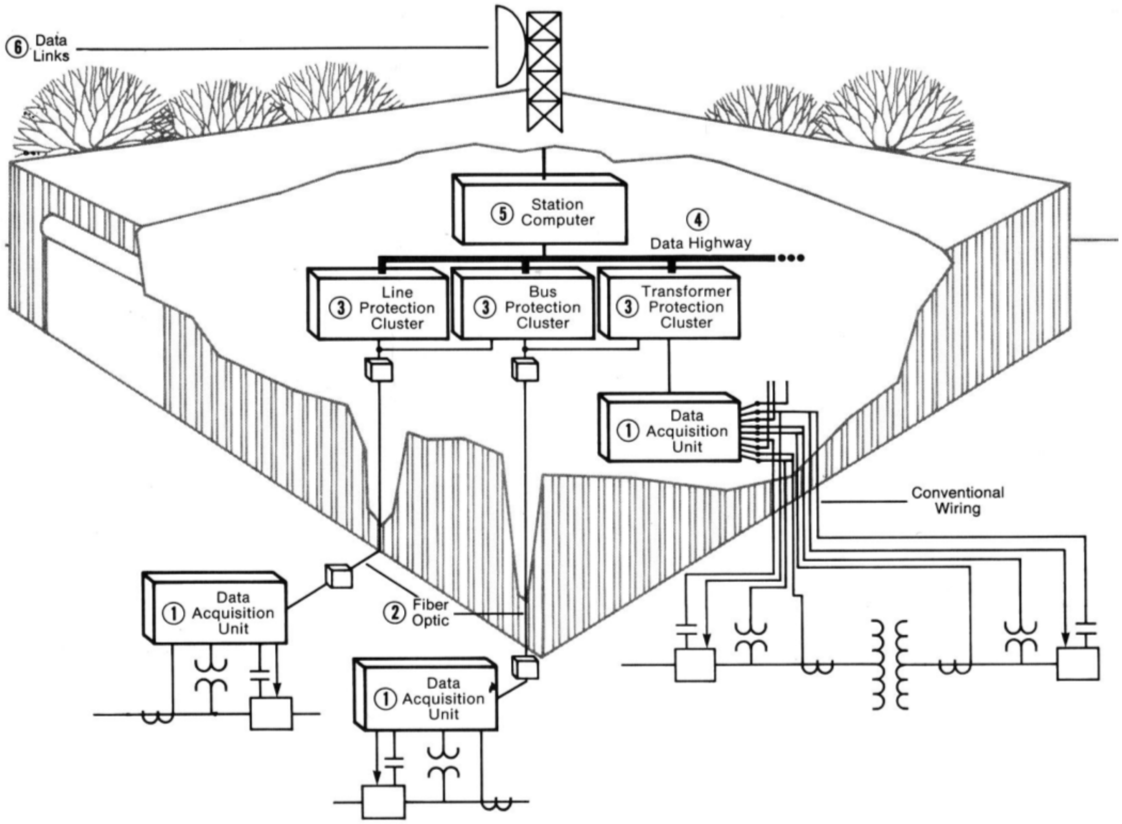


Figure 2. WESPAC integrated system [21].

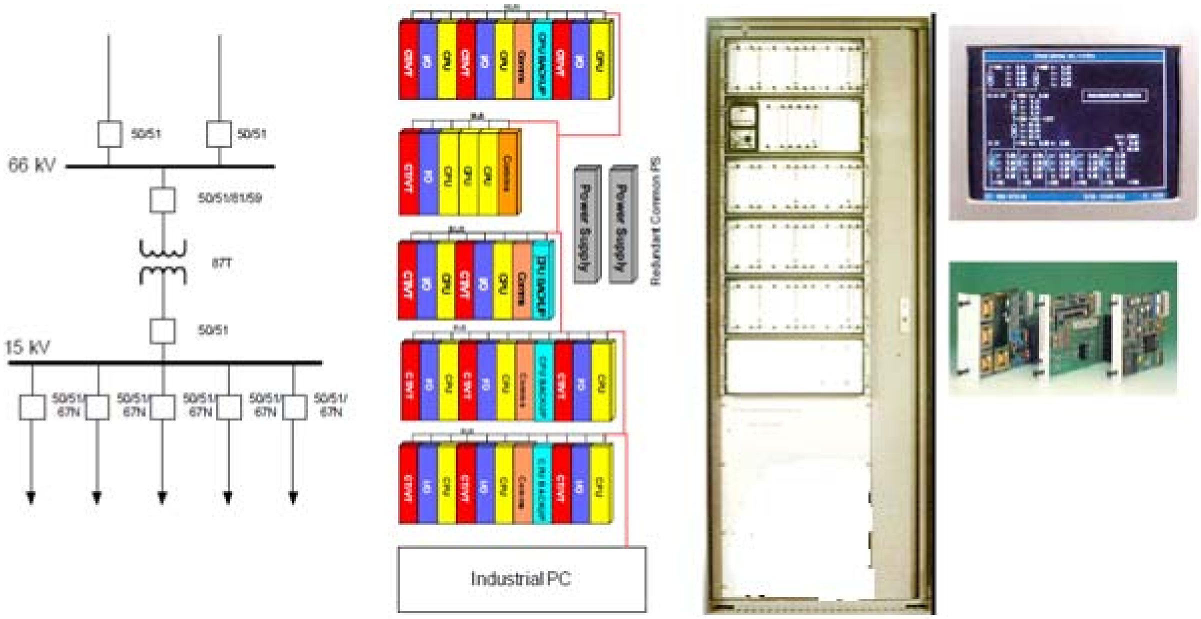


Figure 3. Back-up CPU concept in SIPUR – Spain [4].

2.4.3 Ontario Hydro IPACS System – Canada

Ontario Hydro developed the IPACS (Integrated Protection and Control System), shown in Figure 4, with the first system installed in 1992. IPACS was a computer system designed in one box panel by Ontario Hydro to do all the protection, control, monitoring, and recording for a Dual Element Spot Network (DESN) station. A DESN station is a transformer station that steps voltage down from transmission to distribution levels. Every element (transformer, bus, etc.) are duplicated and configured so that individual elements may be taken out of service without interrupting supply to loads. Ontario Hydro (now Hydro One) has about 300 DESN stations, and IPACS was developed to be a cost effective method to refurbish these stations. 56 IPACS systems were built and installed before the project was abandoned in 1998.

IPACS was an all-in-one solution for DESN substations, and included protection for feeders, capacitors, buses, transformers, etc.; full metering including tapchanger position and DC battery voltage; SCADA RTU functionality for up to 2 masters; local control and HMI; and other functions such as voltage regulation, reclosing, capacitor auto switching, underfrequency load shedding, digital fault recording, sequence of events recording, power quality monitoring, and breaker wear monitoring.

The IPACS system uses a single CPU to implement all functions. Reliability of protection and control is provided by having a second IPACS system, or by other types of redundancy. This can be a completely identical IPACS system, or using a full function conventional protection/metering/SCADA backup, or limited function conventional backup.

2.4.4 Vattenfalls Project - Sweden

Vattenfalls Eldistribution developed a centralized protection and control system, shown in Figure 5, for the island of Gotland in 2000 [5]. The system was developed in collaboration with ABB, with all protection and control algorithms operating on a standard industrial computer. The system was developed starting with technology used for protection and control of HVDC substations, adding AC protection algorithms to the existing control system.

Each protection and control system uses an industrial computer and I/O devices connected to the primary processor. Each computer connects up to 5 I/O racks, with processor cards for analog and digital inputs and outputs. The I/O signals are connected to the computers via a separate cabinet with terminal blocks for each computer. The operating system in the computers is a real time kernel in combination with Embedded Windows operating system. System software and the application programs for the different protection and control functions are run on top of this operating system. The first of these systems were installed in 2000, with 5 different systems in service.

The concept behind developing this solution with standard computers is to support simplified handling of installation and testing, and the future ability to add other novel station functionality, such as internal self-control of the station. The system as designed by Vattenfalls has the ability to implement any protection algorithm, from any vendor. New algorithms can be chosen, and rolled out to all installations simultaneously, providing rapid, system-wide upgrades for protection and control.

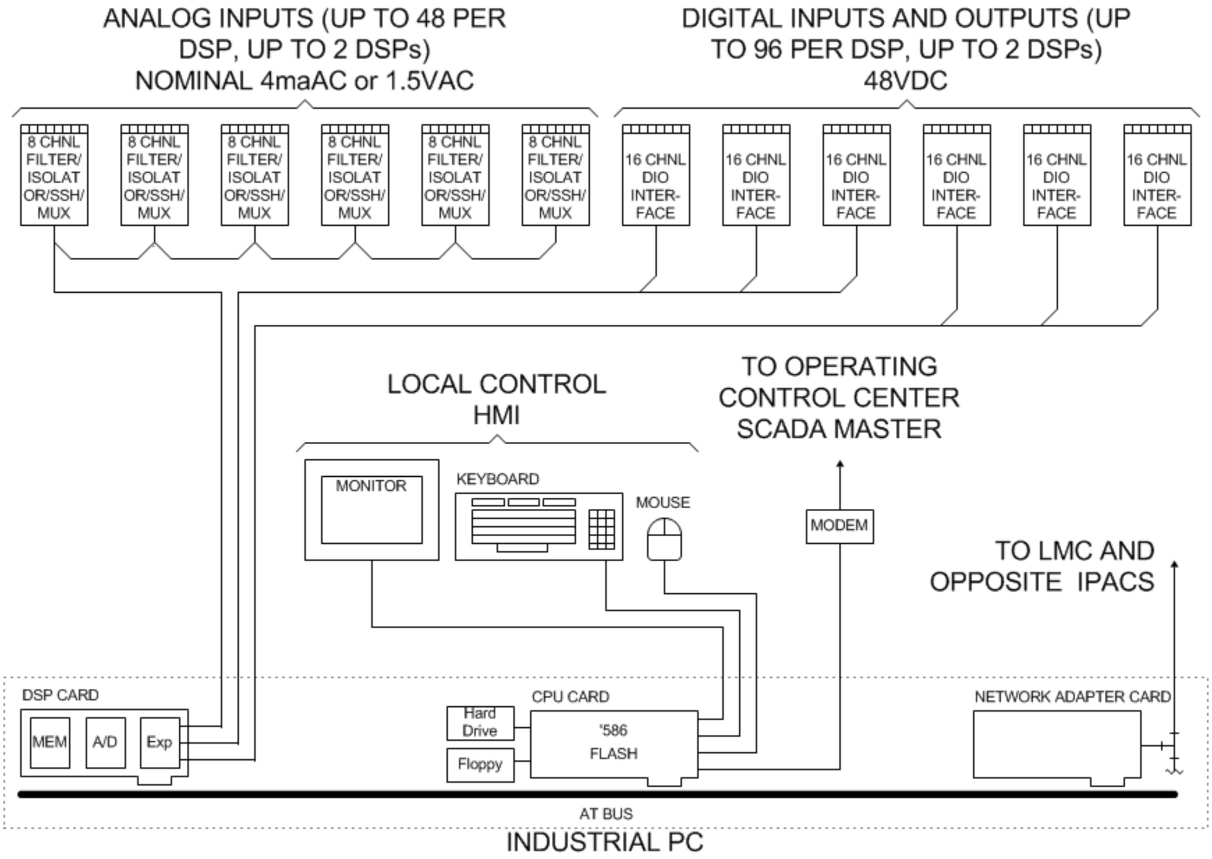

ANALOG INPUTS (UP TO 48 PER DSP, UP TO 2 DSPs) NOMINAL 4maAC or 1.5VAC
DIGITAL INPUTS AND OUTPUTS (UP TO 96 PER DSP, UP TO 2 DSPs) 48VDC
8 CHNL FILTER/ ISOLAT OR/SSH/ MUX
16 CHNL DIO INTER-FACE
LOCAL CONTROL HMI
TO OPERATING CONTROL CENTER SCADA MASTER
MONITOR
KEYBOARD
MOUSE
MODEM
TO LMC AND OPPOSITE IPACS
DSP CARD
MEM
A/D
Exp
Hard Drive
Floppy
CPU CARD
'586 FLASH
NETWORK ADAPTER CARD
AT BUS
INDUSTRIAL PC

Figure 4. Ontario Hydro IPACS System – Canada.

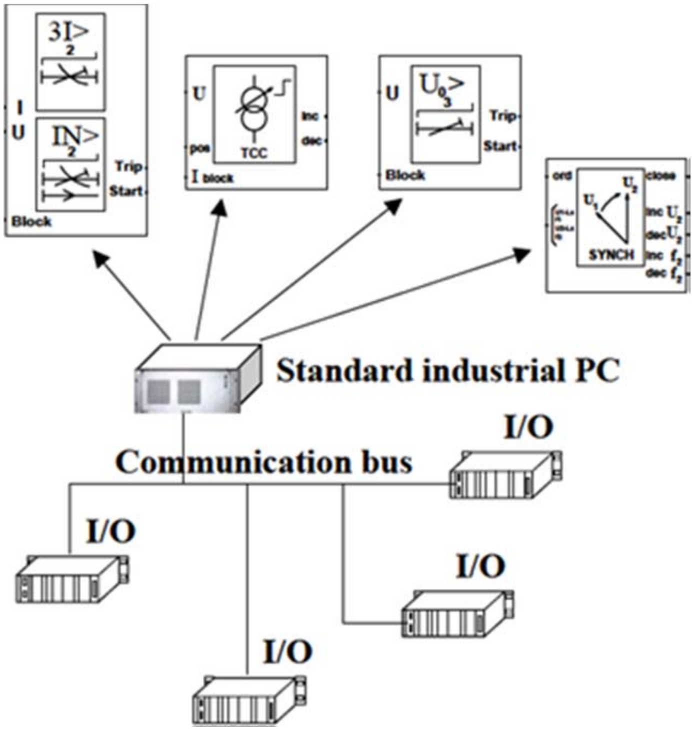


Figure 5. Gotland –Sweden, Centralized protection and control system by Vattenfalls Eldistribution [5].

2.4.5 Typical CPC Architecture

The typical CPC architecture with traditional copper wiring that has been attempted in the past is shown in Figure 6. Completely redundant (working independently & simultaneously) CPCs are directly connected to instrument transformers (redundancy is not shown in the figure) and switchgear using copper wires. CPC inputs/outputs from process level have some kind of (e.g. opto-) isolation. The CPC is connected to the RTU and Engineering stations using Point-to-point Ethernet or serial connection.

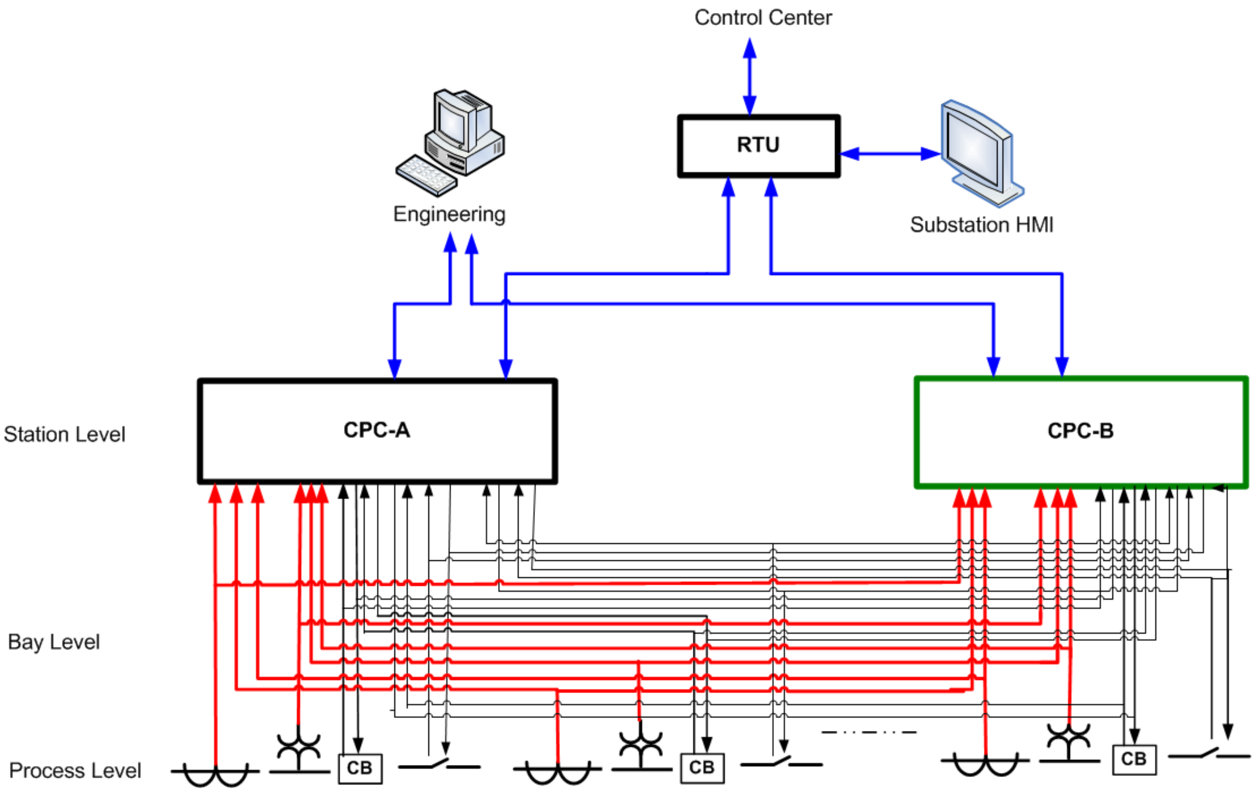


Figure 6. Direct connection between process level and CPC system at station level.

3. IMPACT OF CHANGING GRID TOPOLOGY

Smart grid development is changing power system characteristics, at a time when utilities are also focusing on improving customer service and resiliency of the grid. Wide Area Situation Awareness (WASA) and System Integrity Protection Schemes (SIPS) are gaining more momentum for safe, reliable and stable operation and control of a power grid. The power system changes are more apparent in distribution systems due to the integration of renewable energy resources, energy storage and electric vehicles [22]. The use of power electronics-based equipment for lighting, drives and distributed generation sources are also impacting power quality as well as system operation and control [23].

Figure 7 illustrates the vastness and scale of the North American electric grid with respect to geographical area with diverse natural calamity, public policies and varying power system patterns which are common to other parts of the world. Figure 8 illustrates the evolution of a typical electric power system. The evolving system introduces many new challenges in policies, operation, maintenance, protection and control from inception to life-cycle support.

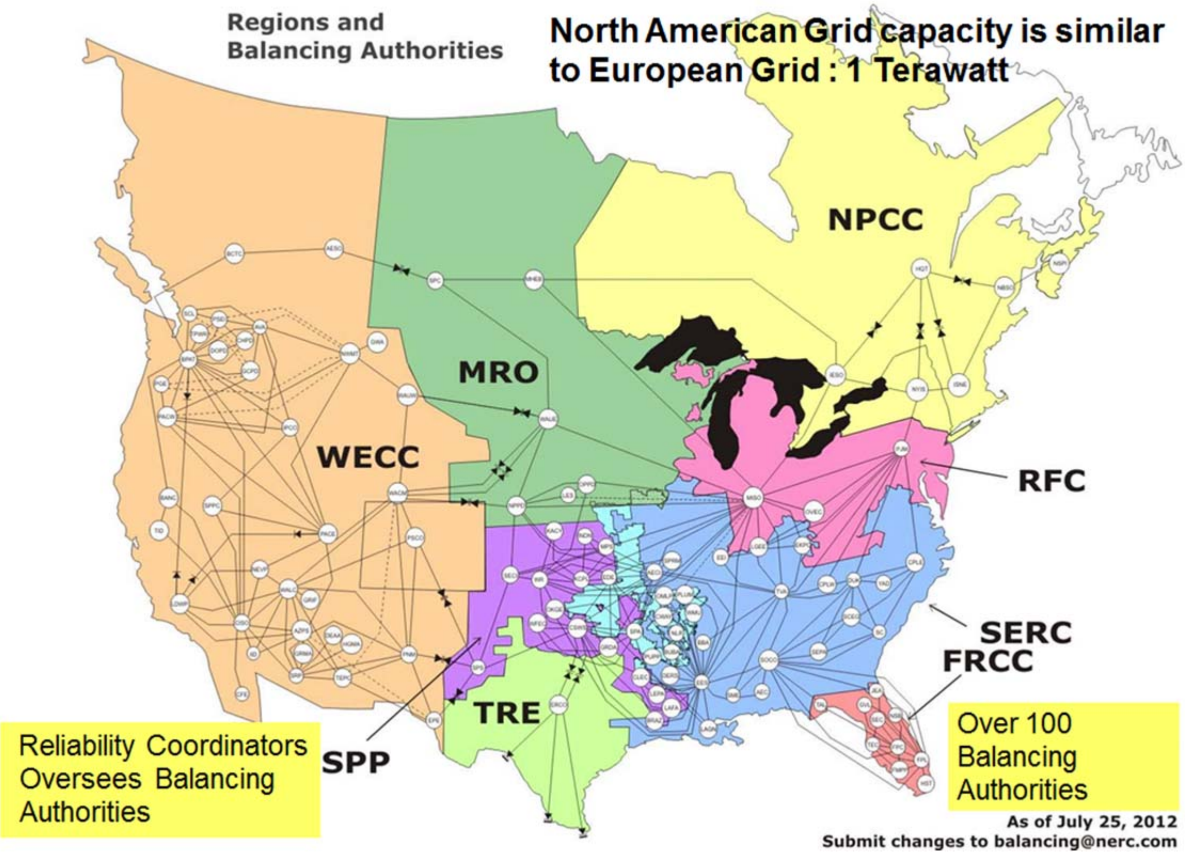


Figure 7. North American Electric Power Grid [22].

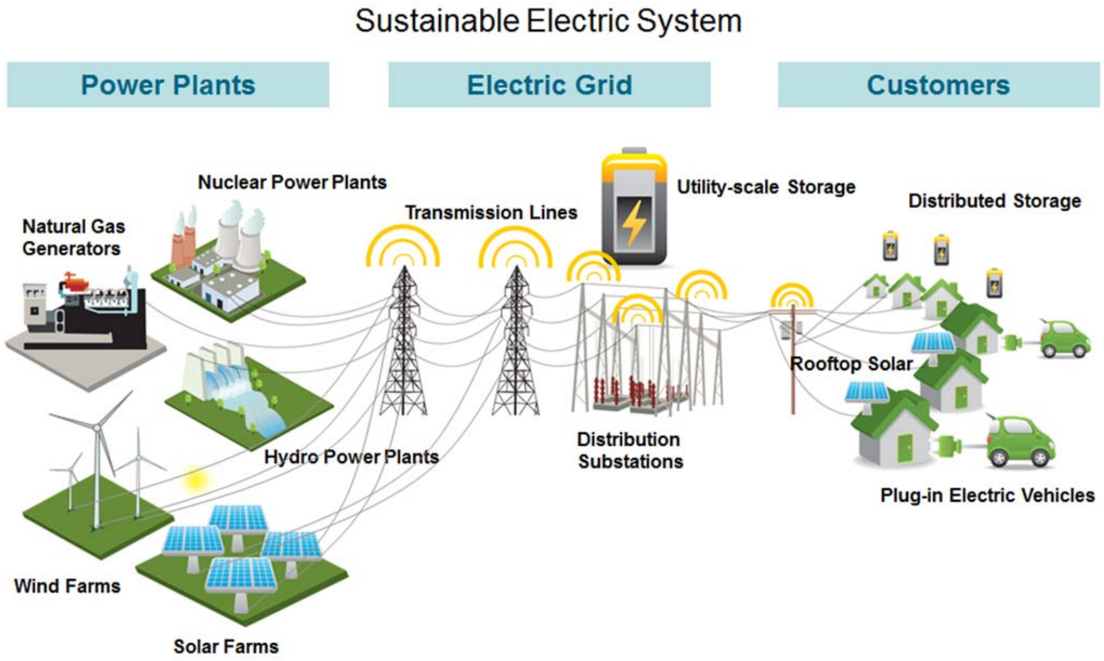


Figure 8. An evolving electric power system [22].

The development of microgrids provides new opportunities in managing the grid - contributions to capacity, reliability/resiliency, and power quality improvement. The evolution of dynamic microgrid will further alter system characteristics. One such scenario is described in Figure 9, which takes a holistic view of a power system from the balancing authority (BA) to the customer loads at distribution level. In this scenario, conventional substations are complemented by microgrids under the control of a DMS as in Figure 9 (b). These microgrids can be dynamic and substations can be used as dynamic control centers of these microgrids in some scenarios. This feature complements the dedicated control centers of some microgrids and offers maximum flexibility from the operation perspective. There is also a possibility for asynchronous connection of microgrids with the main AC grid using medium voltage and low voltage DC links. Applications that typically run today and are expected to run in future at different layers of a power grid are also identified in Figure 9 [24].

Future protection and control systems should adapt to the architecture of the power system shown in Figure 9. Control of active and reactive power at the distribution level while maintaining the regulation voltage profile and frequency across the network will offer opportunities for greater innovation for network owners and managers – utilities, distribution agencies, state or governmental agencies, and reliability coordinators. Greater integration of the control system with the network protection devices will assist in addressing these challenges and reduce the overall ownership cost of a more reliable and robust system protection and control. This integrated approach will also assist in managing assets with performance and retrofit/replacement requirement information for maintaining system reliability [24]. The CPC will play a very important role by combining various protection and control functions required for the evolving grid. One of the benefits of having a high-performance computing platform like CPC at the substation is the possibility of bringing intelligence to the substation. The CPC can act as a node for distributed control architecture.

CPC will also address the hardware replacement requirement and software upgrade of the protection and control system due to various reasons as discussed in [25], while minimizing system downtime.

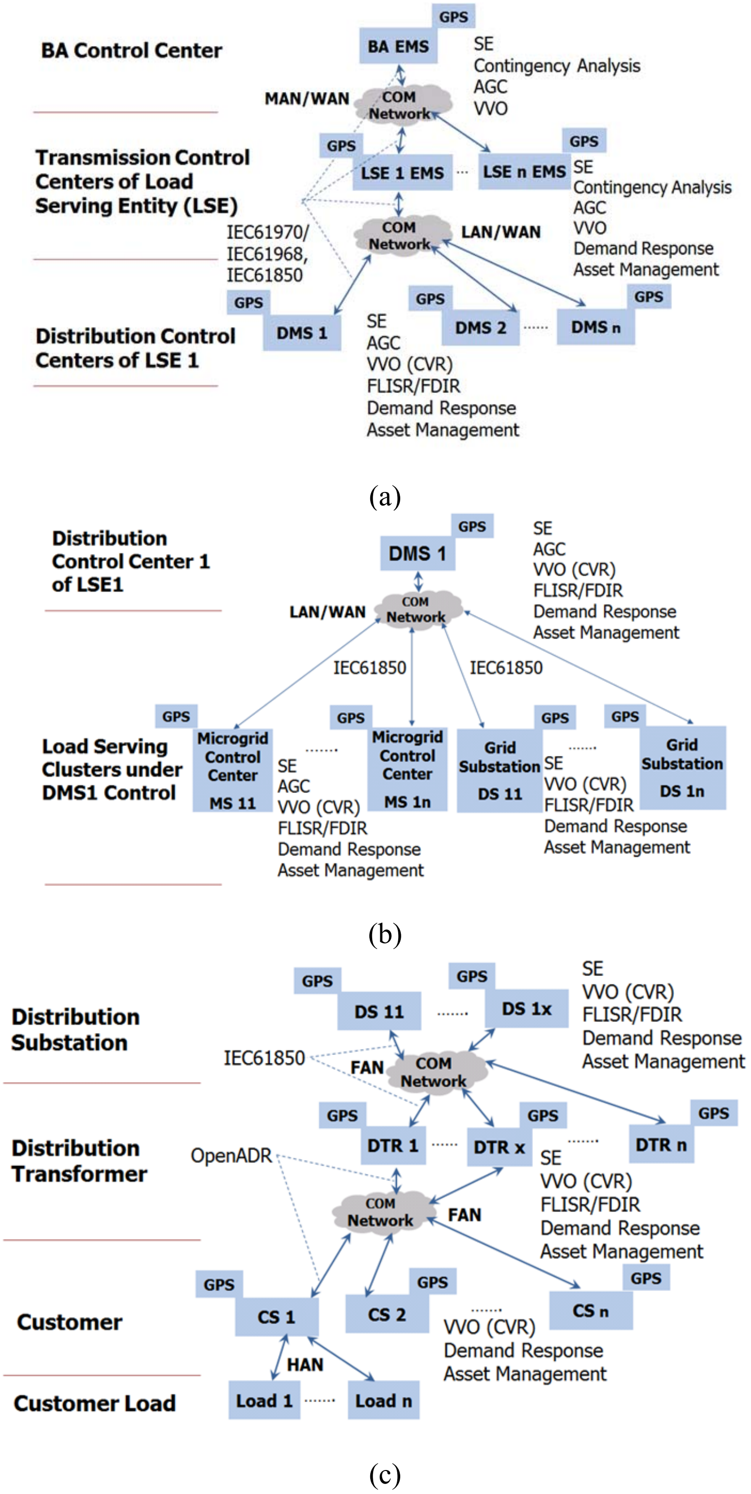


Figure 9. Possible architecture of a distribution system connected to a larger grid, (a) from transmission system to DMS, (b) from DMS to primary and secondary substations and (c) from substations to customer loads [24].

4. Centralized Protection and Control within A Substation

The idea of IEDs sharing information opened up many possibilities with the clear potential of better detection of fault conditions and improvements in protection security and dependability. These possibilities can be implemented in a variety of architectures that may eventually include a central computing platform in a substation to concentrate the information and perform protection using centralized data. A centralized substation protection and control system is comprised of a high-performance computing platform capable of providing protection, control, monitoring, communication and asset management functions by collecting the data those functions require using high-speed, time synchronized measurements. Figure 10, an extension of Figure 1 with the addition of Block 5, illustrates the evolution of the protection, control, monitoring, and communication system leading to CPC [24]. Block 5 shows the transfer of sampled analog values from Intelligent Merging Units (IMUs) to CPCs as well as GOOSE messages from CPCs to IMUs, and MMS messages transferred from IMUs to the CPC using fiber optical communication. It is important to note that CPC technology should be able to co-exist with all technologies in a substation, shown in Figure 10, to be able to attract retrofit application which is often the case in a matured market.

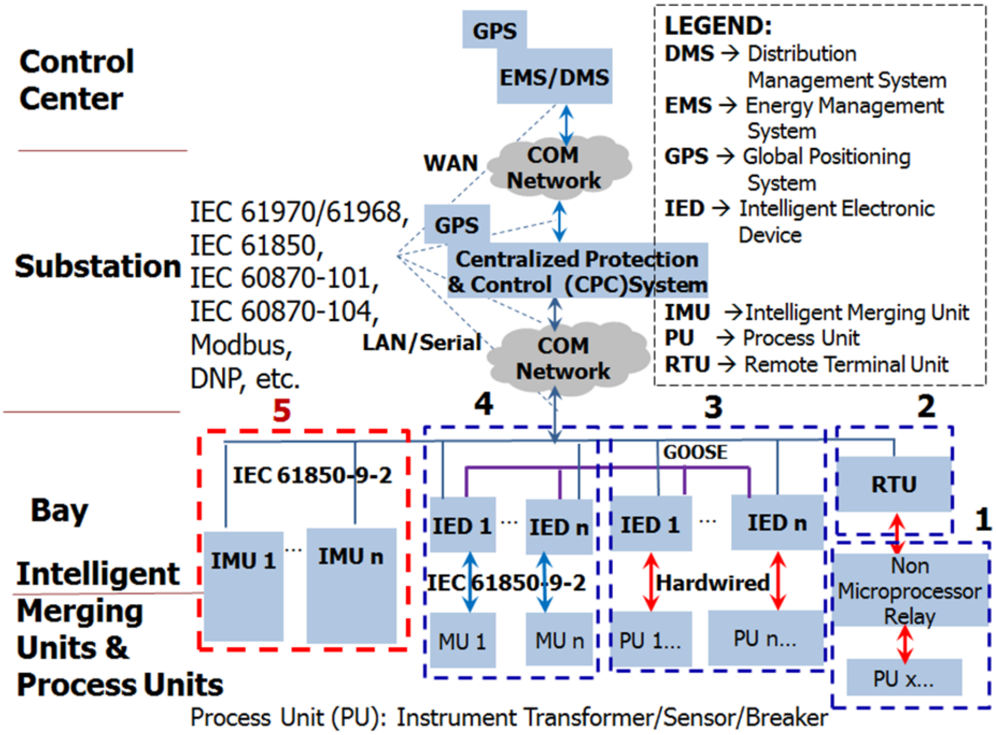

Control Center
Substation
Bay
Intelligent Merging Units & Process Units
GPS
EMS/DMS
WAN
COM Network
IEC 61970/61968, IEC 61850, IEC 60870-101, IEC 60870-104, Modbus, DNP, etc.
GPS
Centralized Protection & Control (CPC)System
LAN/Serial
COM Network
LEGEND:
DMS → Distribution Management System
EMS → Energy Management System
GPS → Global Positioning System
IED → Intelligent Electronic Device
IMU →Intelligent Merging Unit
PU → Process Unit
RTU → Remote Terminal Unit
5
4
3
2
1
IEC 61850-9-2
IMU 1
...
IMU n
IED 1
...
IED n
IEC 61850-9-2
MU 1
MU n
GOOSE
IED 1
...
IED n
Hardwired
PU 1...
PU n...
RTU
Non Microprocessor Relay
PU x...
Process Unit (PU): Instrument Transformer/Sensor/Breaker

Figure 10. Evolution of protection and control system leading to CPC, adapted from [24].

The report compares the traditional approach with CPC in section 4.1.The section 4.2 discusses the existing technologies that are the backbone of various CPC architectures described in section 4.3 and supported by advancement in communication technologies discussed in section 4.4. Reliability and cost analysis of various CPC architectures are discussed in section 4.5 while testing of CPC systems are covered in section 4.6. Section 4.7 discusses some of the advanced applications possible today with the application of CPC.

4.1 Comparison Between Traditional and CPC Approach

Traditional approach refers to all possible technologies – electromechanical, solid-state and IED or a combination of the above technologies applied on a per bay basis. Traditional protection and control within a substation is compared with CPC approach in Table 1.

Table 1. Comparison between traditional and CPC approach.

Feature	**Traditional Approach**	**CPC Approach**
Relay Asset Management	Many relays need to be separately identified, specified, configured, tested, and maintained along with separate records for each device.	A limited number of devices need to be identified, specified, configured, tested, and maintained along with separate records for each device.
Device Management	Each protection IED in a substation typically has numerous configuration choices to enable various features. Firmware versions must be tracked and updated periodically.	A reduced count of devices makes management easier and also the feature set is reduced and limited compared to traditional methods.
Maintenance	Routine maintenance can be frequent and requires experienced and well-trained staff along with expensive calibrated testing equipment. P&C IED maintenance per bay is easily achieved due to separate IEDs per bay.	Limited maintenance is required as the entire substation P&C system uses fewer physical devices. Although, experienced and well-trained staff are still required for maintenance. More robust and reliable systems can be engineered at a lower cost depending on substation size. P&C IED per bay does not exist, and hence independent per bay maintenance is an avoidable challenge.
Security	Multitude of protection IEDs provides more access points for cyber threats.	Very limited number of access points which can also be managed better.
Interoperability	Disparate protocols and difficult to standardize. Modifications to the substation automation system can be complicated.	Capitalizes mainly on the IEC61850 technology and can be more easily adopted than the distributed protection IED model. User requirement of engineering knowledge such as "GOOSE" messaging configuration between IEDs will not be required as it will be internal to the system.
Substation Master Interface	Depending upon the technology, the protection system may have no communication interface with an RTU or data concentrator. More recent technologies have protection IEDs tightly integrated into a substation automation system to transfer data in and out of the substation with limited intelligence.	The CPC becomes the "Gatekeeper" of Device Dynamic Models. Relays are ubiquitous. This provides a master intelligent node for substation-to-substation interaction. Collected data is reduced to information via the dynamic state estimation. Information is exchanged between substations, with control center and downstream intelligent devices versus raw data; tremendous reduction in communication needs.

One of the challenges of CPC approach is the aggregation of functionality which can reduce flexibility for operation and maintenance of the equipment based on present practices as discussed in [26]. The implementation of CPC approach will require a paradigm shift in the way we design, manufacture, install, test, operate and maintain a protection and control system.

4.2 Existing Technologies Supporting CPC

Sensors are the front-end interface of CPC with the process, the power system. Recent advancements in sensor technology make a CPC solution more attractive with the use of appropriate merging units. Advancement in low-cost high-performance computing platforms makes them very attractive for the application of CPCs. Standardized high reliability communication technology can help the implementation of CPC architecture which will be driven by many factors: reduction in Capital Expenditure (CapEx) including the wiring, Operation Expenditure (OpEx) including easy replacement of hardware at the end-of-useful life [25] and seamless upgrade of firmware without any downtime to name a few.

4.2.1 Optical Current and Voltage Sensors

Modern developments in fiber-optics technology and advancements in the associated electronic devices have resulted in the development of non-conventional instrument transformers. One of the non-conventional current transformer designs takes advantage of the Faraday Effect [27]. The basic approach is that two linearly polarized beams are generated and are applied to a fiber optic that takes them to the conductor level. The linearly polarized beams are converted to circular polarized beams, one to a left circular polarization beam and the other to a right polarized beam. The fiber optic takes the circular polarized beams around the conductor several times. As the beams travel through the magnetic field produced by the current, one of the beams is accelerated and other is decelerated; the acceleration and deceleration depend on the intensity of the magnetic field. The circular polarized beams are converted back to linear polarized beams and are sent back to the sensing equipment at the ground level. The change of phase between the beams are measured and then translated to the level of current in the conductor.

One of the non-conventional electro-optic voltage transformer uses the Pockels cells. The basic principle is that when a circular polarized beam passes through the cell, the polarization changes to elliptical polarization. The change of polarization depends on the intensity of the electric field in which the Pockels cell is placed.

4.2.2 Rogowski Coils as Current Sensor

Rogowski coils operate on the same magnetic-field principles as conventional iron-core current transformers (CTs). The main difference between Rogowski coils and CTs is that in the Rogowski coil-based solutions secondary equipment measures output voltages that are scaled time derivative di(t)/dt of the primary current, while in the CT-based solutions, secondary equipment measures secondary currents that are proportional to the primary current. The phase angle between the secondary voltage and primary current is 90°. The reason why the secondary voltage is measured is because Rogowski coils are wound using air-core material (relative permeability is equal one, $\mu r = 1$), the result being that the mutual coupling between the primary conductor and the secondary winding is much smaller than in CTs. The Rogowski coil output voltage is small (mV range during normal operation and several volts during faults), so they cannot drive current through low-resistance burden like CTs are able to drive. Rogowski coils can provide input signals for microprocessor-based devices that possess a high input resistance. The Rogowski coil low-output signal is safer for people and secondary equipment, even when high currents and voltages exist on the primary side. An open circuit or short-circuit in the signal cable will cause no hazards or damage. Signal processing is required to extract the power frequency signal for phasor-based protective devices and microprocessor-based equipment must be designed to accept these types of signals. An important advantage over CTs is the Rogowski coil linear performance characteristic since the air-core material cannot saturate.

Rogowski coils may achieve high accuracy (up to 0.1%). The same sensor can be used for both protection and metering [28, 29]. Rogowski coils are classified as low-power current sensors and requirements are specified by Standards [30, 31, 32]. IEC 61869-10 standard, "Specific requirements for low-power passive current transformers," is under development. IEEE Std. C37.235™-2007 [33] provides guidelines for the application of Rogowski coils used for protective relaying purposes.

4.2.3 Merging Unit

The development of centralized substation protection and control systems is possible today based on the developments of the object models and interfaces defined in the IEC 61850 standard. A function in an IEC 61850 based protection and control system can be local to a specific primary device (distribution feeder, transformer, etc.) or distributed and based on communications between two or more devices over the substation local area network.

IEC 61850 defines several ways for data exchange between IEDs that can be used for different forms of distributed protection and other applications. They introduce a new concept that requires a different approach and technology in order to define the individual components of the system, as well as the overall distributed applications. IEC 61850 defines several different interfaces that can be used for various substation applications. They may use dedicated or shared physical connections - the communications links between the physical devices. The allocation of functions between different physical devices defines the requirements for the physical interfaces, and in some cases may be implemented into more than one physical LANs. The functions in the substation can be distributed between IEDs on the same, or on different levels of the substation functional hierarchy – Station, Bay or Process. They can also be implemented in a central substation computer.

These levels and the logical interfaces are shown by the logical interpretation of Figure 11.

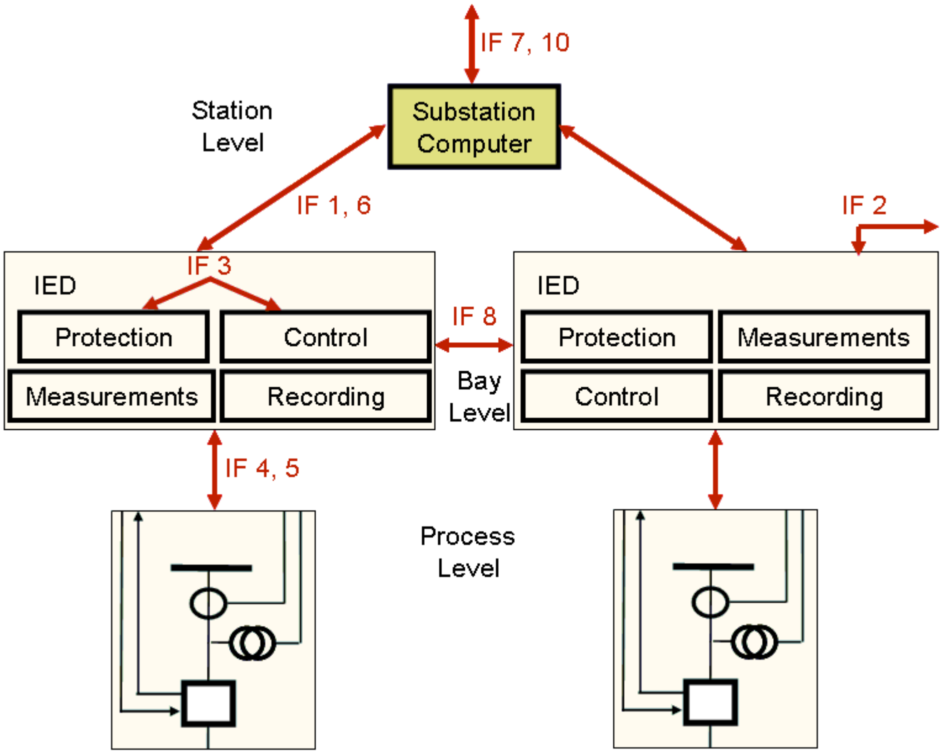


Figure 11**.** Logical interfaces in IEC 61850.

The logical interfaces (IFs) of specific interest to protection applications shown above are defined [34] as:

IF4: CT and VT instantaneous data exchange (especially samples) between process and bay level

IF8: direct data exchange between the bays especially for fast functions like interlocking

The first one is used typically for the so called process bus applications, while the second defines the substation bus communications.

A significant improvement in functionality and reduction of the cost of centralized substation protection and control systems can be achieved based on the IEC 61850 based communications as described below.

Non-conventional instrument transformers with digital interface based on IEC 61850-9-2 [35] (Process Bus) result in further improvements and can help eliminate some of the issues related to the conflicting requirements of protection and metering IEDs.

The interface of the instrument transformers (both conventional and non-conventional) with different types of substation protection, control, monitoring and recording equipment is through a device called Merging Unit. This is defined in IEC 61850-9-1 as:

“Merging unit: interface unit that accepts multiple analogue CT/VT and binary inputs and produces multiple time synchronized serial unidirectional multi-drop digital point to point outputs to provide data communication via the logical interfaces 4 and 5”.

Existing Merging Units have the following functionalities:

- Signal processing of all sensors – conventional or non-conventional
- Synchronization of all measurements – 3 currents and 3 voltages
- Analogue interface – high and low level signals
- Digital interface – IEC 60044-8 or IEC 61850-9-2

It is important that merging units are able to interface with both conventional and non-conventional sensors in order to allow the implementation of the system in existing or new substations. The merging unit has several function blocks as can be seen from Figure 12.

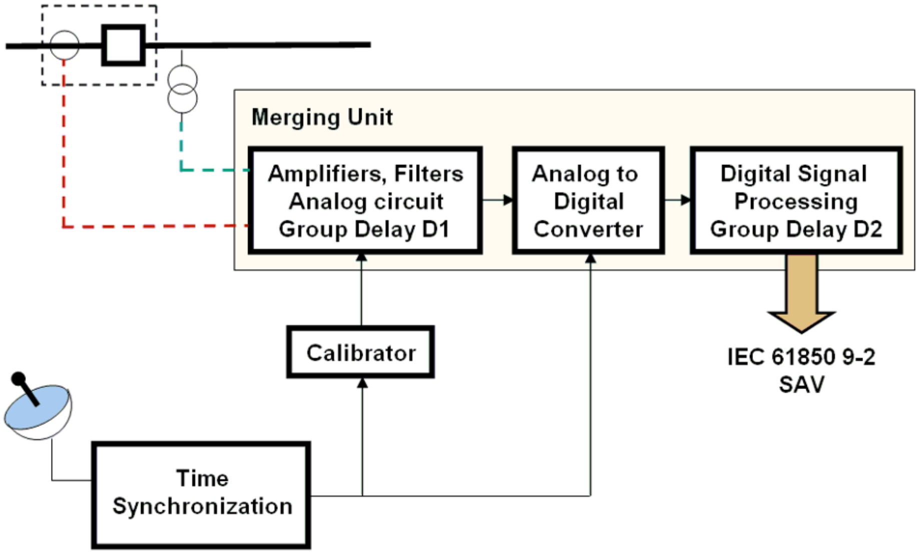

Merging Unit
Amplifiers, Filters Analog circuit Group Delay D1
Analog to Digital Converter
Digital Signal Processing Group Delay D2
IEC 61850 9-2 SAV
Calibrator
Time Synchronization

Figure 12. Merging unit block diagram.

The merging unit can be considered the analog input module of a conventional protection or other multifunctional IED. The difference is that in this case the substation LAN serves as the digital data bus between the input module and the protection or functions in the device. The merging unit and protection functions are located in different physical devices, just representing the typical IEC 61850 distributed functionality.

It requires precise time synchronization that can be achieved using different methods, with Precision Time Protocol (PTP) based solutions being the preferred method for the future applications. Existing IEC 61850 based merging units have been designed according to an IEC 61850 9-2 profile defined by the UCA International Users Group "Implementation Guideline for Digital Interface to Instrument Transformers Using IEC 61850 9-2" (known as IEC 61850 9-2LE).

IEC TC 38 is currently completing the development of IEC 61869 Instrument Transformers Part 9: Digital interface for instrument transformers.

4.2.4 Remote I/O and Process Interface Unit/Device

The remote I/O module (RIO) is intended to be the status and control interface for primary system equipment such as circuit breakers, transformers, and isolators. RIOs under IEC 61850 may support only GOOSE publish and subscribe communications, or may also support MMS client and server communications.

The process interface unit/device (PIU/PID) combines a MU and a RIO into one device. The PIU/PID can publish analog values and equipment status, and accept control commands for equipment operation. From an installation standpoint, a PIU/PID can make more sense in many applications than separate MUs and RIOs.

4.2.5 Intelligent Merging Unit

The intelligent merging unit (IMU), shown in Figure 10, adds RMS-based (simple to derive from sampled values) overcurrent and overvoltage back-up protection functions in a PIU/PID to prevent damage to the related primary equipment in the event of total communication failure between the IMU and CPC during abnormal system conditions. This type of device is not yet available and it is expected to evolve with MU and PIU/PID technology irrespective of CPC application.

4.2.6 High-Performance Computing Platform

The optical isolation between IMUs and the CPC, shown in Figure 10, enables off-the-shelf hardware use for the CPC, which is very important for the deployment of the CPC. Most protection functions from distributed IEDs within a substation are integrated into the CPC. Advancement in low-cost, high-performance rugged computing platforms combined with the availability of standardized high-reliability communication technologies make them very attractive for the CPC applications. A high-performance computing platform based on server technologies for the CPC is shown in Figure 13 [24]. Time synchronization between the CPC (servers in Figure 13) and IMUs is achieved using precision time protocol (PTP) as per IEEE 1588-2008 (v2).

One of the main advantages of using a high-performance computing platform like servers is the efficient management of end-of-life of hardware. Server technology is used by many industries across various technology areas, so the wide availability of next generation of hardware would appear to be guaranteed at a competitive price and users would have much wider choices for hardware supplier.

Use of off-the-shelf hardware for CPC like that used in energy management system will also be very helpful to the IED suppliers. They can focus on developing specialized CPC application software that can run on commercially available standard platforms. In addition, availability of standardized high-performance computing platform opens the opportunity for development of complex protection and control algorithms necessary for the future grid, to accommodate the changing power system characteristics.

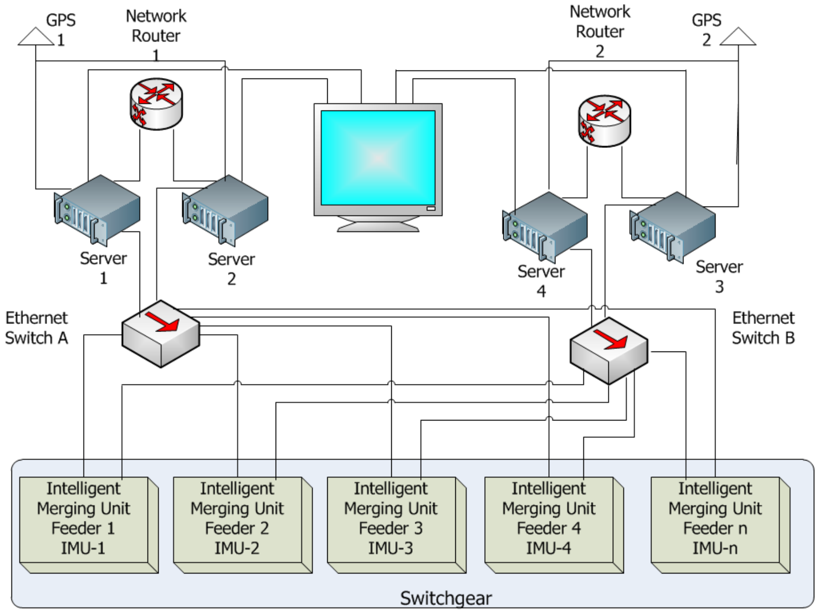


Figure 13**.** Server based CPC system [24].

CPC has to meet applicable standards for substation environment, such as IEEE 1613 and IEC 61850-3:2013. Electrical isolation of the CPC via optical fiber cables for communications is beneficial in this respect. However, a CPC's power supply and other peripheral connections have to withstand the substation environment.

4.2.7 Advancements in Communication Technology

Substation protection and control systems require reliable, secure communications infrastructure which is also true for CPC architectures. These are mission-critical systems that have to process real time events on a millisecond level for protections and control operations. Many of these modern communications networks rely on packet based Ethernet messaging. Applications using digital messages to exchange binary protection signals require that networks never drop more than four consecutive packets or take longer than 15 milliseconds to reconfigure. Applications using digital messages to exchange analog protection signals require that networks never drop more than three consecutive packets to bump-less calculation of mission critical algorithms.

There are a number of existing standard redundant protocols used in substation Ethernet LANs that provide network fault detection, isolation, and restoration for resiliency including IEC 62439-1 Spanning Tree Algorithm (STA) using Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), and Media Redundancy Protocol (MRP) to name a few. Other emerging redundancy protocols without fault detection but that help provide zero (0) second recovery time and zero-packet loss include IEC 62439-3 protocols called High-availability Seamless Redundancy (HSR) and Parallel Redundancy Protocol (PRP) [36]. According to the IEC 61850 Ed 2, the applications using the process bus Sampled Value (SV) and GOOSE messaging require bump-less calculations and low loss communication that can be achieved in HSR/PRP networks. Other examples of future potential technologies/protocols are Time Sensitive Networks (TSN) based on IEEE 802.1 series with Deterministic Ethernet (DE); Software Defined Network (SDN) based on IEEE projects P1903 and 802.1CF; etc.

One of the main criteria for selecting CPC communication architecture is the level of redundancy, overall cost (Capital Expenditures (CapEx), Operation Expenditures (OpEx)) and performance such as switchover time, latency, bandwidth and processing power.

HSR/PRP networks provide:

- Reliability in critical applications
- Seamless switchover, zero-frame loss
- Zero-Loss redundancy
    - No single point of failure
    - Zero-time recovery
    - No packets loss (minimum latency)
- Zero down time
    - devices can be removed from network without traffic loss
- Support for IEEE 1588 clock synchronization

The basic principle of HSR/PRP protocol is that the source node duplicates packets and sends them in redundant directions - across the ring in case of HSR or to both LANs in case of PRP, as in Figure 14. The first packet that reaches the destination will be accepted and the duplicate packet will be rejected. Detailed description of the protocol can be found in [36].

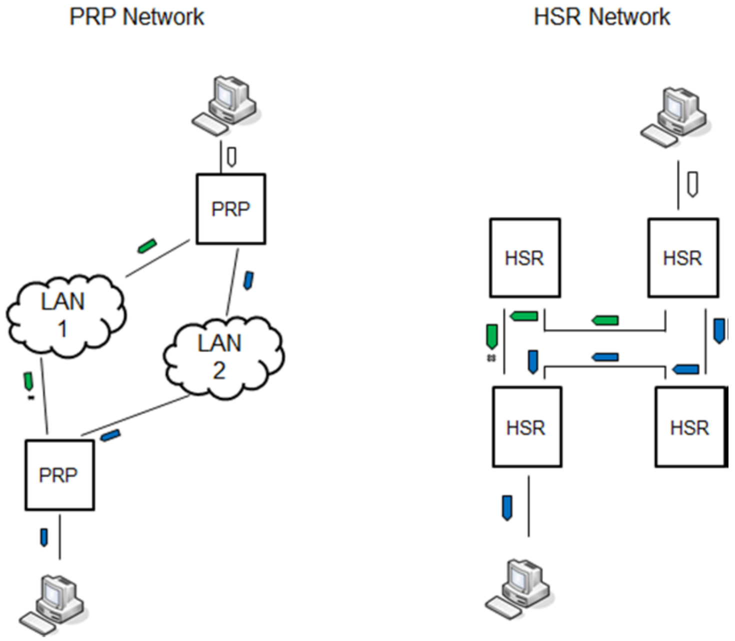


Figure 14. Conceptual diagrams of PRP and HSR networks.

4.2.8 Advancements in Time Synchronization Technology

Time synchronization service is required for various existing and emerging protection and control applications. Two types of time synchronization can be used: synchronization to a relative time and synchronization to an absolute time. Synchronization to a relative time implies synchronization of two or more devices, possibly in a centralized architecture, to a common time that can be different from the absolute time.

Synchronization to an absolute time implies synchronization of two or more devices to a reference of the absolute time, most commonly to a reference of Coordinated Universal Time (UTC). Synchronization to UTC in turn is often achieved using clocks with Global Positioning System (GPS) receivers and time distribution interfaces such as IRIG-B and Precision Time Protocol (PTP). Recently, the US government discussed a proposal to use Enhanced Loran (eLoran) system as a backup to GPS for navigation and time distribution services [37, 38].

Most communication-assisted protection and control systems also require time synchronization to relate and align data from various locations. Communication and time synchronization architectures can be the same, partially overlapping or completely different and independent. Various time synchronization methods and technologies can be used as well. For relative time synchronization various proprietary methods have been used. These are commonly based on exchanging messages with time information between devices, and measuring propagation delay. These methods assume delay symmetry in transmit and receive direction. Terms like "ping pong" or "echo"/ "echo timing" are used for these methods.

It should be noted that methods used for synchronization to an absolute time fulfill requirements for synchronization to a local time as well. For synchronization to an absolute time, GPS has been commonly used to acquire UTC time. To distribute time from GPS receiver to other devices in a substation, Inter-range instrumentation group time codes, commonly known as IRIG time codes are often used [39]. This method requires dedicated cabling, time code signals can be sent over copper coaxial cabling with BNC connectors or over fiber optics that offers advantages of immunity to electromagnetic interferences. Physically signals can be transferred as DC level shift or amplitude modulation at 1 kHz carrier. Other time distribution methods include Network Time Protocol (NTP), Simple Network Time Protocol (SNTP), DNP 3.0, etc. These methods, however, do not provide high time accuracy of 1 microsecond, required for some protection and control applications.

IEEE 1588 Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems specifies Precision Time Protocol (PTP) for time distribution over Ethernet with sub microsecond time accuracy. The second version of this standard published in 2008, specifies multiple ways of achieving the above goal [40]. It introduced the concept of a profile, a subset of available variants, that industries are required to generate to meet requirements of their applications.

IEEE C37.238-2011 Standard Profile for Use of IEEE 1588™ Precision Time Protocol in Power System Applications specifies a PTP profile for power industry [41]. Using Ethernet-based synchronization permits reduction in the number of GPS receivers required and eliminates the need for architecture and cabling dedicated only to time synchronization, such as IRIG-B cabling**.** In addition to protocol details such as Layer 2 communication, multicast messaging, IEEE C37.238-2011 also specifies performance requirements. 1 microsecond time accuracy is expected at the input of the end device located 16 communication hops away from the time source, connected to GPS, shown in Figure 15.

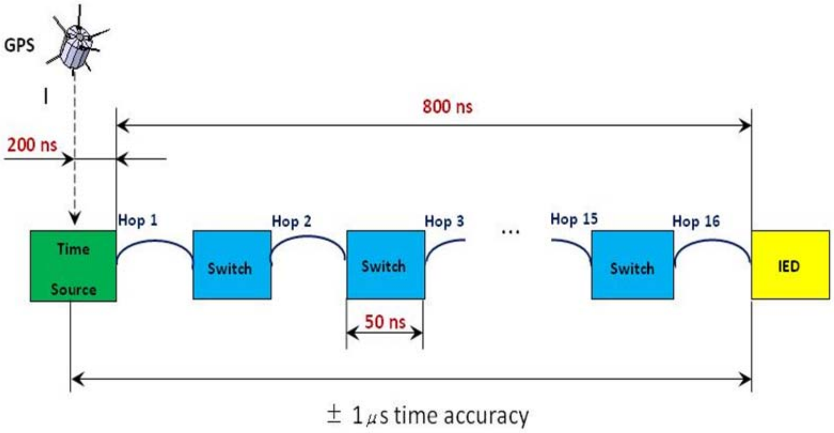


Figure 15. Time synchronization performance requirements specified by IEEE C37.238-2011.

The ongoing IEEE C37.238-2011 revision project led to joint work with IEC TC57 WG10 which resulted in generation of a common Level 1 profile – IEC PAS 61850-9-3: Precision time protocol profile for power utility automation. Once it is approved, it will provide a single common base profile for the power industry; benefiting users, implementers and the industry [42].

Various synchronization methods could be used in the same system simultaneously. Figure 16 provides an example of time distribution architecture with the use of multiple time synchronization technologies. Communication and time synchronization architectures can be the same, partially overlapping or completely different and independent. Figure 17 provides an example of synchrophasor-based application where communications and synchronization are different: GPS receivers are installed in each end device.

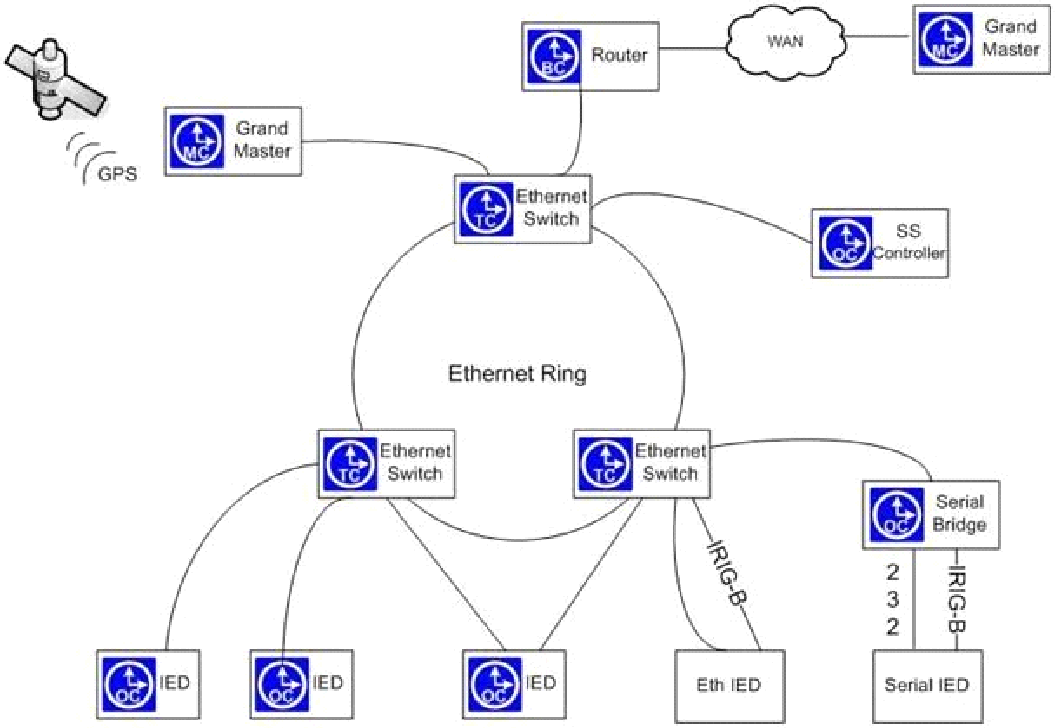


Figure 16. Example of time distribution architectures with the use of various technologies.

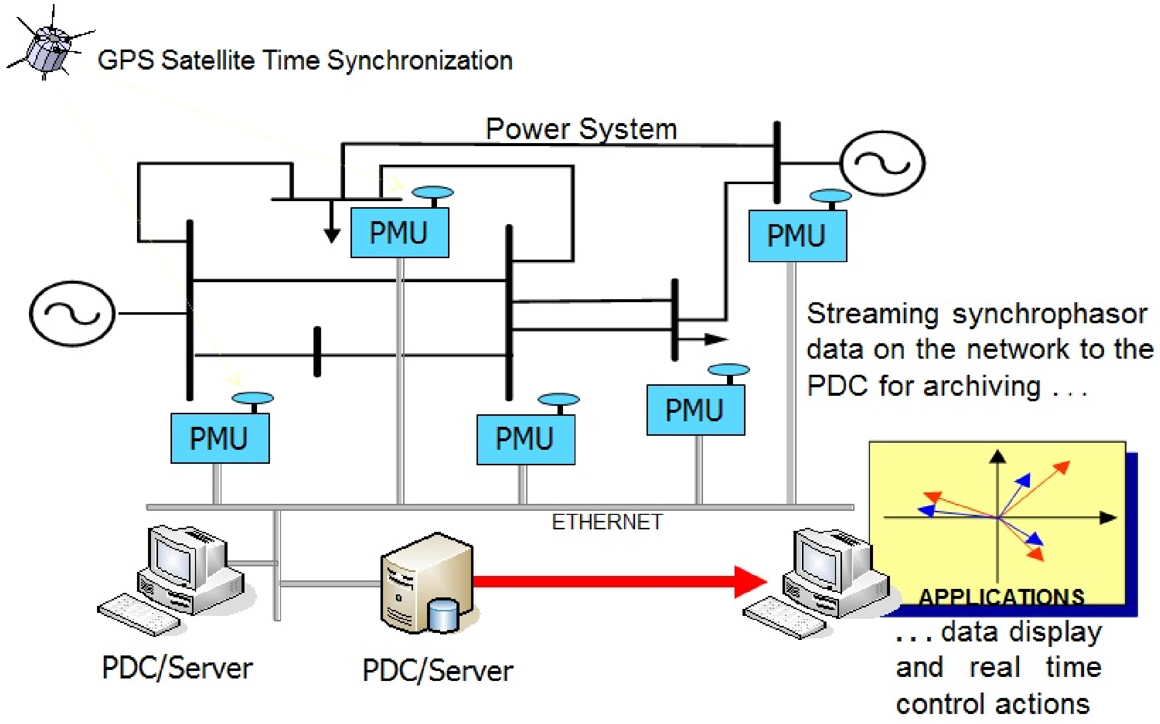

GPS Satellite Time Synchronization
Power System
PMU
PMU
PMU
PMU
PMU
Streaming synchrophasor data on the network to the PDC for archiving . . .
ETHERNET
APPLICATIONS
. . . data display and real time control actions
PDC/Server
PDC/Server

Figure 17. Example of different architectures used for communications and time synchronization.

Using same and different architectures for communication and synchronization has benefits and challenges. The use of same architecture eliminates the need for special devices/wiring used for synchronization only. Redundancy, however, needs to be addressed in this case. Redundancy protocols such as Parallel Redundancy Protocol (PRP), High Availability Seamless Redundancy (HSR) or use of separate independent back up communication network address these challenges.

4.3 Possible CPC Architectures

The implementation of a CPC System within a substation is the result of lessons learned through the evolution of the different technologies currently used in the industry.

Since protection and control is evolving and the concept of CPC is not entirely a new concept, its full implementation will be the result of a learning process. This section introduces some possible architectures that will allow the use of new technologies.

CPC is considered to be a high-performance computing platform capable of providing protection, control, monitoring, communication and asset management functions. The specific hardware/software architecture/configuration of CPC system is implementation dependent and outside the scope of this document. However, a general guideline for hardware selection and functions that should be available in CPC is discussed in section 4.3.1, based on the architectures discussed in this section.

In this sub-section, major CPC architectures/configurations are identified with the introduction of substation communication networks (e.g. stations bus, and process bus). Please note that further variations of these architectures may exist, which are not discussed here for brevity.

Cyber security (e.g. Firewalls) and each level redundancy are not shown to avoid complexity. The term redundant CPC and back-up protections are considered in the following discussions which does not exclude the use of redundant CPC as another main CPC. In this report, the term “redundant” refers to hardware/device level redundancy whereas the term “backup” refers to functional backup located in different physical devices. Further coordination between CPC systems should be considered while designing the system. Each main/redundant CPC system may have its own redundancy and its management. Peer substation and control center may be connected to CPC (RTU/gateway function inside CPC) over station bus – with cyber security (e.g. firewall) measures. GPS based time synchronization is connected to the CPC in these diagrams, whereas, time synchronization of other devices such as IEDs and Merging Units (MUs) is not shown, and it can be provided using GPS/IRIG-B or IEEE 1588 PTP.

CPC Architecture-1

Figure 18 illustrates the first possible architecture, in which IEDs at bay level are interfaced with process level equipment (i.e. instrument transformers and switching) over traditional copper wire. The IEDs are performing primary protection and control functions; and communicating GOOSE, Sampled Values (SV) or Synchrophasors (IEC 61850-90-5 based Routable Sampled Values (R-SV)) to the CPC.

With this architecture, CPC can perform backup (may not be completely independent, as it depends on IEDs ability to communicate the desired information) protection and control (P&C) functions of the entire substation, as well as other substation P&C schemes (e.g. backup of bus/line differential, load shedding, breaker failure, etc.). Individual P&C IEDs at the bay level perform primary (system-A) P&C functions per bay; whereas, the CPC provides all back-up (system-B) P&C functions for the entire substation. This architecture replaces all backup (system-B) P&C IEDs with CPC. There may be more than one CPC (redundant) in this architecture.

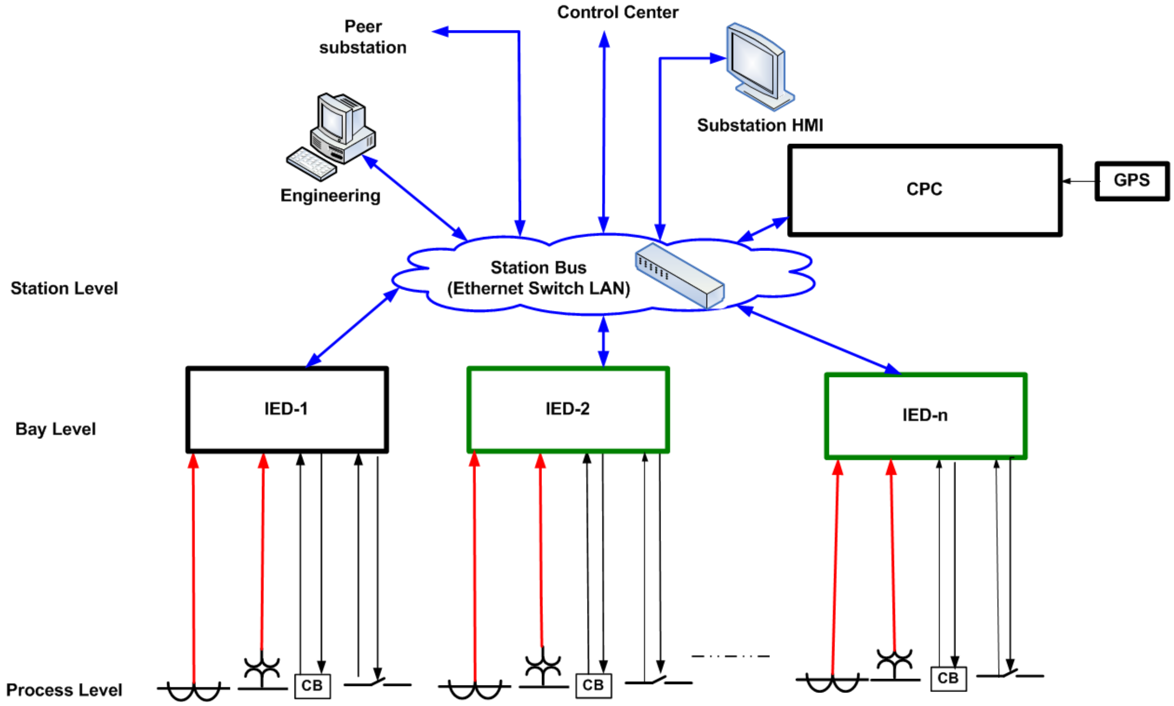


Figure 18. IEDs process input over copper wire and CPC interfaced with IEDs.

CPC Architecture-2

IEDs and CPC may be connected to merging units over multiple point-to-point (unicast) process bus interfaces, as shown in Figure 19. Intelligent Merging Unit (IMU) or Process Interface Unit (PIU) at the process level (in switchyard) is connected to IEDs and CPC over a Point-to-Point (Unicast) connection. The same IMU can be directly interfaced with IEDs and CPCs using SV unicast from IMU to IEDs and CPC; two way GOOSE unicast between IMU and IEDs/CPC. As in Architecture-1, the CPC can perform backup P&C functions of the entire substation, as well as other substation P&C schemes; and hence, CPC replaces all backup P&C IEDs (system-B).

Compared with Architecture-1, Architecture-2 utilizes sample value (SV) directly from IMU at process level, and hence CPC need not be interfaced with bay level IEDs.

Redundant IMU and CPC may exist in this architecture with independent point-to-point connections from IMU to redundant CPC (not shown in this figure).

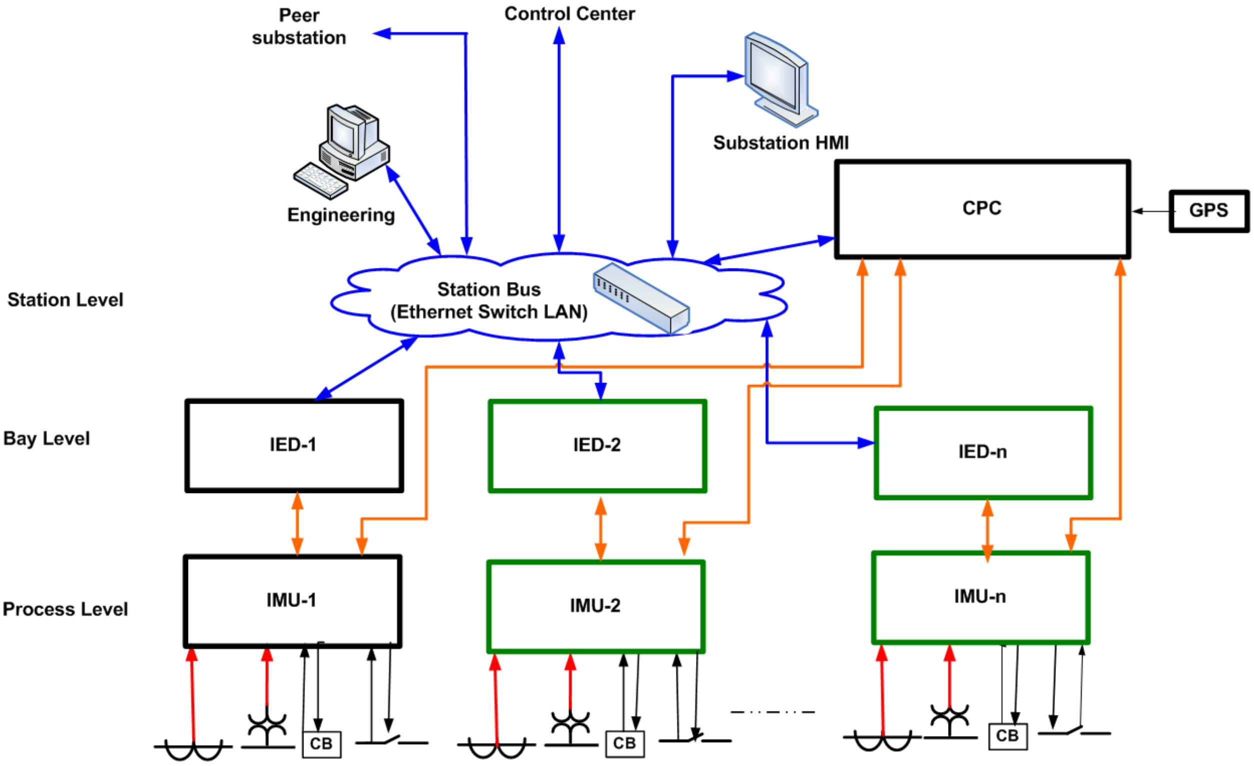


Figure 19. IEDs and CPC connected to merging unit’s point-to-point process bus architecture.

CPC Architecture-3

Figure 20 demonstrates Architecture-3, in which all individual bay level P&C IEDs are replaced by CPCs at station level.

IMUs at process level (in switchyard) are connected to CPCs over Point-to-Point (Unicast) connection. The same IMU may be directly connected to multiple CPCs using SV unicast from MUs to CPC; two way GOOSE unicast among IMUs and CPCs.

Compared with Architecture-2, all P&C functions within a substation are facilitated in each individual primary & backup CPC. There may be more than two CPCs at the station level to further enhance reliability and availability (not shown in this figure).

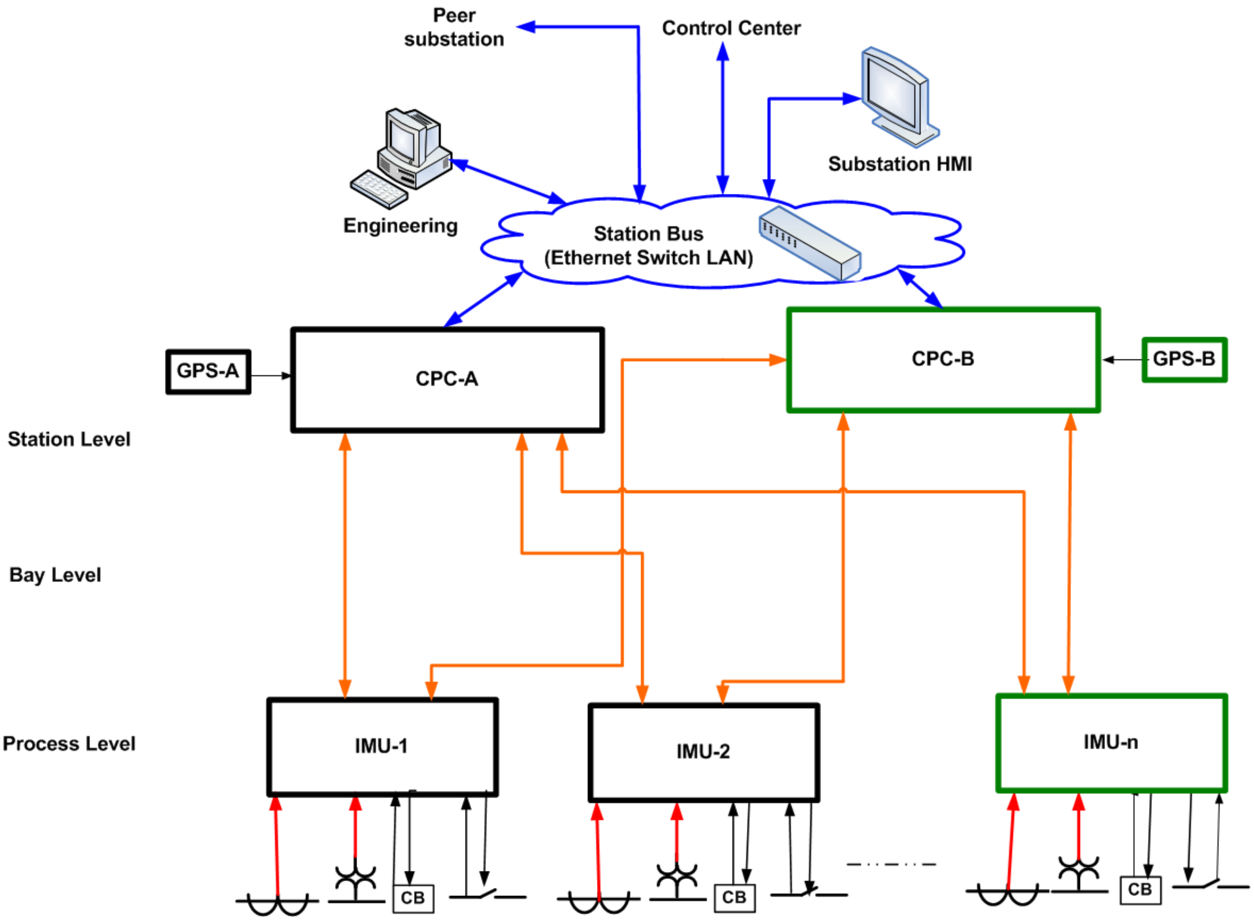


Figure 20. CPCs directly connected to MU over point-to-point process bus architecture.

CPC Architecture-4

Figure 21 illustrates the Architecture-4 with Ethernet switch network at process bus level. In this architecture, IMUs at process level (in switchyard) are able to interface with IEDs and CPC over Ethernet switch (Local Area Network (LAN)) process bus network. Since, the Ethernet switch provides a shared communication network, multicasting of SV and GOOSE streams can be deployed in this case. IMUs multicast SV and GOOSE to IEDs and CPC; and IMU receives multicast GOOSE from CPC and IEDs. Ethernet LAN networks with managed switches facilitate Quality of Service (QoS) using IEEE 802.1Q based VLANs and priority tagging, and redundancy with IEC 62439-3:2012 based Parallel Redundancy Protocol (PRP) or High-availability Seamless Redundancy (HSR) which were described in 4.2.7.

Careful design/engineering considerations should be given to examine performance and availability of process bus communication network. Similar to Architecture-2, in this architecture IEDs performs primary substation P&C functions; whereas, CPC provides redundant P&C functions and/or substation P&C schemes.

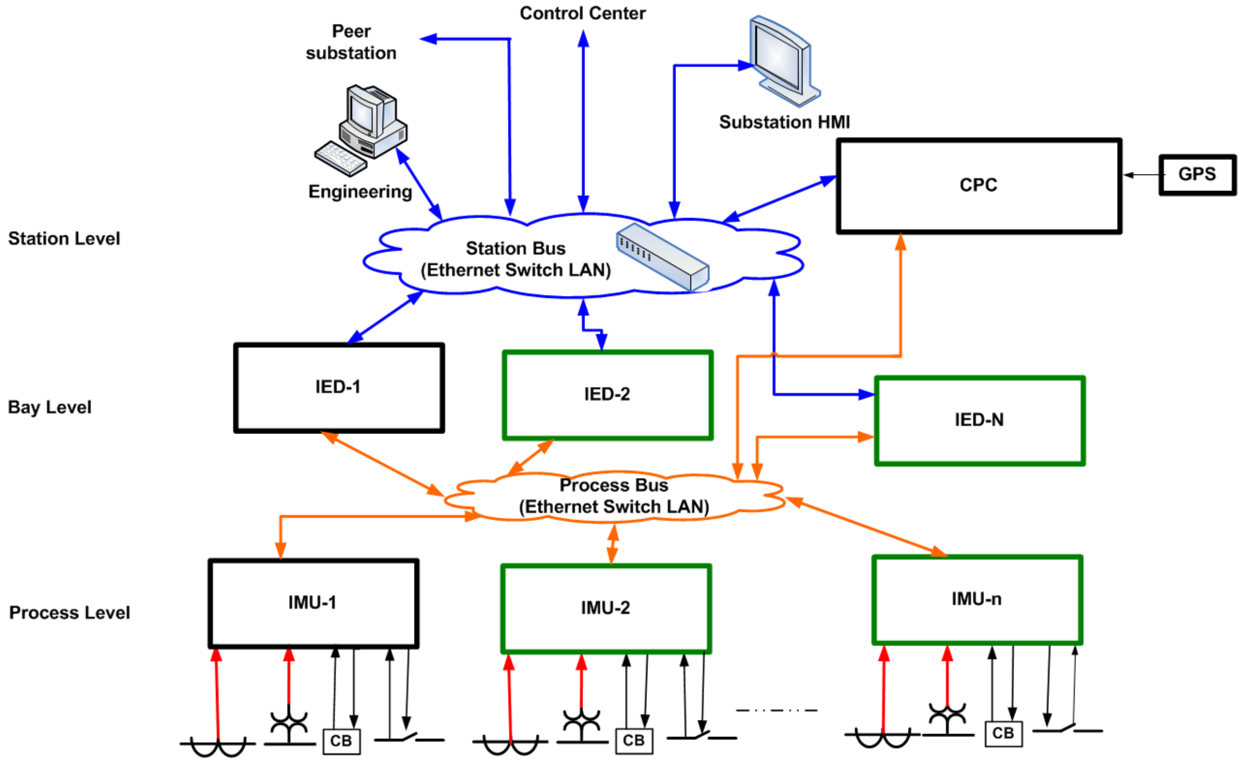


Figure 21. IEDs and CPC are connected to MUs over Ethernet LAN architecture.

CPC Architecture-5

CPC Architecture-5, shown in Figure 22, illustrates the IMUs at the process level (in the switchyard) interfacing with the CPCs over a process bus Ethernet LAN network. IMUs are multicasting SV and GOOSE to CPCs, and each IMU receives multicast GOOSE from CPCs.

Since CPCs perform primary and redundant P&C functions, there may be more than two CPCs at the station level to further enhance the reliability and availability of the entire system. As explained in Architecture-4 on the Ethernet switched network, the shared communication network at the process level requires a careful design and engineering including but not limited to performance and reliability analysis. IMUs at the process level are interfaced with CPCs over the Ethernet switch process bus network.

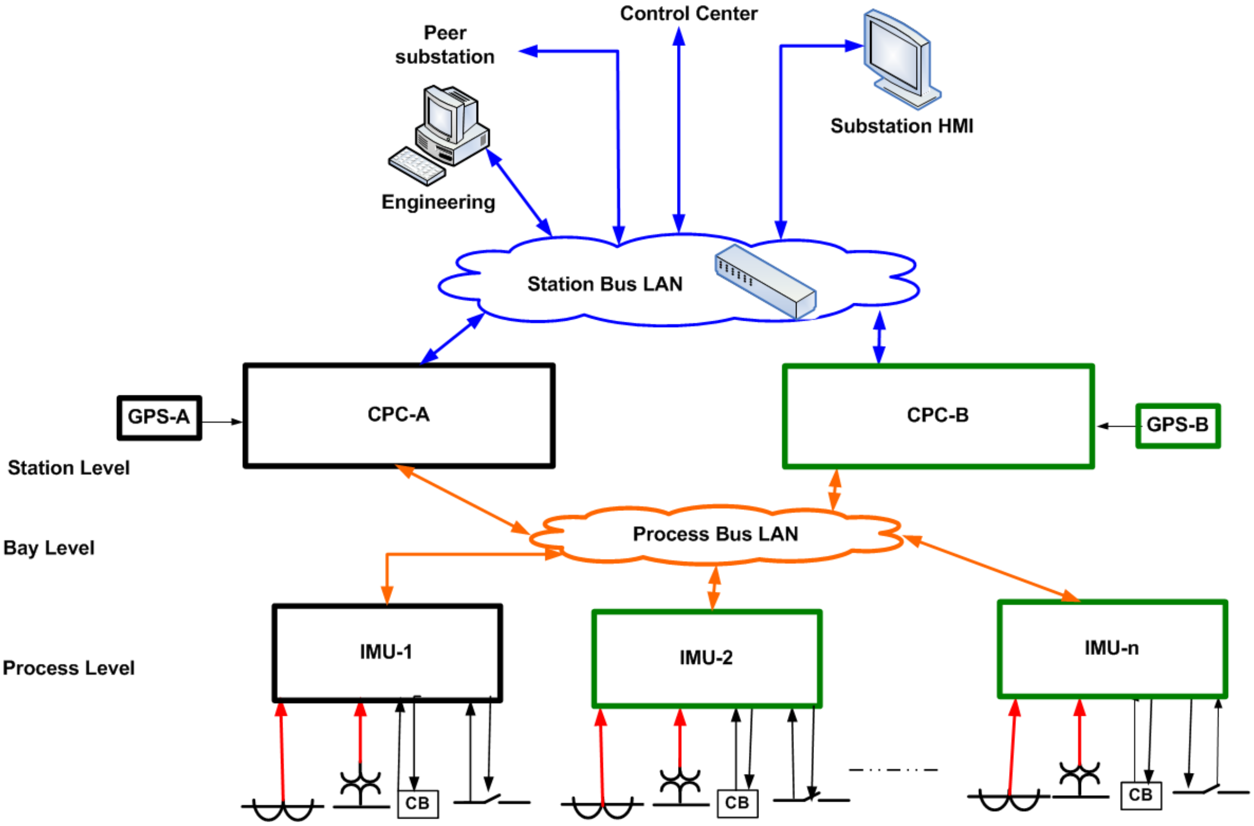


Figure 22. CPCs are connected to MUs over Ethernet LAN architecture.

CPC Architecture-5a

A variation of Architecture-5, Figure 23 demonstrates Architecture-5a with complete redundancy (other Architectures 1 through 4 can have similar redundancy architecture variation) to enhance reliability of the substation P&C system.

Redundant CT/VT secondary and switchgear I/Os are connected to completely redundant IMUs/CPCs (system-B). In addition, IEC 62439-3 proposes network level redundancy architectures (PRP and HSR) with cross connections (not shown in this figure).

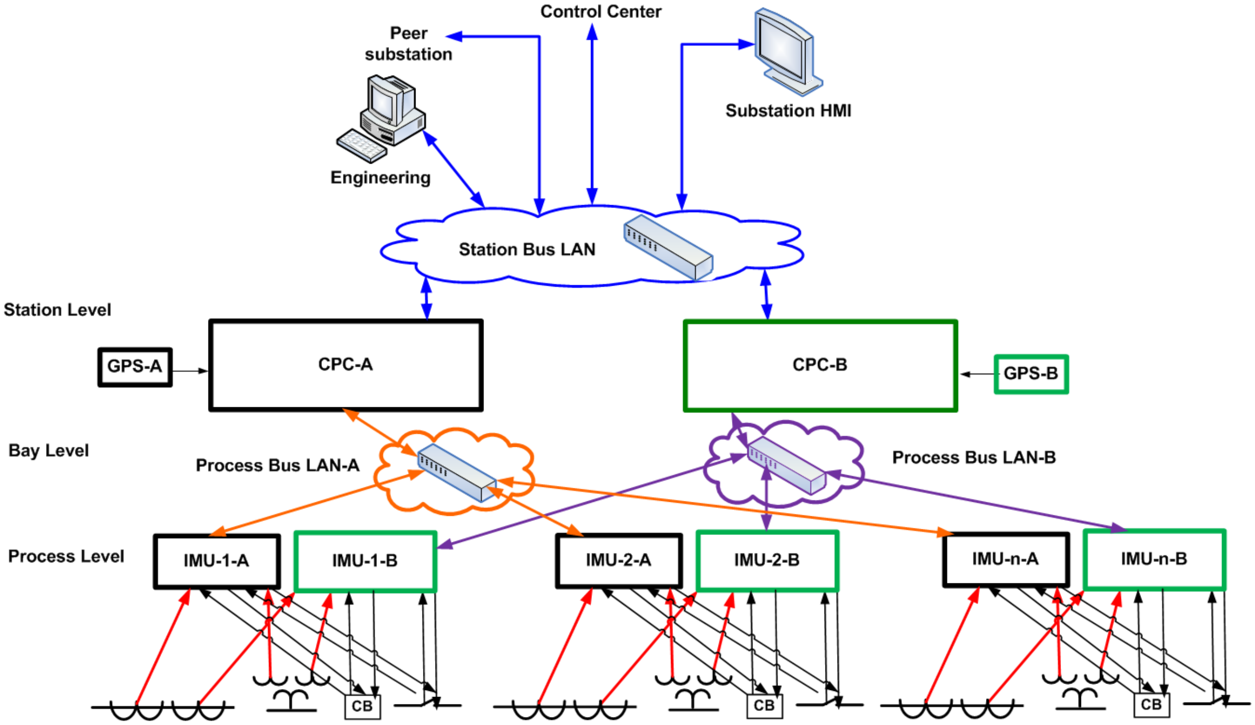


Figure 23. CPCs are connected to MUs over redundant Ethernet LAN architecture.

4.3.1 An Example CPC System

This subsection provides an example CPC system using one of the proposed conceptual architecture-5 for a simple substation with three lines, one transformer and one bus. Redundancy is not considered as in conceptual architecture-5.

As illustrated in Figure 24, IMUs 1 to 6 interface with substation primary equipment. Each CPC (A or B) is interfaced with all IMUs 1 through 6 over the process bus LAN. Therefore, a CPC may be configured to receive inputs (or event redundant inputs) from all of the substation primary equipment (CT/VT measurements, sensor inputs, status inputs, etc.) and to provide outputs (commands, control signals, etc.) to all switchgears through IMUs based on application requirements.

Figure 25 shows the mapping of conventional IED functionalities to the substation CPCs. The substation level CPC is able to perform all or some of the P&C functions which are today performed by several bay level P&C IEDs. A CPC combines several bay level IEDs into one device. For the given substation configuration example, CPCs combine all P&C functions in Line-1, 2, 3 IEDs, Transformer-1 IED and Bus-1 IED. There may be more than one CPC to facilitate hardware redundancy, testing, maintenance, etc.

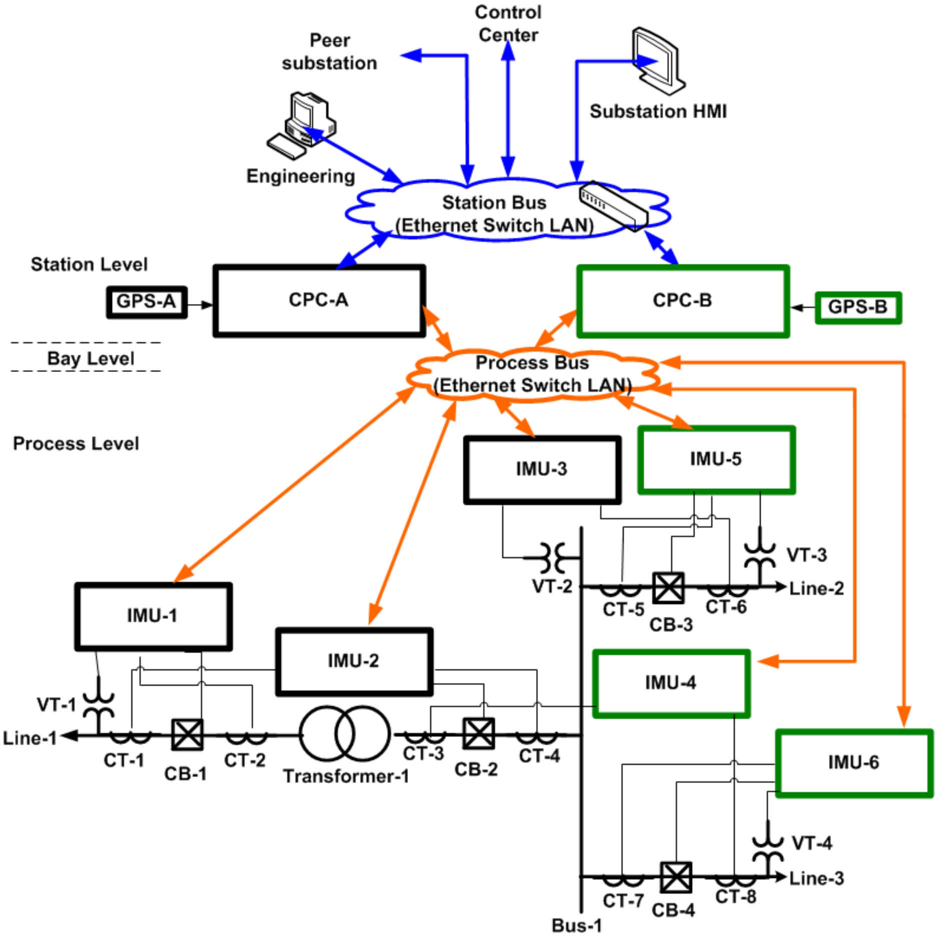


Figure 24. An example of conceptual architecture-5 with one substation configuration.

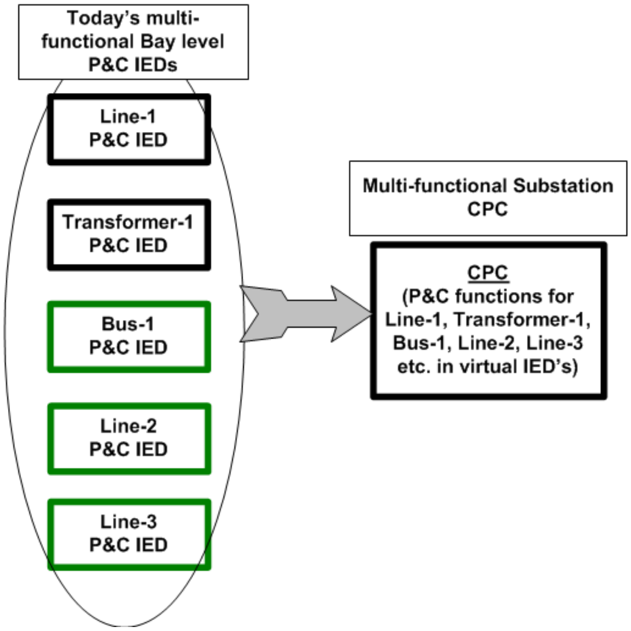

Today's multi-functional Bay level P&C IEDs
Line-1 P&C IED
Transformer-1 P&C IED
Bus-1 P&C IED
Line-2 P&C IED
Line-3 P&C IED
Multi-functional Substation CPC
CPC
(P&C functions for Line-1, Transformer-1, Bus-1, Line-2, Line-3 etc. in virtual IED's)

Figure 25. Envisioned substation CPC for the example substation configuration.

4.4 Communication Architecture for CPC

As described in 4.2.7, Parallel *Redundancy Protocol* (PRP) and *High-availability Seamless Redundancy* (HSR) networks [36] are considered to be the best standardized option available for substation CPC communications architectures.

Key elements of HSR/PRP networks are:

SAN	Singly Attached Node
DAN{H,P}	Doubly Attached Node using HSR or PRP
RedBox	Device attaching single attached nodes to a redundant network
QuadBox	Quadruple port device connecting two peer HSR rings, which behaves as an HSR node in each ring and is able to filter the traffic and forward it from ring to ring.

The CPC communications infrastructure can be implemented using different HSR/PRP topologies. Each process and station bus can be implemented as PRP, HSR or a combination of both as mentioned in Table 8 of [43] and is influenced by many factors:

Data Bandwidth, network throughput and the CPC computational performance

- The process bus data bandwidth requirement can be quite high when carrying SV data. For example, SV traffic at 4.8MHz transmission rate limits the number of devices on one 100Mb/s Ethernet segment to 6 as shown in Annex A of [35]. The obvious choice to remove this bottleneck is to increase line rate to 1 GB/s.

Level of redundancy

- For example, segmenting HSR networks into multiple rings increases overall network resiliency.

Latency

- It's always better to use hardware implementation of HSR/PRP to keep latencies low. Latencies also can be reduced by splitting HSR rings to minimize the number of devices in one ring and use QuadBoxes to interconnect the rings.
- CapEx saving can be achieved by simplifying network topologies and use lower bit rates and higher device count in one HSR ring if latency requirements are relaxed.

Greenfield or retrofit installation

- To preserve investment in case of retrofit, less optimum solution that still complies with performance criteria may be implemented. For example, if switches are already used at the bay level then it makes sense to duplicate LANs and use PRP for process bus (Figure 26).

Segregation requirement of station and process buses

- One redundant PRP network between IMUs and CPC [Figure 27] if segregation is not required.
- If segregation is required then topologies shown in Figure 26, Figure 28 and Figure 29 or some variation of them should be considered.

These principles are demonstrated in a few possible CPC network architectures presented in Figure 26 to Figure 29. Process bus is implemented as PRP network and station bus as a regular LAN (or HSR/PRP for better performance) in Figure 26. In this figure, there are two PRP LANs, A & B - same applies to other figures. The single PRP network for both process and station buses is shown in Figure 27. The architectures in Figure 26 and Figure 27 represent process and station bus topologies primarily based on PRP networks.

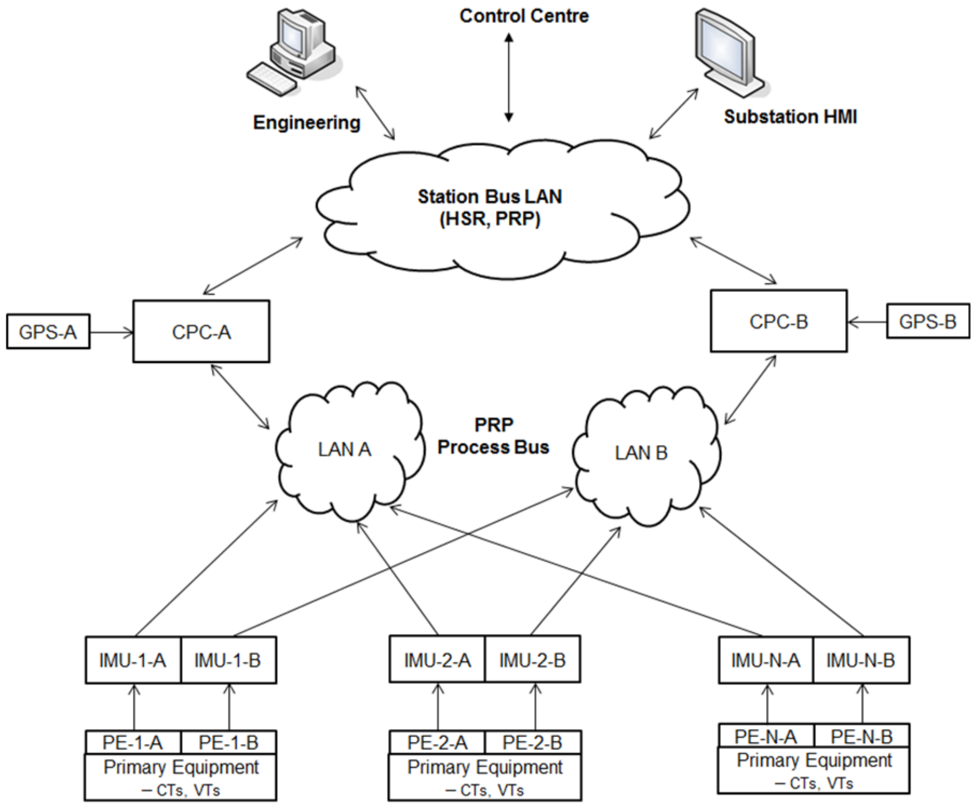


Figure 26. Process bus PRP architecture: CPCs are connected to IMUs over redundant Ethernet LANs.

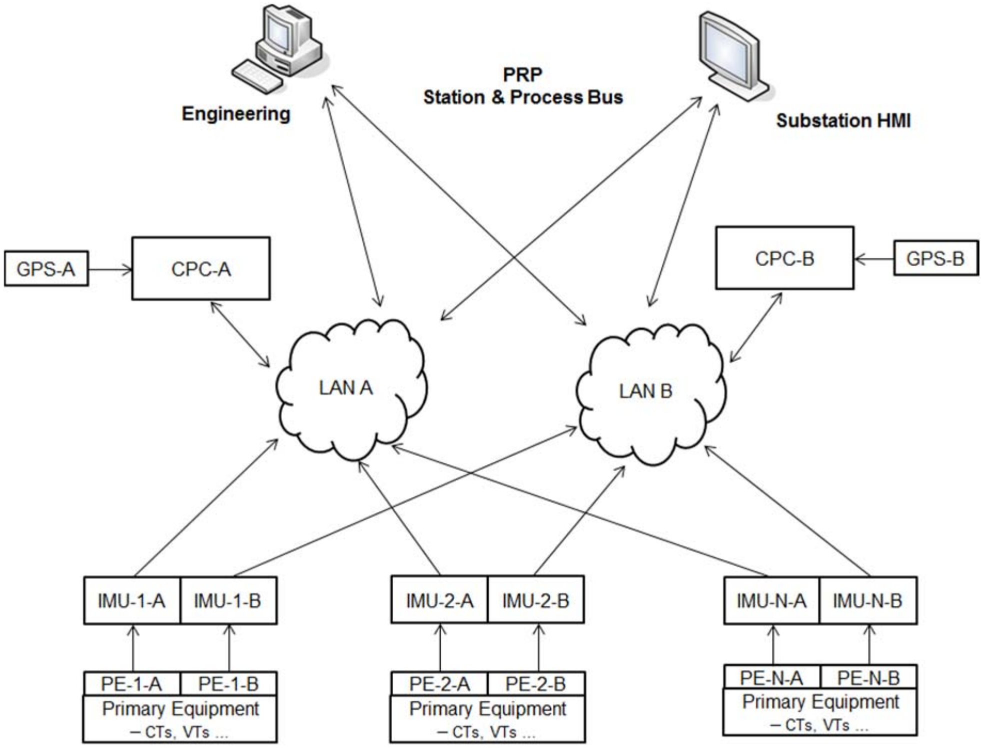


Figure 27. Single PRP network for both process and station buses.

The architectures in Figure 28 and Figure 29 represent converged process and station bus topologies based on mixed HSR-PRP networks. The station and process buses are physically converged but logically separated; mission critical protection related traffic (multicast SV, GOOSE) will be contained mostly in HSR domain and control traffic (unicast MMS etc..) will use PRP networks.

This separation allows processing of protection traffic with minimum latency, while still providing access from any node to any node. The RedBoxes connecting HSR rings to PRP networks in Figure 28 and Figure 29 act as bridges with multicast filtering, preventing high utilization of the process bus multicast traffic entering station bus with primarily unicast control traffic. Delays in HSR networks will be around 5 microsecond per node for store and forward and sub-microsecond for cut-through architectures as in section 6.4.10.4 of [36].

These networks provide end to end redundancy, starting with redundant Primary equipment (CTs, VTs, sensors etc.) and going all the way to redundant CPCs.

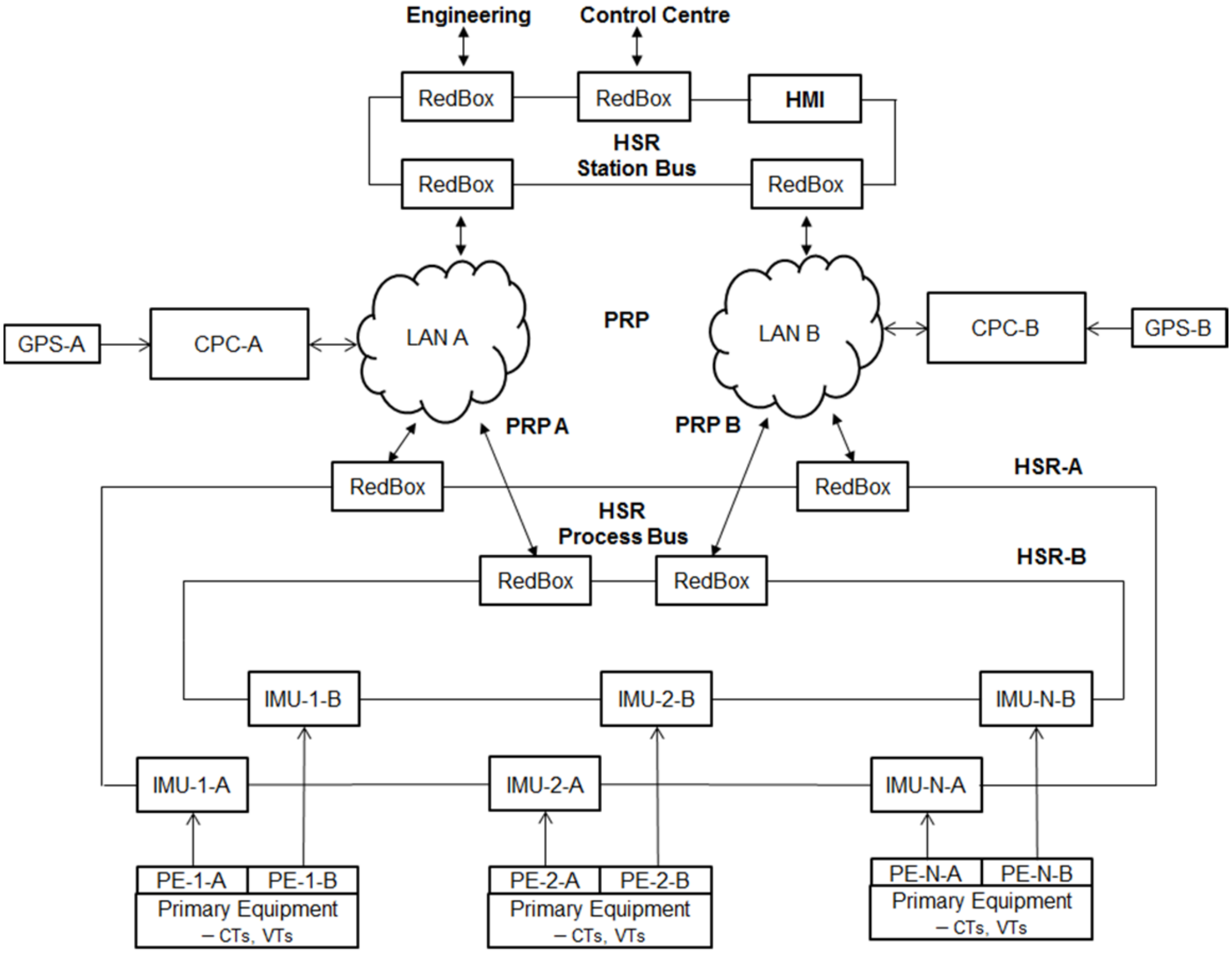


Figure 28. Mixed HSR/PRP networks with CPC connected to PRP (station bus).

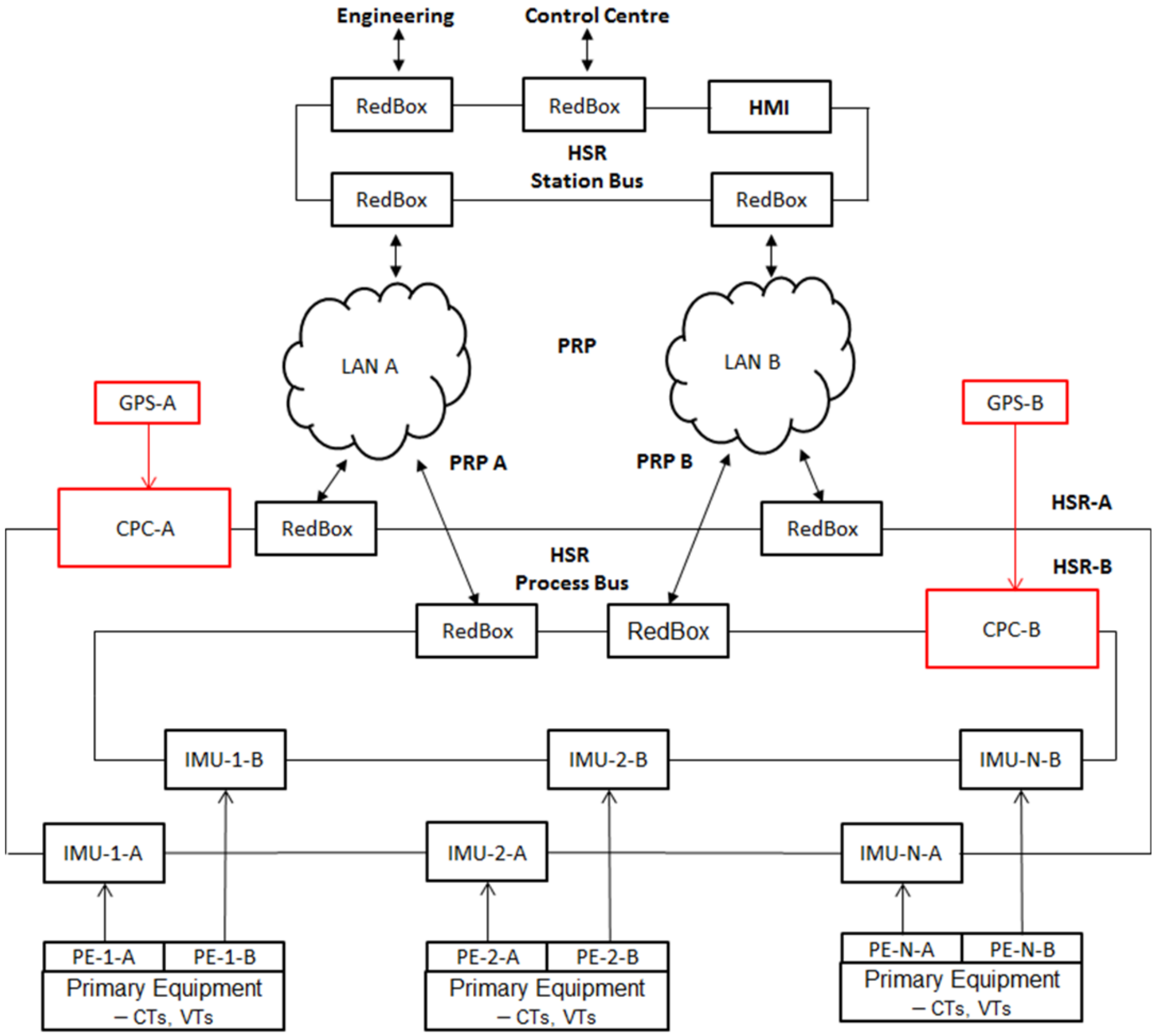


Figure 29. Mixed HSR/PRP networks with CPC connected to HSR (process bus).

There are two HSR rings in Figure 28 and Figure 29 with N IMUs in each ring. To reduce latency more HSR rings can be created with less number of IMUs in each ring.

Redundant CPCs with any timing references like GPS and/or IRIG-B can be connected to redundant PRP LANs A and B (Figure 28) or located on HSR rings (Figure 29) depending on the network design and CPC processing power to be able to handle high load of protection traffic. There can be only one PRP network and HSR rings cannot be connected between themselves by QuadBoxes since this will create loops.

The timing synchronization will be based on 1588 Precision Time Protocol using the IEEE C37.238-2011 Standard Profile [41] for use in Power System Applications.

Other elements in these networks that can be connected as:

- SANs to LAN A,B,
- Sub-rings to any HSR ring by using QuadBoxes and
- SANs to PRP RedBoxes.

4.5 Reliability and Cost Analysis

The objective for the reliability and cost analysis is to compare the architectures qualitatively with a simplified approach based on estimates of reliability and cost values of individual components. This analysis can be used as a starting point to develop a much more detailed value proposition.

4.5.1 Reliability Analysis

The reliability and availability of the possible CPC architectures described in Section 4.3 is evaluated and reported in this section. In all of the architectures, Ethernet communication devices can be connected in various combinations. Several network topologies can be realized, such as 1-Cascade, 2-Ring, 3-Star-ring and 4-Redundant-ring. As reported in [44], redundant-ring provides the highest reliability as compared to other three studied topologies while cascade provides the least reliability. In this report, the Ring configuration is selected for reliability evaluation and comparison as it provides the average reliability and cost among all possible configurations. In addition to this, the time synchronization can be employed using different techniques, such as external time synchronization source using IRIG-B protocol [39] or time synchronization on LAN using 1588 v2 [40]. As reported in [44], time synchronization based on 1588 v2 shows higher reliability as compared to time synchronization based on IRIG-B. It this report, time synchronization over communication network (LAN) is used for reliability evaluation.

The quantitative values of reliability and availability for the possible CPC architectures are obtained using the Reliability Block Diagram (RBD) technique [45]. Although the reliability analysis using other methods such as fault tree, cut set, path set, etc. have different formal presentations, they all may give similar results as RBD [45]. For qualitative and quantitative analyses, RBD is more preferable as it is easy to understand, and hence it is used for this work.

Reliability can be represented as a mean time to failure (MTTF), which is the average time between system breakdowns or loss of service. The MTTF values of various protection devices for reliability calculations are adopted from [46, 47], and are tabulated in Table 2. The basic assumption is applied here that the failure modes are independent from each other [45]. Further, using mean time to repair (MTTR) of 24 hours reported in [46], the availability of individual components is calculated.

Table 2. MTTF and availability of various devices within CPC System.

SAS component	MTTF (in years)	Availability
IED with communication interface	100	0.999972603
IMU with communication interface*	100	0.999972603
TS with communication interface	150	0.999981735
Ethernet Switch	50	0.999945208
Fiber cables	500	0.999994521
CPC with communication interface (assumed)	100	0.999972603

*available MU data is used for IMU in the reliability and cost calculation.

Using these tabulated individual component values, the MTTF and availability are calculated for possible CPC architectures. Availability and MTTF calculations basics are discussed in Appendix E of [44]. For performance comparison, it is assumed that

1. The reliability of copper cable is very large and is considered as 1 (MTTF = inf, Availability = 1) in the evaluation process,
2. The reliability of the instrument transformers and circuit breakers is not considered in the evaluation as it is common among all the architectures,
3. The protection element implemented in CPC requires access to various data provided by a combination of total 16 devices including IEDs and IMUs,
4. The process bus or the station bus includes 4 Ethernet switches connected in a Ring configuration.
5. The downtime for software upgrade or hardware replacement is zero. Many CPC systems can be designed with adequate redundancy where this can be achieved. It is one of the hallmarks of the CPC based system. However, to achieve this goal a paradigm shift is required in the design, production, installation, operation and maintenance of a CPC based system.

Architecture-1

In this architecture, it is assumed that the CPC is connected to 16 IEDs through a station bus. The CPC requires the information of all 16 IEDs to make a decision. The reliability can be calculated from

Reliability = (IED^16)*(ESW^4)*(3 out of 4 Fibers)*(1 Fiber)*CPC

A = 0.999309829697314 and MTTF = 3.914988814317673

Architecture-2

In this architecture, the CPC is connected to 8 IEDs through a station bus and has direct communication with 8 IMUs through fiber optic cables. 16 IEDs communicate with 16 IMUs through 16 direct fiber optic cables. The CPC requires the information of 2 IEDs connected to each switch (total of 8 IEDs) and 8 IMUs to make a decision.

Reliability = (IED^8)*(ESW^4)*(3 out of 4 fibers)*(1 fiber)*CPC*(IMU^8)*(Fiber^8)

A = 0.999266028788814 and MTTF = 3.684210526315789

Architecture-3

In this architecture, each CPC is connected to 16 IMUs by direct fiber optic cables. Each CPC requires the information of all connected IMUs to make a decision. At least one out of two CPCs must operate for correct operation.

Reliability = (1 out of 2 CPCs)*(IMU^16)*(Fiber^16)

A = 0.999474115330214 and MTTF = 5.033557046979866

Architecture-4

Two options have been considered for this architecture. In Option 1, the CPC requires the information provided through 16 IMU through the process bus. In this case, Reliability = (IMU^16)*(ESW^4)*(3 out of 4 Fibers)*(1 Fiber)*CPC

A = 0.999309829697314 and MTTF = 3.914988814317673

In Option 2, the CPC is connected to eight IEDs through four Ethernet switches (two IEDs each) and directly communicating with eight IMUs through fiber optic cables. In this configuration, 16 IEDs communicate with 16 IMUs through a ring process bus with four Ethernet switches (four IMU each). The CPC requires the information of all eight IEDs and eight IMUs to make a decision.

Reliability= (MU^16)*(IED^8)*(ESW^4)*(3 out of 4 cables)*(Fiber^2)*CPC*(ESW^4)*(3 out of 4 cables)

A = 0.998866402225986 and MTTF =2.376103190767142

Architecture-5

Each CPC is connected to 16 IMUs through a ring bus Ethernet switch network. Each CPC requires the information of all connected MUs to make a decision. For correct operation, at least one out of two CPCs must correctly operate.

Reliability= (1 out of 2 combined (CPC and Fiber))*(MU^16)*(3 out of 4 fibers)*(ESW^4)

A = 0.999342682857271 and MTTF = 3.977272727272727

Architecture-5a

There are two CPC and process bus networks. Each CPC is connected to 16 IMUs through a dedicated ring bus Ethernet switch network. Each CPC requires the information of all connected IMUs to make a decision.

Reliability= 1 out of 2 combined (CPC*(1 fiber)*(IMU^16)*(3 out of 4 fibers)*(ESW^4))

A = 0.999999523664953 and MTTF = 5.872483221476509

Table 3 shows the availability and MTTF of possible architectures. As shown, Architecture 5a has the highest rank while Architecture 4 option 2 has the lowest rank.

Table 3. Performance evaluation of different architectures.

	Availability	MTTF (years)	Rank
Architecture 1	0.99930983	3.9	4
Architecture 2	0.999266029	3.7	5
Architecture 3	0.999474115	5.0	2
Architecture 4 (Option 1)	0.99930983	3.9	4
Architecture 4 (Option 2)	0.998866402	2.4	6
Architecture 5	0.999342683	4.0	3
Architecture 5a	0.999999524	5.9	1

4.5.2 Cost Analysis

Only the architectures that employ the CPC for the primary protection of substation apparatus are considered in the cost analysis study and are limited to Architectures 3, 5 and 5a. The number of IMUs, Ethernet switches and fiber cables as well as network configuration, are the same as in the reliability analysis study. A very simplistic approach is adopted in this analysis by only considering the approximate cost of the main pieces of equipment. In practice, accurate cost analysis should be performed, including the cost of installation, commissioning and testing.

Let's assume that the cost of each IMU is C_{IMU}, the cost of each Ethernet switch is C_{ESW}, the cost of each long fiber cable is C_{FCX}, the cost of each short fiber cable such as the one within the control room or between IMUs and Ethernet switches is C_{FCI} and the cost of each CPC is C_{CPC}.

Architecture-3

In this architecture, each CPC is connected to 16 IMUs by direct fiber optic cables. Each IMU communicates with two CPCs through two dedicated fiber cables. Therefore,

$$\text{Cost}= 2*C_{CPC}+16*C_{IMU}+32*C_{FCX}$$

Architecture-5

Each CPC is connected to 16 IMUs through a ring bus Ethernet switch network. Each CPC requires the information of all connected IMUs. It is assumed that the fiber optic cables among IMUs and Ethernet switches are short while the cables connecting Ethernet switches to CPCs are long.

$$\text{Cost}= 2*C_{CPC}+16*C_{IMU}+2*C_{FCX}+(16+4)*C_{FCI}+4*C_{ESW}$$

Architecture-5a

There are two CPC and process bus networks. Each CPC is connected to 16 IMUs through a dedicated ring bus Ethernet switch network.

$$\text{Cost}= 2*C_{CPC}+32*C_{IMU}+2*C_{FCX}+2*(16+4)*C_{FCI}+8*C_{ESW}$$

To be able to have an initial cost comparison, let's assume the following costs.

$$C_{IMU} = \$2500,\ C_{FCX} = \$1000,\ C_{FCI} = \$300,\ C_{ESW} = \$7000$$

Table 4 shows the cost of the possible architectures studied here. As it is shown, Architecture 5a is more costly but it provides the highest reliability. The costs of Architectures 3 and 5 are very close while Architecture 3 is more reliable with MTTF of 5 years, compared to 4 years for Architecture 5.

Table 4. Cost evaluation of different architectures.

	Cost	Cost Rank	Reliability Rank
Architecture 3	$2*C_{CPC}+72000$	1	2
Architecture 5	$2*C_{CPC}+76000$	2	3
Architecture 5a	$2*C_{CPC}+150000$	3	1

4.6 Testing and Maintenance Aspects

The CPC concept does not change the general need for testing protection and control systems, but this concept can change the specific requirements for, or methods of, testing. The biggest change is that the CPC separates the application controller (and therefore, application program) from the physical I/O devices. This allows for separate testing of the CPC and the I/O devices, and sets different testing goals for the CPC and I/O devices. This modular nature also allows for comparisons that can change many current testing activities into future self-monitoring activities: comparison between I/O signals and measurement in one CPC, and comparison between operating decisions between multiple CPCs.

There are, in general, four different types of testing required or performed on protection and control products and installations. These test types are:

- Acceptance testing, where a specific type or model of device is approved for use on the power system. This normally involves extensive bench or laboratory testing of the device against common operating scenarios.
- Commissioning testing, where a device or system is tested after installation or significant configuration change or upgrade. This is to ensure the device or system is working correctly, and is installed and configured as intended and as designed for the specific application.
- Maintenance testing, where an installed device or system is tested to ensure it is still operating within performance parameters, and to detect any possible hidden failures in the system or device.
- Troubleshooting, where an installed device or system is analyzed after an operating event indicated the device may not have performed as expected or desired.

The implementation of the CPC concept, and the split of the protection and control system into a virtual controller communicating to physical I/O, impacts the methods used for all of these testing types.

4.6.1 Elements to Test

Under the CPC concept, there are 3 different elements that need testing, and all 3 elements have different testing requirements. These elements are the CPC itself, the I/O devices, and the communications network between the CPC and the I/O devices. One advantage of the CPC concept is the modularity of the system. If all 3 components (CPC, I/O, and communications) are working correctly, then the whole system is working correctly. This allows testing the 3 different elements independently of each other.

The CPC must be verified as working correctly. Since the CPC is an application controller, the major goal is to ensure the CPC is configured correctly for the specific application, and that it communicates correctly to I/O devices. The CPC must be shown to accept status information from I/O devices, and must be shown to send control commands to I/O devices. Part of this testing must ensure protection decisions are made correctly and timely, so that processor loading and application priority is not a factor. Performance testing of the CPC will probably require different processes and techniques than used for testing traditional relays. These processes and techniques are not clearly defined at this time, and will be dependent on the capabilities and implementation of a specific CPC.

I/O devices must be shown to be working correctly. This means that the I/O devices are measuring power system quantities (analog measurements, equipment status and alarms) and can control power system equipment (through output contacts or other control commands). This also means I/O devices must be shown to send data to the CPC, and to be able to accept control commands from the CPC. Since I/O devices are essentially hardware devices, testing of the physical components, especially contact inputs and output contacts is required.

The communications network must also be tested. The requirements for communications networks will be reliability: ensuring messages between the CPC and I/O devices will always go through, and that the latency of these communications will be within desired parameters. Beyond these minimal requirements, testing of communications network is a specialized endeavor.

4.6.2 Acceptance Testing

CPC has little impact on the general requirements for acceptance testing, other than the requirements for tools and procedures. It is necessary to verify that the CPC itself will perform protection functions as desired, even with the maximum number of functions enabled. This will require verifying the performance of individual protection elements, along with verifying the performance of the entire CPC. The processes, tools, and models necessary for acceptance testing of a CPC will take careful thought and design. It is also necessary to understand the number of I/O devices a CPC can connect, the number and types of messages it can receive and send, and specific performance requirements for the communications network. I/O devices must be tested for functionality and communications, including the number and types of control messages it can receive.

4.6.3 Commissioning Testing

Commissioning testing is where the CPC concept has a large impact. The modularity of the system allows the individual elements to be commissioned separately and independently of each other. The virtual nature of the CPC itself allows commissioning in an office environment, before sending the device, and device configuration, to the actual physical location.

The section of the power system the CPC is intended to protect and control can be modeled through digital simulation and the communications to and from I/O devices can also be simulated. This allows engineers to verify their configuration and design, against actual anticipated fault events, without requiring extensive field testing or actual I/O devices. This is true when commissioning CPC configurations for brand new installations, or when commissioning a changed CPC configuration for upgrades to an existing installation. For existing installations, the CPC configuration can be retrieved from the field device, modified, commissioned, and returned directly, without necessarily requiring onsite action.

I/O devices still require commissioning to prove the physical parts of the hardware; such as analog measurement channels, contact inputs, and contact outputs, are operating correctly. These can be tested without connection to the communications network or CPC. The communications messages to and from the I/O devices can be monitored and simulated to help prove the I/O device is working and installed correctly. I/O devices can become tightly integrated into primary equipment, and this commissioning can (and should) become part of the factory acceptance testing of the primary equipment.

The communications network must be proven to operate within performance parameters during commissioning, including during contingency events such as loss of a network element, path reconfiguration, and network loading situations.

Though a CPC system is modular, and the individual elements can be commissioned separately and independently, the total system must still work. It is therefore desirable to perform final checkout commissioning on site, to verify that the CPC is communicating with the correct I/O devices, and that any other physical interconnections (such as to teleprotection equipment) are correct. But this checkout commissioning should only verify connections, not completely retest and recommission the entire system.

4.6.4 Maintenance Testing

The CPC concept has a large impact on maintenance testing, once again due to the modular nature of the system, and the splitting of the application from the physical I/O hardware.

There is no need for maintenance testing of the CPC itself. As an application controller, internal self-testing and monitoring will show if the unit (and software) is performing correctly. With multiple CPC units in a substation, voting methods, or comparisons between trip decisions, quantities, and status will be a further degree of self-monitoring. If all CPCs are reaching the same conclusion, then all units are operating correctly. Discrepancies between units should be investigated. Additionally, the CPC configuration can be retrieved, compared against a digital simulation in a laboratory, and verified as correct. Using state estimation simplifies this even more, as the state determined by the CPC should match the physical state of the power system.

There is limited need for testing I/O devices. Using multiple I/O devices to collect the same data allows comparison of analog measurements, and to a limited extent, contact inputs, inside of a CPC. This adds self-testing capability for analog channel measurement. Discrepancy between comparisons of two measurements that should be the same indicates a measurement channel failure given that reference value is known. State estimation of data will also identify discrepancy in measurements. However, the physical I/O, especially output contacts, must still be verified to be operating correctly. This can be performed through simple trip testing and alarm assertion during normal primary equipment maintenance outages.

The communications network also requires no maintenance testing, as it is continually monitored during normal operations. Messages are being sent between the CPC and I/O devices continuously. Messages not received, or not being received within operating parameters, will be recognized and alarmed.

4.6.5 Troubleshooting

The CPC concept helps improve troubleshooting when the protection and control system doesn’t operate as expected or intended. The configuration and the performance of the CPC itself can be quickly verified in a laboratory setting. The CPC configuration is retrieved, and all recorded data (oscillography, sequence of events logs, system logs, etc.) are retrieved. The CPC configuration is installed in the lab, along with a digital simulation of the power system, and the specific event is recreated. This will prove or disprove the operation and configuration of the CPC against this event.

I/O devices, if a possible cause, must still be tested using more traditional methods. The only difference is that the communications messages can be simulated or monitored without actually going to or from the CPC. State estimation can also point out possible problems with I/O devices. The communications network performance can be verified by comparing sequence of events logs from I/O devices and the CPC.

4.7 Advanced Applications

This section discusses some of the advanced applications that are either not possible or difficult to implement within an IED in a substation because they require data from many IEDs and in some cases data from neighboring substations. These features can be implemented at the substation level. CPC provides a unique opportunity to centralize all physical IEDs in a substation based system and minimizes communication of processed data and enables reliable implementation of the applications discussed in this section. Many other applications, not used today, such as dynamic control of load and distributed generation at the substation level based on distributed intelligence, will become more attractive to develop once a CPC system is implemented.

4.7.1 Detection of Hidden Failures

Hidden failures are the most difficult issue to deal with in the present state of art in protection systems and per bay IEDs detect some of them [48]. Fundamentally, the present per bay protective relay approach, i.e. a protective relay monitoring a number of quantities (typically three voltages and three currents) and performing protective functions based on this information alone, may not have the capability to detect many hidden failures.

There are a number of other possible hidden failures such as wrong CT or VT ratios, control wire burnout or disconnection. Present methods address the issue of hidden failures by periodic maintenance and physically checking the relay instrumentation, relay settings and testing of relay functions. This approach may require protection outages, it is time consuming and this type of maintenance program is expensive.

A better alternative is a centralized protection approach instead of the present per bay protective relay approach. Specifically, a substation protection approach means that all the measured quantities at the substation will be collected at the substation CPC. These measurements provide enough redundancy to determine which measurements are valid and which measurements are bad data. Redundancy is the key here. Consider the case of voltage measurements of the same bus with two sets of VTs. Assuming all breakers are in the close position (this is also a measurement), the voltage measurements received at the relay must be same within the accuracy of the instrumentation. Now consider the possibility that one fuse at one of the VT circuits is blown. In this case, the voltage measurements coming from the same bus via two different sets of VTs will be different. The conclusion is that one of these sets of measurements is wrong. One can look for additional information to determine which is wrong and which is right. For example if one set of voltage measurements is nearly balanced and all current measurements are also near balanced, then the nearly balanced voltage measurements are the correct ones while the other are the wrong measurements. This analysis indicates the location of the blown fuse.

The above example indicates the complexity of analyzing redundant measurements to first identify the existence of bad data and then to determine which data are wrong. There is much prior work that provides good systematic and robust solutions to the problem of detecting the presence of bad data and then identifying the location of the bad data (detection and identification). Once the bad data have been identified, this also indicates the type of hidden failure in the system. Specifically, the detection and identification of bad data is done in a systematic and mathematically rigorous way by means of state estimation. A full description of modern state estimation is beyond the scope of this report.

For the purpose of detecting hidden failures in the substation relaying system, state estimation can be implemented in several alternative ways. Figure 30 illustrates the application of state estimation on the phasor data collected by all relay instrumentation in a substation. Figure 31 illustrates the application of state estimation on the sample data waveform collected by all merging units in the substation. Figure 32 illustrates an implementation that is partly based on merging units and partly on legacy numerical relays. All three approaches are feasible today. As a matter of fact the approach illustrated in Figure 30 has been implemented in several substations (pilot projects). The implementation shown in Figure 32 is very important in the sense that it allows smooth transition from one technology to another as substations are being upgraded.

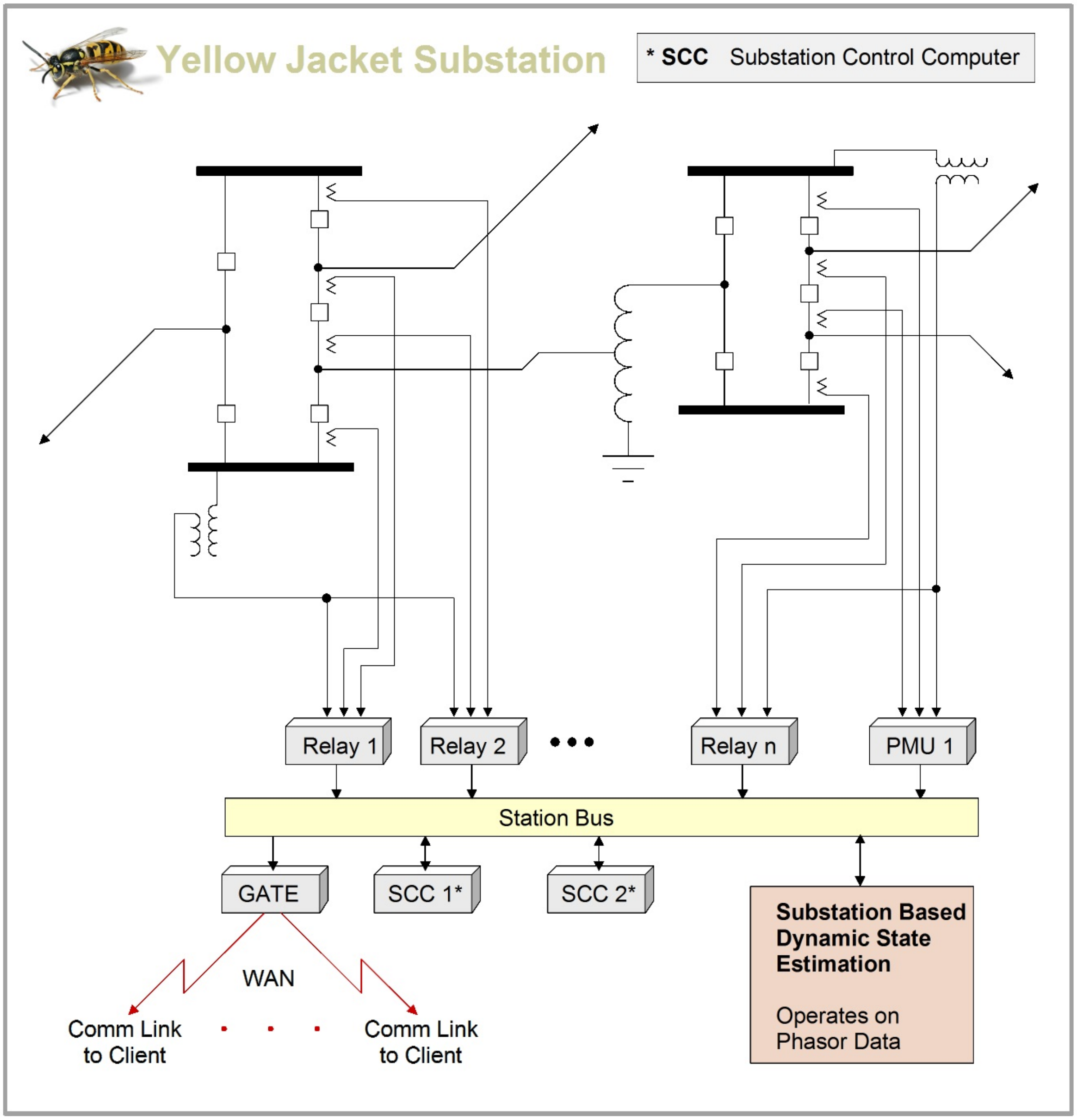


Figure 30. Using legacy numerical relays.

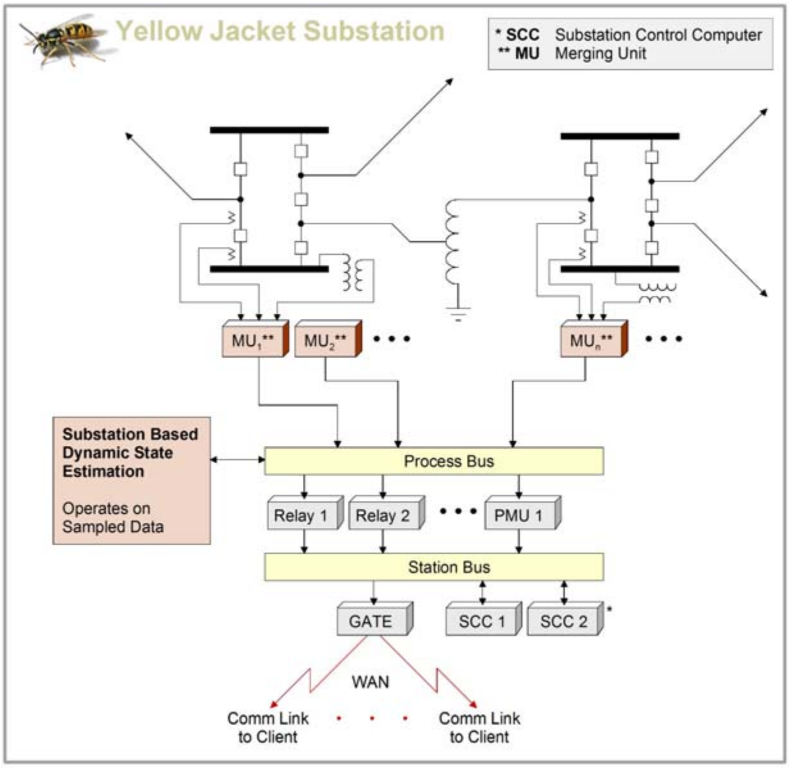


Figure 31. Using merging units and process bus.

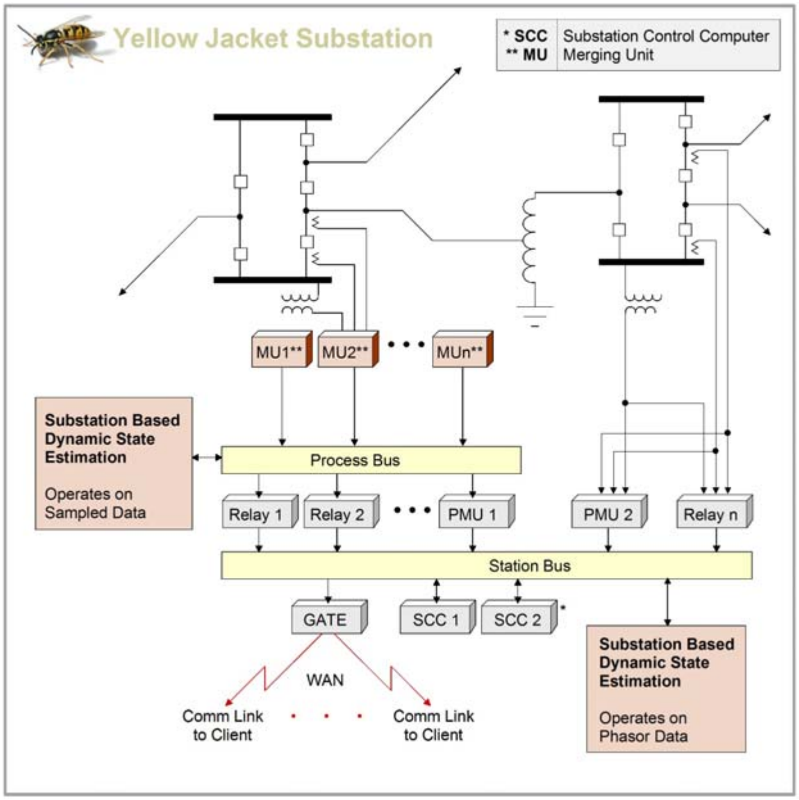


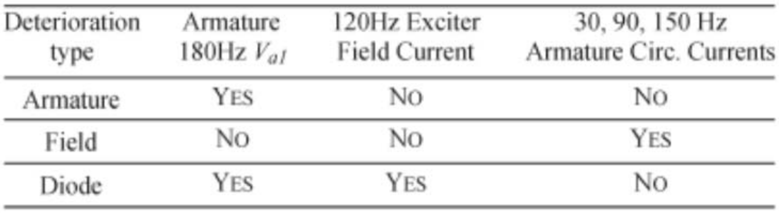
Figure 32. Hybrid implementation using legacy numerical relays and merging units.

4.7.2 Incipient Fault Detection

Incipient fault detection refers to detection of faults during their beginning stage so that remedial actions may be taken to avoid catastrophic failures. Examples include loose or noisy primary connections, fuse failures, impending arrester or insulator failures, capacitor failures, sporadic foreign interference identification. Incipient splice failure detection in underground cable is already available, and similar techniques are being field tested to be able to detect incipient failures in arresters, capacitor cans, and power transformers and VTs. Bushing failures have traditionally been predicted through manual testing. Field tests are currently underway to gather data of the in-service predictive impending incidents and conditions [49, 50, 51, 52].

There are different methods for detecting incipient faults for different components. A proposed method for detecting incipient faults in generators is described in [53]. The method uses detectors that include the 180-Hz positive-sequence stator voltage as an indicator of armature-winding deterioration, the 30-, 90-, and 150-Hz armature circulating currents as indicators of field winding deterioration, and the 120-Hz exciter field current as an indicator of rotating rectifier diode shorts. Acquisition of these quantities requires only standard current and voltage probes. Table 5 shows the sensitivity of detectors to different types of deterioration.

Table 5. Sensitivity of detectors to different types of deterioration.



Deterioration type	Armature 180Hz V_{a1}	120Hz Exciter Field Current	30, 90, 150 Hz Armature Circ. Currents
Armature	YES	NO	NO
Field	NO	NO	YES
Diode	YES	YES	NO

A distribution fault anticipation system is proposed in [54], where voltage and current waveforms at selected locations were continuously recorded and analyzed. The signatures contained in the waveforms may be used for detecting incipient faults. As an example, an underground secondary cable incipient failure caused current bursts on the primary current, as shown in Figure 33. An algorithm that is able to detect the bursts can signal potential problem, and timely corrective actions will avoid bigger problems.

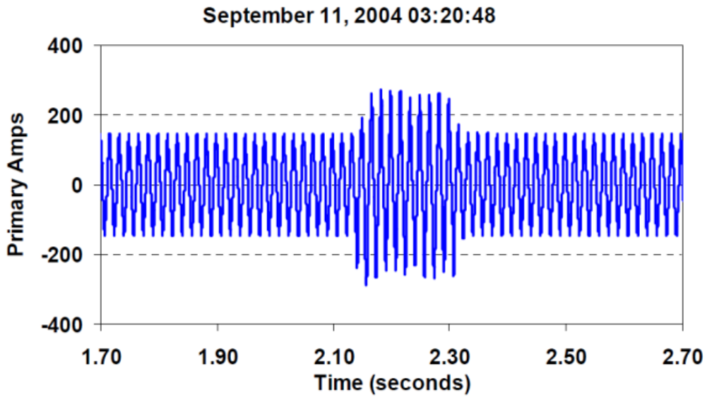


Figure 33. Current bursts recorded due to a cable failure.

Digital protection systems with IEDs could provide some of the incipient fault detection functionality for certain power equipment or components, but these individual protection devices data are isolated. With a CPC system, the data for different equipment protection can be readily combined into a central location for analysis. For example, it may be possible to determine the reason for a cable failure, which may be caused by a lightning event, or caused by overloading based on integrated analysis of records collected from different devices.

4.7.3 Data Analytics

Various types of measurements including voltage, current, frequency, and power may be obtained from different locations of the power grid. Different types of applications can be developed to analyze the data to derive useful information. This section will present two applications: fault location and power quality disturbance classification.

Fault location

Accurate and speedy fault location on transmission and distribution lines helps maintenance crews pinpoint and fix faulted components, reduce outage time and enhance system reliability [55].

Various fault location methods have been proposed in the past. Transmission systems and distribution systems have different characteristics. Transmission systems are usually equipped with more data recording devices than distribution systems, and transmission systems are usually balanced and meshed. Hence, different fault location methods have been proposed for transmission and distribution systems in the past [56, 57, 58, 59, 60].

Some fault location methods are based on injecting signals of a specified frequency at the substation. Other methods rely on analyzing voltage and current measurements, which can be magnitude, phasor, or waveforms, captured during a fault. These methods have less strict requirements of hardware, and are more easily implemented. These methods are further classified into impedance based methods and traveling wave based methods. Traveling wave methods derive fault location by multiplying the traveling wave speed and the time which it takes for the fault-generated traveling wave to travel from the fault point to the bus location. It usually requires a high sampling frequency in the range of one MHz to get a good estimate, and thus imposes higher demand on hardware. The impedance based fault location approach utilizes fundamental frequency voltage and current phasors to calculate the fault location. With increasing deployment of recording devices including digital fault recorders, digital relays, phasor measurement units, etc., impedance based fault location methods have been widely adopted in practice.

Depending on availability of recording devices, one-terminal, two-terminal, or multi-terminal fault location methods have been developed for transmission lines. Methods that utilize sparse measurements and the network data has also been proposed recently, where the voltage and current signals at a bus location which may be far away from the faulted line can be used to calculate the fault location [58]. For distribution systems, most of the proposed methods utilize local measurements to estimate the fault location. The network topology may be updated through the SCADA system, and passed to the fault location module for enhanced fault location accuracy.

Power quality disturbance classification

Due to various reasons such as nonlinear loads and faults, voltage and current waveforms may deviate from the normal sinusoidal waveforms. Such deviation is called power quality disturbance or power quality event. Common types of power quality disturbances include voltage sag, swell, interruption, harmonic, impulse, flicker, switching transient, and notch, etc. An increasing number of power quality meters have been deployed in power systems, so automated classification of captured power quality disturbances is desirable. Typical methods utilize Fourier transforms and wavelet transforms to extract features and intelligent techniques like artificial neural network, and adaptive neuro-fuzzy inference system (ANFIS) for making a decision. As an example, a seven-input ANFIS system for power quality disturbance classification is shown in Figure 34 [61].

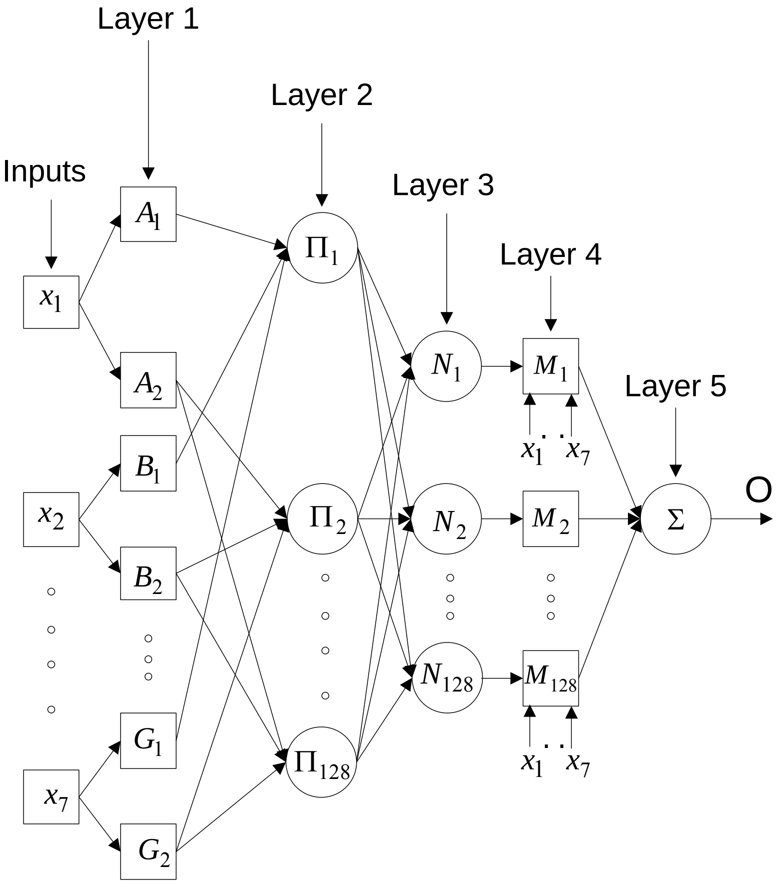


Figure 34. A seven-input ANFIS architecture.

In the figure, $x_1, x_2, \dots . x_7$, represent the seven features extracted from the analyzed voltage or current waveforms. Layer 1 parameters $A_1, A_2, \dots . G_{1,} G_2$ symbolize the fuzzy sets of the seven inputs. For example, $A_1, and\ A_2$ are the fuzzy sets of the feature x_1. The five layers of the network are explained as follows. The first layer yields the membership of the feature. The second layer yields the firing strength of a rule involving the incoming signals from the previous layer. The output of each node in the third layer is the ratio of its firing strength to the sum of all rule's firing strength. In the fourth layer, the output of each node is calculated according to the output of layer 3, input features and the network parameters. The node of the output layer, i.e., layer 5 computes the overall output by summing all incoming signals.

Conventional IEDs could provide some functionality of fault location and PQ analysis. But these individual IEDs data are isolated. With a CPC system, the data from different (virtual) IEDs can be readily put into a central location for analysis. For example, a fault event may be determined to be due to a lightning event or due to line sagging into a tree because of overloading and hot weather based on correlation analysis of records collected from different devices. In another example, a sag power quality event may be correlated to a fault event or big motor starting event based on integrated data analysis of multiple (virtual) IEDs.

4.7.4 Distributed Asset Management

State-of-the-art IEDs have readily-available, detailed information, such as log files, operating and event records, self-diagnostics, settings, and performance data. These devices can be discrete sensors used to monitor operating, mechanical, or electrical conditions, or they can be part of a complex device such as a protection IED or piece of communication equipment or a device controller (tap changer, battery charger, breaker controller, etc.). Further, the source of information can be obtained from the device itself or a component within the device such as a logical node in an IEC 61850 enabled device. Network communication provides the medium for the interrogation and retrieval of data. The information produced by these devices can be communicated to a central location or distributed among the various devices (nodes) on the network and used within the local and/or enterprise network.

An emerging application using this bourgeoning availability of data is asset management. For example, breaker operating information has been used for some time now as an input into breaker maintenance and performance analysis. I^2t (I squared t), operation counters, or interrupting current can be used as metric in the evaluation of device performance. These traditional applications have typically been local to the device and obtained from discrete, non-networked devices and used for specific purposes such as maintenance. Today, the same information on breaker operation, and likely much more, is readily available from protection IEDs or breaker monitoring IEDs.

Distributed asset management, however, involves obtaining equipment data from various IEDs as input to asset management analytics. This differs from traditional asset management approaches in that this process is dynamic – the analysis can take place frequently (or on demand), not once during the design stage, or perhaps just prior to a rate case application or sale of the assets. The advantage of this dynamic process is obvious, the asset manager now has a reliable and up-to-date reflection of the state of their equipment for maintenance, capital, and regulatory use, among others.

Asset management analysis typically examines devices in bulk or with similar characteristics. With a distributed approach, individual devices can be monitored and either their aggregate performance or unique individual performance determined. The information available from distributed assets can be further enhanced by integrating information from more than one source into a single analytic. For example, instead of simply looking at breaker data to evaluate the state of a breaker, distributed asset management could also correlate breaker data with line loading or temperature data or even load characteristics.

Distributed asset management will play an import role in a CPC strategy due to the high availability of data useful for managing assets at the substation level.

5. DEMONSTRATION PROJECT

Centralized substation protection and control has been attempted in the past based on the available technology. This evolution is now at the intersection of sensing, protection and communication technologies, providing the unique opportunity to develop a more reliable and maintainable CPC system. This section discusses a software based substation protection, automation, and control system (PACS), iSAS, developed by LYSIS LLC, Russia which is under trial operation at the 110/10 kV "Olympic" substation in the town of Surgut in northwest Siberia [62].

The philosophy of iSAS is based on PAC function element implementation as per IEC 61850 logical nodes (LN). The software modules were developed independently of particular hardware and could be placed in dedicated IEDs as well as in one powerful computer. When the software modules are located in the same device they interact with each other through the iSAS software core over its internal mechanisms. However, when they are distributed among various devices then they use Process and/or Station Bus communication services. The decision about the allocation of functions depends on particular project requirements and performance of available hardware and resource consumption by software modules. Conformity to the IEC 61850 information model and configuration language (SCL) was one of the main priorities of the project.

5.1 Overview of iSAS project

iSAS is implemented in a PAC system for a 110/10 kV substation pilot project for one Russian Distribution System Operator (DSO) - *Tumenenergo*. The project is completely managed and implemented by iSAS' software developer - LYSIS LLC. The project has the following goals:

- Search for an optimal system architecture, methods and approaches for iSAS lifecycle management,
- Research and analyze system characteristics and behavior under real-life conditions,
- Provide technical and economic analysis at all stages of the system lifecycle, as well as comparison with conventional systems with similar functionality,
- Conduct a reliability analysis and comparison with a system with conventional architecture,
- Quantify the advantages and disadvantages of the PACS system, along with the suitability for the DSO to spread out such experience widely.

The selected 110/10 kV *Olympic* substation, for the pilot implementation of a centralized digital PAC system, contains two power transformers, two incoming 110 kV overhead power lines and 40 feeders connected to four 10 kV busbars. The digital software-based PACS implemented in the project has to perform the full functionality of protection, control and metering systems for the entire substation according to regulatory standards and customer's requirements. According to the contract, the project has five phases:

1. Design,
2. Procurement, installation and testing,
3. Trial operation of the system for one year,
4. Analysis of regulators requirements, rules, and standards, and proposing amendments in these documents for homologation of software-based PAC systems in the Russian market, and
5. Certification of measuring method for process bus-based systems with separate measuring (process interfacing devices, PID) and calculation (IEDs) parts.

At this time, LYSYS LLC has completed the design, procurement, installation and testing phases and the system has been put in trial operation. Phases 4 and 5 are expected to be completed by the end of 2015.

5.1.1 Protection Subsystem

The single line diagram of the substation is shown in Figure 35.

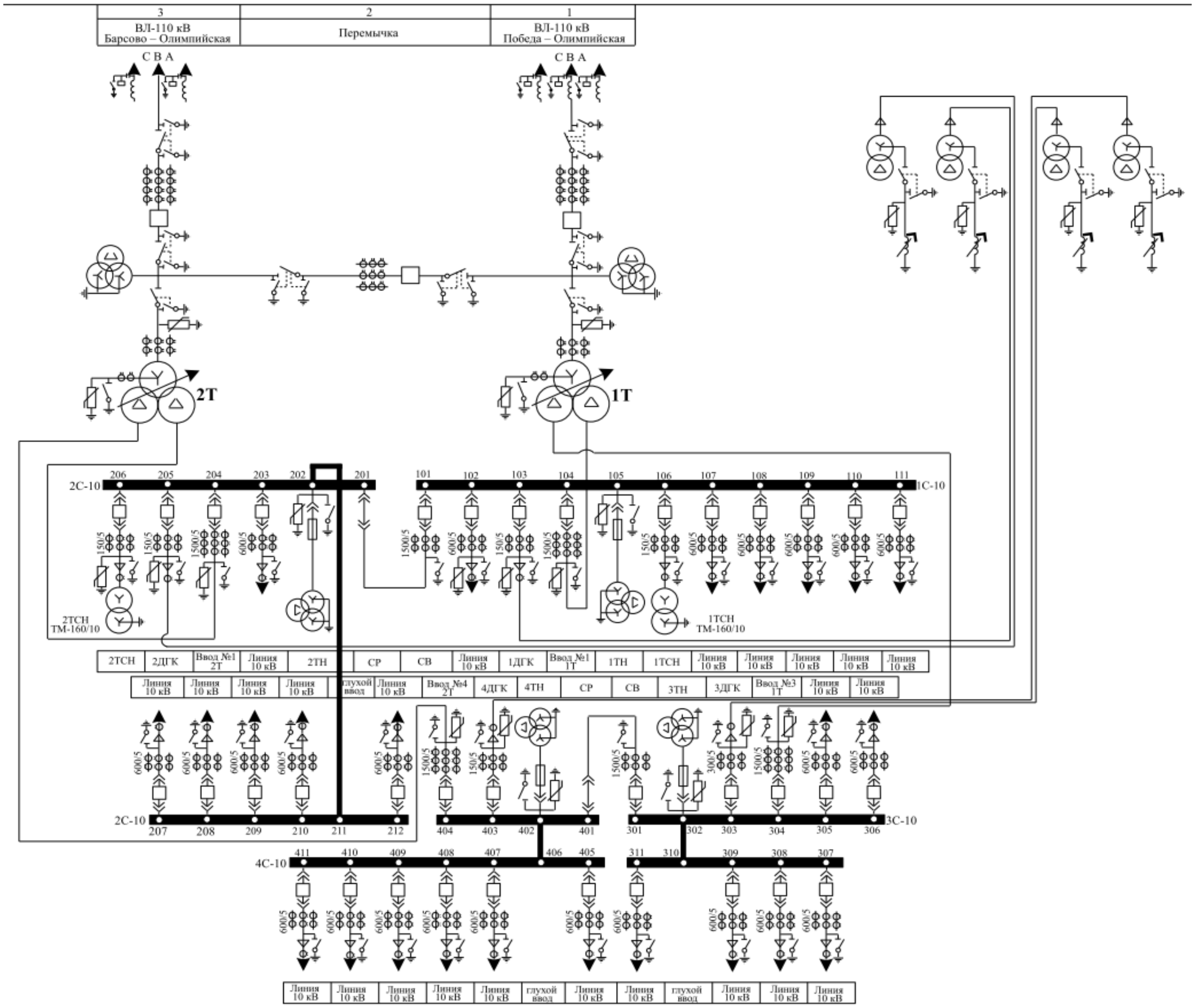


Figure 35. Single line diagram of 110 kV *Olympic* substation [62].

Protection and related automatics of the two 110 kV power lines include the following functions:

- Line Differential Protection(87L) include an equipment at the remote terminal,
- Three stages of Distance Protection (21P),
- Four stages of Ground (Earth) Overcurrent Protection (51N),
- Instantaneous Phase-to-phase Overcurrent Protection (50P),
- Automatic Reclosing (79), and
- Breaker Failure Protection (50BF).

110 kV busbars are protected by Busbar Differential Protection (87B) function.

110/10 kV Transformer protection and automatics contains following functions:

- Transformer Differential Protection (87T),
- Transformer Overload Protection (51),
- HV-side Time Overcurrent Protection (51P),
- LV-side Time Overcurrent Protection (51P), and
- Automated Voltage Regulator.

10 kV side of transformers connected bus-bars and Feeders are equipped with:

- Two stages Phase-to-phase Time Overcurrent Protection (51P),
- Breaker Failure Protection (50BF),
- Interlocking Overcurrent Busbar Protection,
- Automatic Closing of Bus-tie Breaker,
- Under Frequency Load Shedding, and
- Under Frequency Load Restoration.

5.1.2 Control Subsystem

The control subsystem is associated with operator activity. It is aimed at primary equipment and process monitoring and control. The system includes following functions and possibilities:

- Control and state monitoring of all motorized switching apparatus, such as disconnectors, earth switches and circuit breakers,
- Providing one and two-step (select before operate) control models,
- Automatically performing predefined sequences of operational actions,
- Gathering of analog and discrete data of primary equipment and process parameters and their visual representation at HMIs,
- Access, retrieval and visual representation of archived data including alarm and event lists,
- Bay level and substation level interlocking,
- Transformer tap changer manual control, and
- Remote control of system parameters like settings of protection and control algorithms.

All the above control functions are accessible to operator via local HMIs as well through local and remote SCADA using the virtual telecontrol gateway provided by iSAS software.

5.1.3 Revenue Metering System.

The revenue metering system was implemented in compliance with energy market rules and contains following functionalities:

- Active Energy and Power metering,
- Reactive Energy and Power metering,
- Energy and power are measured in both forward and reverse directions,
- Storing energy and power in 30 minute profiles for up to 150 days, and
- Integration of the system into existing DSO-scale metering and billing system.

5.1.4 Monitoring and Recording Subsystem

The monitoring and recording subsystem is comprised of two components – alarm and event management (AEM) and transient recording. AEM allows detection of the alarming state of monitored parameters and forms a record in alarm and event lists and archives. Alarming state detection is based on a predefined configuration that includes logical scheme and activation conditions. For example, the open position of circuit breaker will generate alarm if it is not the result of operator action. It is necessary to monitor the signal that has led to opening of switchgear to relate the cause of circuit breaker open state. Possible cases are depicted as logical expression that defines whether to alarm for status of an event.

Some custom LNs were developed to model AEM functions as per IEC 61850. The alarm and event messages are logged and accessed by standard IEC 61850 Log service.

Fault recorder function is able to register currents, voltages, protection start and trip signals, primary equipment states and operational parameters etc. It is possible to register as raw instantaneous values as well as derived calculated parameters like RMS values. Performance and resolution of recording function is enough for recording transient processes like short circuits at monitored equipment. Also, IEC 61850-9-2 LE Sampled Values data streams (80 samples/cycle and 256 samples/cycle) are recorded. The function provides access to records in COMTRADE format as per IEC 60255-24:2013/IEEE Std. C37.111-2013. The recorder covers all control points available by GOOSE and Sampled Values at the substation. Moreover, the COMTRADE format was expanded to allow storage of quality information of IEC 61850 Data Attributes.

5.1.5 Fault Locator Function

This function detects fault locations on both 110 kV power lines. Single-ended measurements are used with a target error of less than 5% of line length.

5.1.6 Power Quality Monitoring Function

PQ monitoring and analysis are harmonized with international standards IEC 61000-4-30 and IEC 61000-4-7, although there are some differences. PQ monitoring is done at all the four busbars of the 10 kV system to comply with the project requirements. The PAC system provides following parameters:

- Frequency deviation,
- Positive and negative voltage deviations,
- Steady-state voltage deviation,
- Voltage dips, Overvoltage and Voltage interruptions,
- Current and voltage harmonics up to 50-th order,
- Subgroup total harmonic distortion (up to 50-th order) for voltage and current,
- Group interharmonic distortion (up to 50-th order) for voltage and current,
- Centered subgroup total interharmonic distortion (up to 50-th order) for voltage and current,
- RMS harmonic components (up to 50-th order) for current and voltage,
- RMS harmonic subgroup (up to 50-th order) for current and voltage,
- RMS interharmonic group (up to 50-th order) for current and voltage,
- RMS interharmonic centered subgroup (up to 50-th order) for current and voltage,
- Positive-, negative- and zero- sequence voltages,
- Zero-sequence voltage unbalance factor,
- Negative-sequence voltage unbalance factor, and
- Sequence power.

5.2 Software-based PAC System Architecture

The core of the designed PACS is the iSAS software suite that allows freedom to decide where and how to place a particular function. The iSAS is not dependent on hardware used and provides freedom to allocate function modules among available computation platforms. Therefore, the logical structure of the system is independent of its physical implementation and both are harmonized by their own rules considering their own requirements. Optimization research was performed to define the most suitable and effective system physical structure for this particular substation.

An optimization procedure was used to gradually approach the desired values of system's quality metrics, starting from the simplest and cheapest structure that provides system operability in required functionality using an iterative approach. The simplest system means:

- No redundancy,
- Maximum functions concentration in single hardware,
- No periodical checking and testing, and
- No diagnostic.

At each next step of the optimization algorithm, one improvement measure is added. The improvement measure is chosen from the list that was ranked by cost efficiency. At the start, the measures with highest efficiency rating are used. PAC functions availability and maximum affordable repairing rate was applied as system's quality metrics. Normative values of system metrics were taken from the conventional PAC system of the same substation. The customer’s requirements, such as placing revenue metering and PQ functionality into a dedicated server with its separate cabinet, were taken into consideration. Optimization studies resulted in the system structure shown in Figure 36.

The optimized software-based PACS structure contains **five** layers:

Layer 1: The first layer is the interface to primary equipment.

This layer is formed mainly by process interfacing devices (PID). The interaction with primary equipment has been accomplished at the 110 kV and 10 kV switchyard cubicles slightly differently. In the 110 kV AIS, significant part of information is exchanged by a redundant interface, while in the 10 kV cubicles the interface with primary equipment does not have a redundant option.

The control and monitoring signals of switching devices of 110 kV incomers bay are connected to Bay Main PID (BMPID) as shown in Figure 37. The current and voltage transformers for protection as well as for metering purposes are connected to BMPID. The BMPID was installed in the cabinet closest to the line AIS CB drive's cubicle. BMPID has modular structure and could be fitted to requirement by addition of appropriate boards into device basket. It has two optical Ethernet interfaces connected to a PRP redundant network. The device implements IEC 61850 XSWI, XCBR, TCTR, TVTR and the other sensor models which can be selected by configuration. BMPID supports both IEC 61850 GOOSE and Sampled Values protocols. Time synchronization of BMPID is accomplished with IEEE 1588v2 protocol. There are redundant 220V AC/DC power supplies installed into devices.

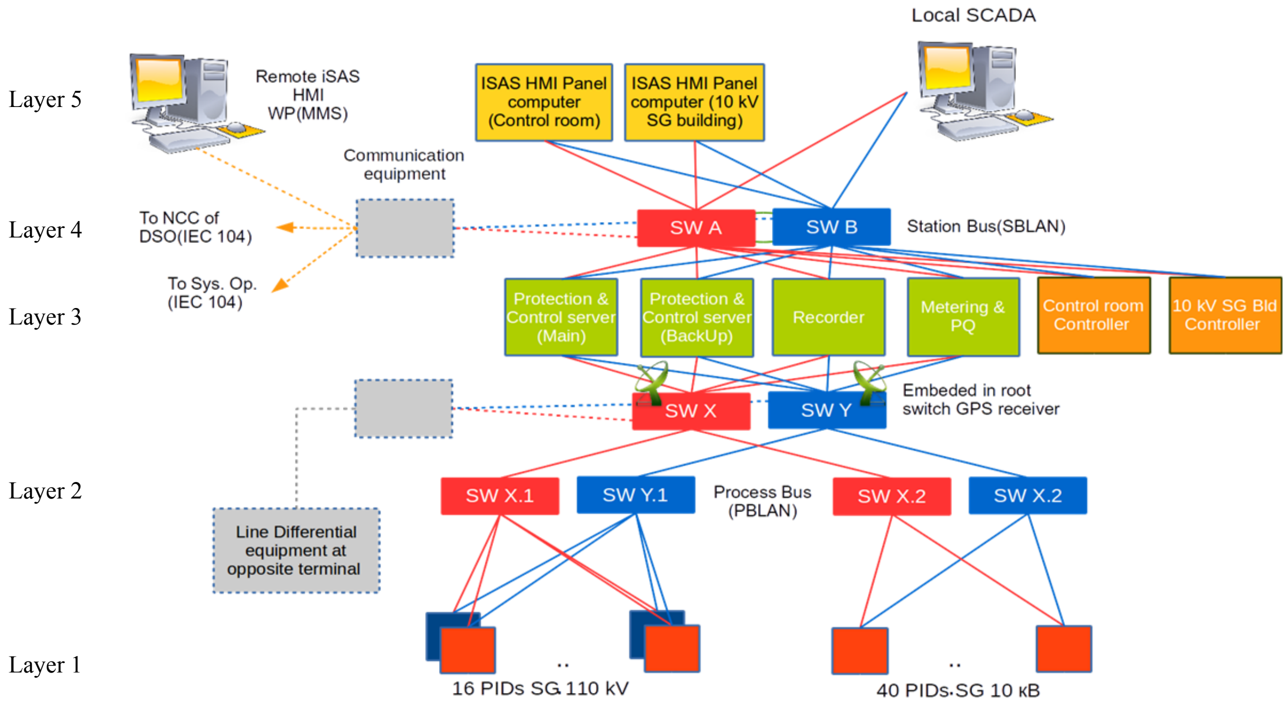


Figure 36. The PACS structure of 110/10 kV *Olympic* substation in Northwest Siberia, Russia [62].

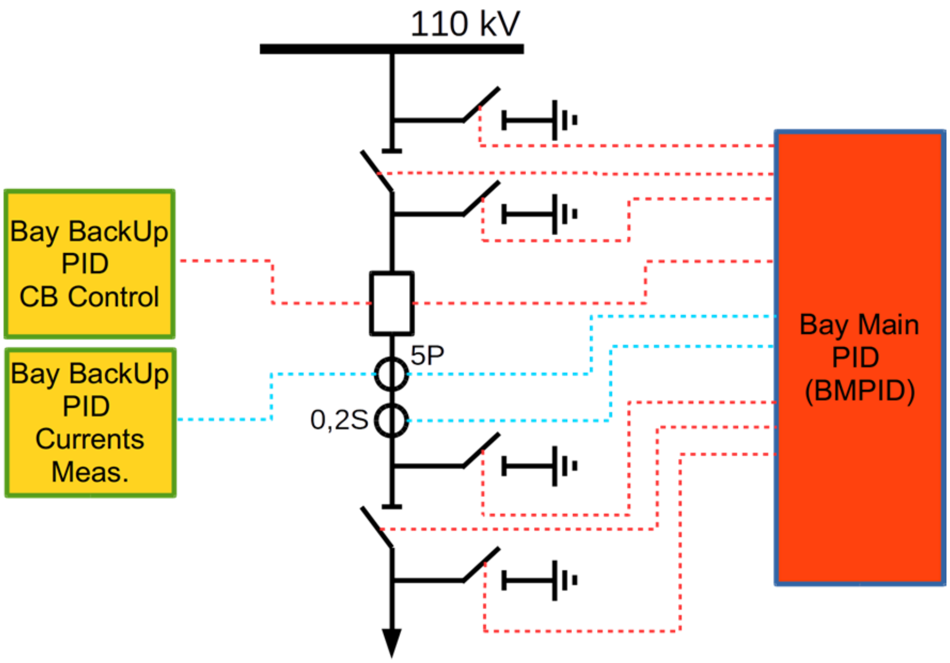


Figure 37. Connections of Main and BackUp PIDs to bay 110 kV apparatus [62].

For redundancy reasons, the measurements of protection currents and voltages as well as circuit breaker control and monitoring functions are duplicated by additional devices. The backup devices were placed in separate cabinet in the switchyard as shown in Figure 38. The backup devices have characteristics like BMPID, and have a fixed set of inputs and outputs in a rugged enclosure. Several devices are installed in the 110 kV switchyard for redundancy of current and voltage measurements and circuit breaker control. The rigid enclosure with IP 65 protection and extended operational temperature range of -55^{0}C to +70^{0}C allowed the installation of such devices in the AIS substation without any additional shelters. Switchgear emulators have been installed in the BMPID and BackUp PID cabinets as shown in Figure 39, since interaction with primary equipment is not allowed during the trial operation period.

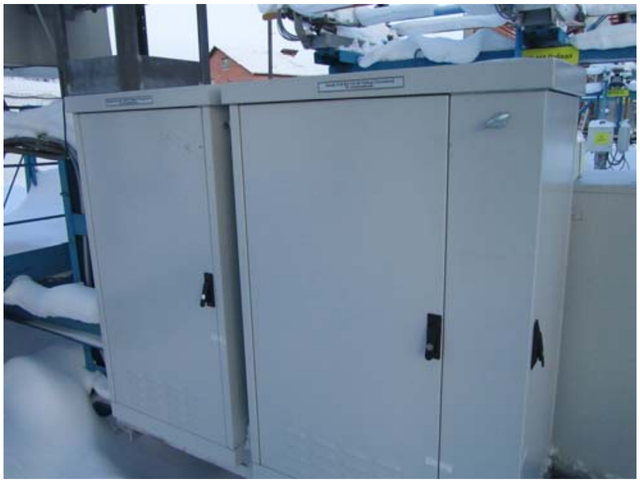
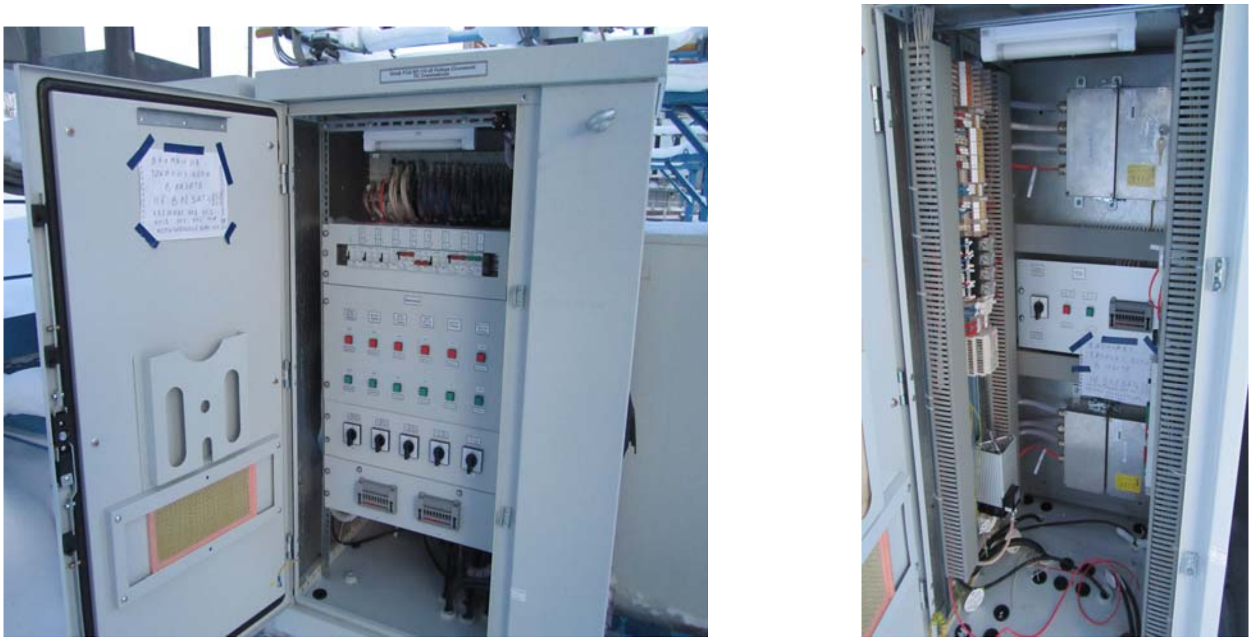


Figure 38. Main and BackUp PID cabinets installed at the 110 kV AIS [62].



(a)

(b)

Figure 39. (a) BMPID cabinet with CB simulator and (b) BackUp PIDs outdoor cabinet with CB simulator [62].

PIDs for 10 kV switchgear are installed directly into cubicles. These PIDs are combined devices and provide measurement of currents from both 0.2S (for revenue metering) and 10P (for protection) coils and also provide control of bay circuit breaker, earth switch and interlocking actuators. 10 kV PID also provides information from arc sensors. These devices do not have redundancy, excluding the 10 kV inputs and tie breakers, because they are required for transformer protection. Station controllers connected to station bus were installed at the substation control room and 10 kV switchgear building to collect data from common equipment like security system, auxiliary supply system, etc.

Layer 2: The layer two of the system is a process bus LAN.

Process Bus LAN (PBLAN) uses double star topology with PRP support. Therefore, all devices connected to PBLAN are double attached network nodes. The PIDs have 2x100BASE-FX interfaces, while data processing devices are connected to LAN with redundant 1000BASE-SX interface. One of the interfaces of the above mentioned devices is connected to the first star with the rest connected to the other star. Connections between PBLAN Ethernet switches inbounds of one star do not have redundancy and transmit data at 1000 Mbit/sec. The Process Bus LAN is based on optical media for better EMC performance than copper wires. Root switches of PBLAN double stars have embedded PTP servers and play the role of a precision timing source for PIDs and other system equipment. A particular source for synchronization is chosen by the Best Master Clock algorithm. The root switches of PBLAN are synchronized with GLONASS satellite system signals. This feature allows implementation of Line Differential Protection and other functions that need exactly synchronized information from different synchronization domains (substations).

Physically the PBLAN is organized by switches that are mounted in the same cabinets as the data processing servers. Moreover, the switches of the different subnetworks are concentrated at different cabinets for reliability reasons. The cabinets where switches and servers are installed are connected with AIS and the 10 kV switchgear building by four (one per subnetwork per direction) trunk multi-fiber cables. The trunk cables have splice boxes at the end where multi-fiber cables are split to individual cables for each connection. Required cable lengths and construction costs are optimized by changing the mounting places of splice boxes at 110 kV AIS and at the 10 kV switchgear building.

The PBLAN switches provide diagnostic information about health of each connection for the PAC system health monitoring function. The SNMP are used for that purpose because the switches do not support MMS. The PBLAN switches support necessary traffic management means as VLAN tagging and filtering as well MAC address based filtering.

PBLAN is also used for communications with equipment on other end of 110 kV overhead lines. These communications gather information from other end of the protected line for Line Differential Protection. There is a dedicated fiber optic channel between substations for these protection-related communications. Information from remote terminals of line is transferred by IEC 61850-9-2 Sampled Values. The format is slightly different from IEC 61850-9-2 LE. Sampled values at 80 samples per cycle are aggregated into a group of 8 samples and sent as single data packet with 8 ASDUs. Thus, the sending frequency is 500 packets per second and the required protection performance and available bandwidth are optimized.

Layer 3: Layer three of the system is composed of computational devices.

Computational devices in layer 3 receive and process input data, make decisions and perform actions according to their algorithms. Based on optimization results, customer requirements and chosen hardware capabilities the complete PACS functionality has been divided among four powerful servers. They are main and backup protection and control servers, a Metering and Power Quality server, and a substation-scale faults and transient events recorder server. The servers were installed into two cabinets, moreover main and backup P&C servers were mounted separately. The cabinets in turn were installed in the existing communication equipment room with strong protection from electromagnetic influences.

As a computational platform for iSAS software deployment, DELL PowerEdge R815 server was selected. All servers are identical and have following characteristics:

- redundant power supply,
- four 2.6 GHz AMD Opteron 6344 CPUs with 12 cores on board of each computer,
- 1000 BASE-SX Ethernet adapters connected to process bus and station bus LANs.

The servers are connected to both LANs as double attached nodes. The servers support the PRP to communicate with field PIDs through PBLAN reliably and seamlessly. Servers are connected to substation bus ring using rapid spanning tree protocol (RSTP). Red Hat Linux OS with real time extensions and iSAS applications are installed in the servers.

Full protection and control functionality for the particular 110 kV substation is performed by 2546 logical nodes. The nodes are distributed among 10 virtual IEDs (vIED). From external perspective, vIED looks like familiar physical IED with its own MMS server and works asynchronously with the other vIEDs even if they are placed at the same computational hardware.

Layer 4: A station bus LAN (SBLAN) represents the fourth layer of the system.

The SBLAN is formed by RSTP ring based on two SBLAN switches. The edge nodes are connected to anchoring switches by a 100 Mbit/s and a 1 Gbit/s Ethernet links.

Several protocols are used in the SBLAN. The main communications use IEC 61850-8-1 MMS reporting, logs retrieval and controlling services. MMS reports are utilized for providing monitoring information about events and operational parameters. The MMS reports are created and sent by physical and virtual IEDs in order to inform devices like HMI and local SCADA about performance of controlled equipment as well as PACS itself. IEC 60870-5-104 protocol is used to communicate with DSO's National Control Center (NCC) and system operator branch office. The iSAS software incorporates the special object (that looks like a virtual gateway) that converts the IEC 61850 information model's data into IEC-104 protocol PDUs based on ideas provided in IEC 61850-80-1.

Besides the protocols mentioned above, another innovative protocol has been implemented in the iSAS software module. The Hypertext transfer protocol (HTTP) based protocol is named CRQ and is used for metering data transfer into DSO's billing system.

The SBLAN connects the iSAS servers from one side, and two operator panels, remote HMI terminal, substation SCADA server and NCC from the other side. Station controllers gather and send common equipment signals to the iSAS servers by MMS reports through station bus network. Physically the SBLAN is organized exactly like the PBLAN. It also uses the same trunk cables at some locations although different fibers are used.

Layer 5: The fifth layer includes operator's interface with PACS.

The fifth layer includes HMIs and NCC as well as other external interfaces to provide interaction of computational core of PACS with operational crew and control centers of DSO and system operator.

Two operator panels (OP) with iSAS HMI software and dedicated SCADA system were installed at the substation to meet Russian regulatory standards and customer requirements. Operator panels are placed at the substation control room and 10 kV switchgear building to allow the crew to control and monitor primary apparatus from both buildings. The operator panel is a touch screen computer with redundant power supply and two Ethernet interfaces connected to SBLAN as double attached node.

The software that is installed at the operator panel is a part of iSAS suite and represents powerful visualization tool based on mosaic-like concept. Each small piece of interface like lamp or button is an element of the complete picture; that has inputs, outputs and parameters. They look like a logical node. It is easy to combine these components to obtain an interface of any required view and functionality. The IEC 61850 MMS client underlies the modular visual representation engine.

The iSAS HMI configuration, including visualization, is an essential part of overall substation configuration file (SCD). The HMI description rules were developed by LYSIS engineers and based on IEC 61850-6 SCL and with its legal extension. There is a special configuration tool for visual construction of HMI's screens. Operator panel gives personnel access to information about substation equipment operational parameters:

- real-time view of general information in the form of one-line diagram,
- event and alarm lists with filtering,
- indicators, tables ,curves, vector diagrams,
- capability to change the controlled equipment state such as motorized switchgear, tap changer,
- ability to manage a parameters of PAC algorithms like active protection setting group, and
- possibility to observe state and health of PAC system equipment.

Although, installation of additional iSAS servers and HMI SCADA system appears to be excessive, it mainly duplicates the iSAS functionality as per the customer’s request. The SCADA interacts with iSAS servers by IEC 61850 MMS services as well.

One remote operator workstation with iSAS HMI software and exactly same capabilities as panels on substation was installed at the DSO office. Two interfaces were organized for exchanging selected data with remote control centers. The first one is a communication channel to system operator branch office. There is only monitoring data exchange by this link. Second one is communication with NCC of the DSO. There are both monitoring and control data exchange in this link. Both interfaces use IEC 60870-5-104 protocol. Communication equipment for both channels is connected to SBLAN segment by redundant connections.

6. EMERGING AND FUTURE APPLICATIONS

This section discusses some of the emerging and future applications for the power system protection and control. This will require a paradigm shift in the way we approach the engineering, operation and maintenance of the power system protection and control. Some of these applications can only be applied with a CPC approach while others will significantly benefit in having the high-performance computing platform at the substation. CPC will enable the development of newer applications for robust and flexible protection and control system that can be replaced without any downtime at the end-of-useful life with an overall reduced ownership cost with enhanced benefits to the user.

6.1 Dynamic State Estimation Based Protection

One of the most secure protection functions is differential protection. An additional advantage of differential protection is that it does not need coordination with any other protection functions. The principle of differential protection is that the sum of currents into a specific protection zone must equal to zero. Thus if the relay monitors the sum of the currents and the sum is near zero then the differential protection logic indicates normal operation. If the sum of the currents becomes substantially different than zero the differential protection function concludes that there is an internal abnormality in the protection zone.

The principle of monitoring a physical law (Kirchhoff's current law in the case of differential protection) can be extended to include other physical laws that a protection zone must obey, such as Kirchhoff's voltage law, electro thermal laws, magnetic flux versus voltage laws, etc. All the physical laws that a protection zone must satisfy are expressed in the mathematical model of the protection zone. The mathematical model is a set of equations in terms of the various variables of the model, such as voltage, current, magnetic flux, temperature, etc. This principle is illustrated in Figure 40. Monitoring of the validity of all these equations by measuring certain quantities and determining whether the measured quantities satisfy the model equations can be done in a systematic and mathematically rigorous way via dynamic state estimation (DSE) procedures. Details of the DSE can be found in the literature [63].

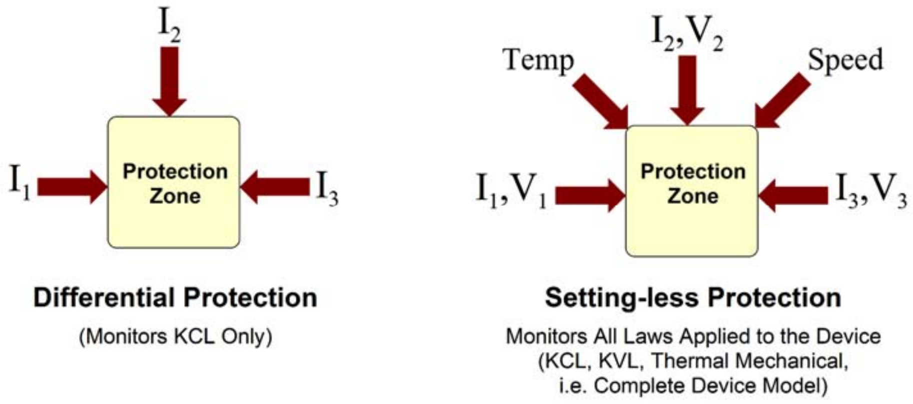


Figure 40. Illustration and comparison between Differential protection and Dynamic State Estimation based protection (a.k.a. Setting-less protection).

The DSE based protection method (a.k.a. setting-less protection) requires a monitoring system of the component under protection that continuously measures terminal data, (such as the terminal voltage magnitude and angle, the frequency, and the rate of frequency change - this task is identical to present day numerical relays), other variables such as temperature, speed, etc., as appropriate, and component status data (such as the tap setting, breaker status, etc.). The DSE processes these measurements and determines whether the measurements are consistent with the model of the protection zone, i.e. whether the measured data "fit" the model. A good fit between the measurements and the model equations indicates normalcy and also provides an independent verification of the model of the protection zone. This is why many times we refer to this procedure as providing the real time dynamic model of the protection zone.

The DSE based protection requires settings similar to differential protection and no coordination with other protection functions. The settings are in terms of thresholds similar to differential protection as well as limits on operating characteristics of the protection zone, for example maximum permissible operating temperature for a transformer. The thresholds can be quite refined and expressed in statistical terms or in terms of probability that the measurements do not fit the model of the protection zone. This type of threshold is implemented within the DSE and provides a reliable way to detect internal faults or internal abnormalities of the protection zone. For example, the DSE can provide the probability that the measurements fit the protection zone mathematical model within the instrumentation metering error. When this probability goes to zero, it indicates an internal abnormality in the protection zone. Because of the simplified settings of the dynamic state estimation based relay, the approach has been also named setting-less protection.

The more accurate the instrumentation is the more sharp the detection of the fault condition becomes. It is well known that merging units can provide the most accurate instrumentation for relaying by virtue of the fact that they eliminate the errors introduced by long control cables, increased burdens on CTs and VTs, induced voltages on instrumentation cables and other sources of error. For this reason it is recommended that setting-less protection be used with merging units to obtain better protection.

Figure 41 shows an overall generic demonstration of the setting-less protection approach. Figure 42 illustrates the data flow. Note that the implementation shown in the figure operates on two consecutive sets of sampled data. The model of the protection zone is in the Quadratic Algebraic Companion Form. The end results of the DSE are estimates of the measurement as well as estimates of the protection zone state. Because the state estimation operates on sampled data, any changes in the protection zone will be "seen" by the relay immediately, as soon as the processing of two sets of consecutive sampled data has been completed. Typical relaying instrumentation operates at sampling rates of 2.4 ks/s to 10 ks/s. This means that the dynamic state estimation is performed every 200 microseconds for a sampling rate of 10 ks/s to 833 microseconds for a 2.4 ks/s rate.

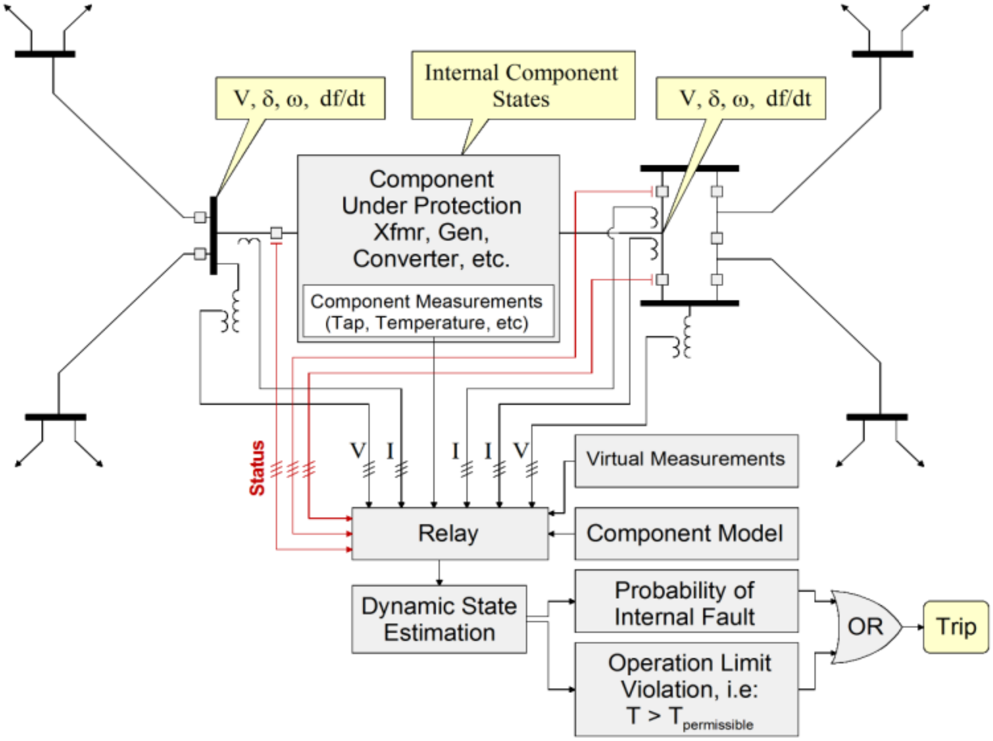

V, δ, ω, df/dt
Internal Component States
V, δ, ω, df/dt
Component Under Protection Xfmr, Gen, Converter, etc.
Component Measurements (Tap, Temperature, etc)
Status
V
I
I
I
V
Virtual Measurements
Relay
Component Model
Dynamic State Estimation
Probability of Internal Fault
Operation Limit Violation, i.e: T > T permissible
OR
Trip

Figure 41. Illustration of Setting-less component protection system .

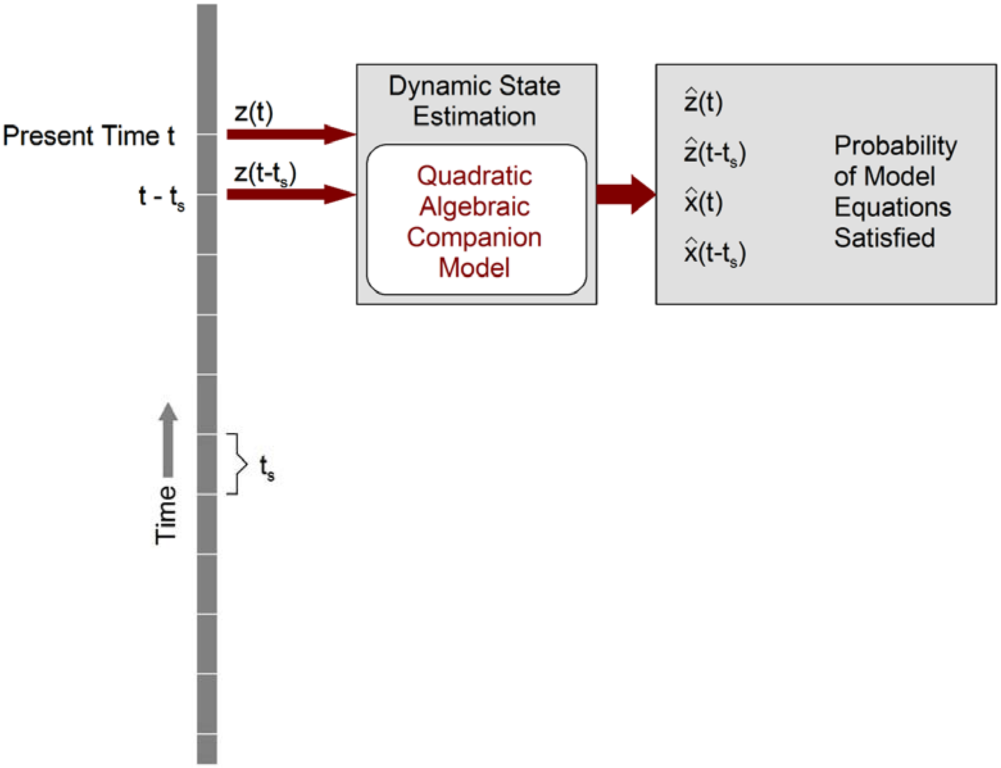


Figure 42. Illustration of data flow and computations of a Setting-less protection function.

Typical results with the DSE approach are shown in Figure 43 for a capacitor bank. The results show actual and estimated three phase voltages at the terminals of the capacitor bank (first set of traces: six are shown – three measurements and three estimated values). Note that there are two events in this period: an external fault and an internal fault (one capacitor can failure). Note that during the external fault the measured and estimated voltages are very-very close, there is no distinction by looking at the graph. During the internal fault there are noticeable differences between the measured and estimated voltages. The second set of traces show the measured three phase currents at the terminals of the capacitor bank and the estimated values of the currents via the DSE. Note that during the external fault the measured and estimated currents are very-very close, there is no distinction by looking at the graph.

During the internal fault there are noticeable differences between the measured and estimated voltages. The third trace is the confidence level, i.e. the probability that the measurements fit the model of the capacitor bank within the accuracy of the instrumentation. Note that the confidence level is 100% for all cases including the period of time during the external fault and it goes to zero during the internal fault. The fourth trace is the trip/no trip signal. This signal is the integral of the confidence level over a rolling time window times a constant and minus another constant. The constants are so selected that the trip signal is zero when the confidence level is 100% for a period of the rolling window and it is one when the confidence level is zero for at least a period equal to the rolling time window. When the confidence level goes to zero, then the trip signal will become one after a short delay depending on the selection of the rolling time window. Comparing the third and fourth traces one can see how the protection function works. Finally the last trace shows the execution time for each one of the state estimations. Note that execution times are in the order of 1.5 to 3 microseconds for this example.

Another advantage of the DSE based protection is that the protection continuously monitors the validity of the protection zone model. In addition parameter estimation methods can be integrated to fine tune the parameters of the protection zone model, if necessary. The end result will be that the DSE based protection will have a validated model of the protection zone. It can then make this model available to other applications. Since each application may need the model in a specific form and format, a filter can be employed to transform the model from the DSE based protective device format to the specific format of the specific application. All of these functions are shown in Figure 44.

A comparison between traditional approach and DSE based protection using CPC is shown in Table 6.

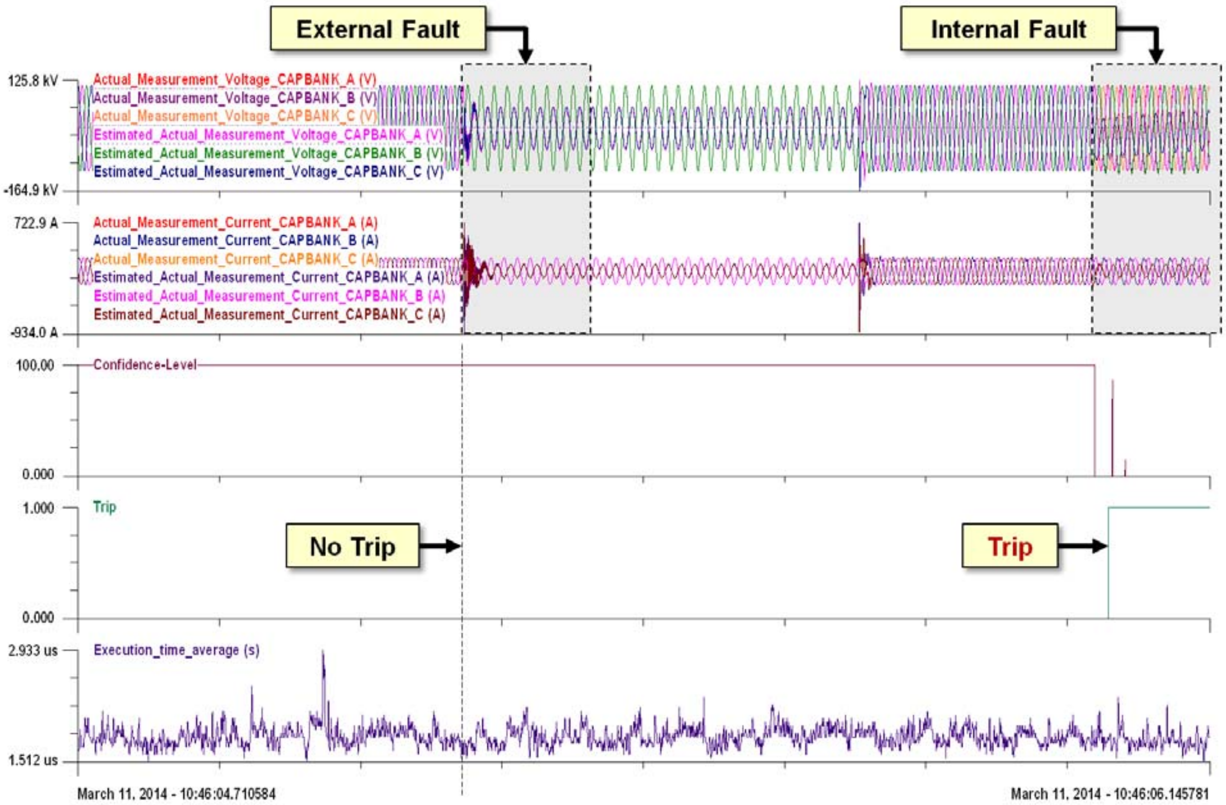


Figure 43. Example performance of a Setting-less protective relay.

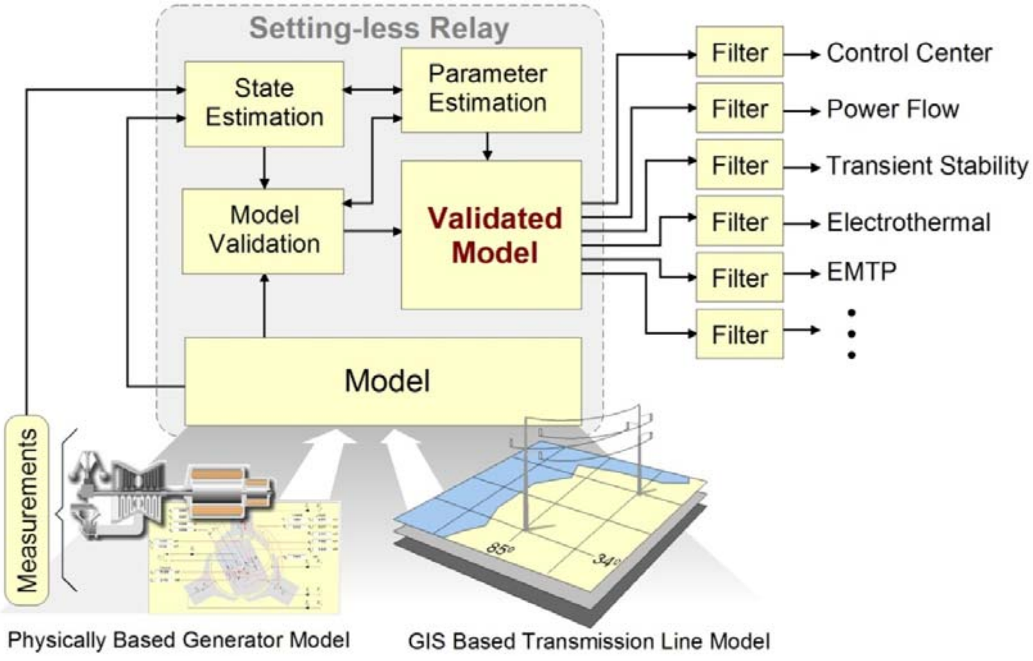


Figure 44. Setting-less protective relay as the gatekeeper of the Protection Zone model.

Table 6. Comparison between traditional approach and DSE based protection using CPC.

Feature	Traditional Approach	DSE based protection using CPC
Power System Model	Model is developed and maintained by humans and prone to error.	Model is continuously validated via dynamic state estimation. CPC transmits the validated model upstream (substation, control center, enterprise, etc.). Models are available with minimum latencies. Models can be used for other applications in a process that is Free of Human Error.
Internal Relay Method	Some approaches are simplistic but others can be somewhat arcane and requires expert knowledge to apply and troubleshoot.	Capitalizes on simple laws of nature (and specifically that the protection zone must obey): KVL, KCL, thermal, mechanical, etc.
Setting Process	Protection setting has become a very complex process requiring compromise among conflicting factors and subject to human error. In addition, with IEDs the settings may require multiple organizations to complete the setting task. For example, protection, SCADA, and asset management may all need to provide input into the settings.	Reduces complexity and reduces potential for human error. Also capable of protecting against traditionally problematic faults such as 1. Faults near neutrals of generators or transformers, faults in series compensated lines 2. High impedance faults / downed conductors 3. Load encroachment, etc.
Setting Calculations	Setting calculations require power system fault studies and relay setting tools be employed to determine appropriate settings and coordination.	Settings determined automatically by the DSE based protection.
Setting Management	Each relay contains the settings and is maintained separately. System changes may require re-computation of settings.	Single system contains the rules for the CPC based protection approach. System changes do not influence the process.

6.2 Pattern Recognition Based Protection

Pattern recognition essentially involves selecting representative features from a certain dataset, and mapping the selected feature(s) to class(es). The main idea behind feature selection is to retain the optimum salient characteristics necessary for the recognition process and reduce the dimensionality of the measurement space, so effective and easily computable algorithms/methods can be devised for classification.

An example of feature selection known to relaying engineers is the resolution of a time series signal into a spectral coefficient corresponding to the fundamental waveform using Discrete Fourier Transform (DFT), and then using the coefficient for classification using simple rules – e.g., over/under voltage/current. In some cases, coefficients corresponding to other harmonics are extracted as well, and more rules are used to classify. In this case, the original measured data are a time series, DFT is the feature extraction method to create a feature space, and the classifier is constructed of simple rules.

In the area of analyzing *time series*, there are over a dozen feature extraction and dimension reduction approaches. Some classical representatives are Discrete Fourier Transformation (DFT), Single Value Decomposition (SVD), Principal Component Analysis (PCA), Discrete Cosine Transformation (DCT), Discrete Wavelet Transformation (DWT). More recently, we see more advanced dimension reduction approaches such as Piecewise Aggregate Approximation (PAA), Adaptive Piecewise Constant Approximation (APCA), Chebyshev polynomials (CHEB), Symbolic Aggregate approXimation (SAX), Indexable Piecewise Linear Approximation (IPLA). All these methods transform the original data series. Another recent trend is to extract representative subsequences in the original data series as features. Time series shapelets falls under this category. Despite all these approaches, there is no superior *general* feature extraction method in *all* the situations.

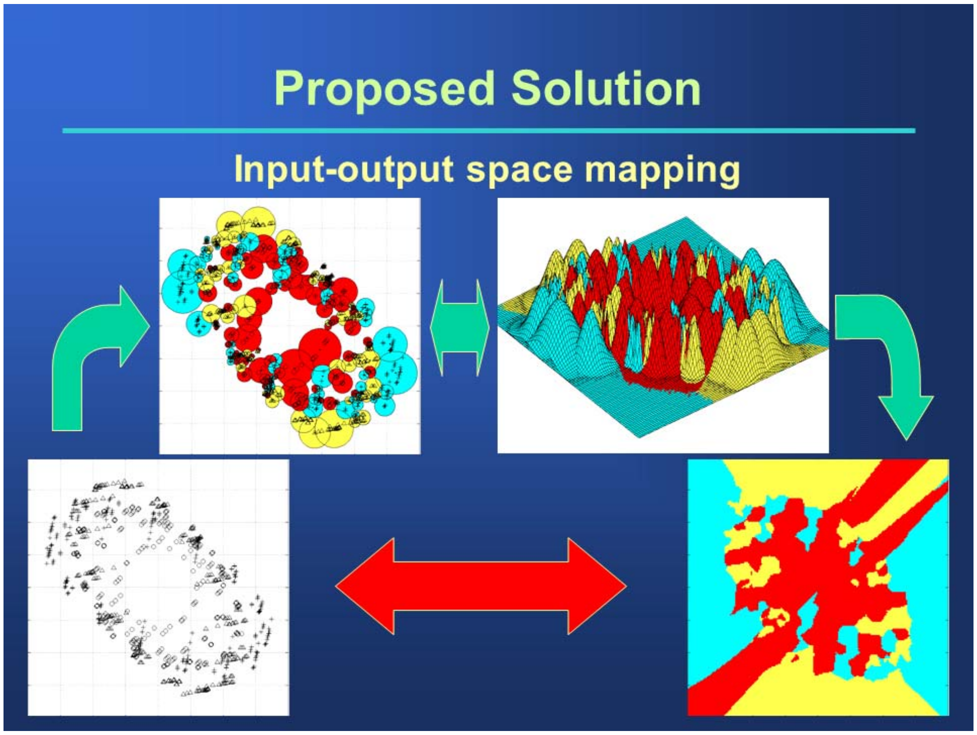
In many cases, simple threshold based classification may not be possible. In such cases more advanced methods are used to map features to classes. Supervised classification, which is the most relevant to our purpose, involves previously known classes, and known representatives from each class, also called ground truths. This information is used for making the classifier *learn* the features, so later, when a feature set with unknown class is encountered by the classifier, it is able to classify the feature set correctly. Well known classifiers include, but are not limited to Bayesian Classifier, k-Nearest-Neighbor (kNN), Support Vector Machine (SVM), Expert Systems, Decision Tree, Neural Network, Genetic Algorithms (GA). For patterns that may include information overlapping across classes (vague), Fuzzy approach is also used.

Most relaying functions are essentially a classification. However, the classification is in most cases based on thresholds and/or simple rules. Learning is not required for such functions. Moreover, availability of real-world data for training any classifier-based relays is a challenge. The fact that such relays would have to be retrained if used for another part of the power system is also a drawback.

6.2.1 Pattern Classification Based Protection

The concept of using pattern recognition is to employ well known heuristic methods that look at input signals and based on particular signal properties (features) captured through techniques such as neural network of fuzzy logic, classify such properties into domains that differentiate between faulted states and normal states, and also allow classification of fault types and other fault properties such as location, fault resistance, etc. [64]. An example of such an approach using neural networks is shown in Figure 45. Further details are given in [65] and [66]. Going from left hand lower corner clockwise, one can note the steps involved in this process, which is actually reduced to input-output space mapping using neural networks.

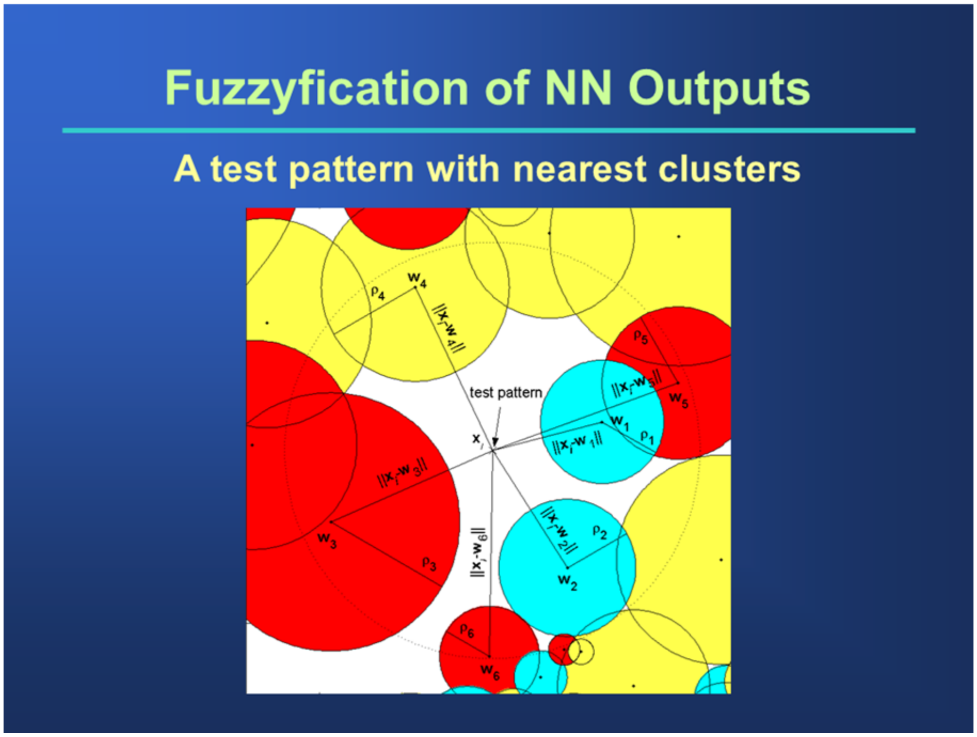
Fuzzyfication of NN outputs: In this case, as shown in Figure 46, a k-nearest method enhanced with fuzzy variables is used to fill in the gaps in the pattern space. Filling in the gaps is actually done by associating the new patterns that fall in the space between the clusters to a given cluster based on the k-nearest principle. In this case, the regions for category classification are extended beyond the clusters and any new pattern can be recognized as a particular type of event. This way the last two steps in the input-output space mapping shown at the beginning are accomplished. This example illustrates how differentiation between different events, including fault types, can be made using just the input patterns and no settings at all. This approach can be combined with the traditional approach to improve dependability/security, as well as an automated analysis of a protection system [67], [68].



Proposed Solution

Input-output space mapping

Figure 45. Mapping from sample (feature) space to fault/no-fault patterns.



Fuzzyfication of NN Outputs

A test pattern with nearest clusters

**Figure 46.	Fuzzyfication approach.**

6.2.2 Wide Area Protection

Power blackouts over the world have shown that power systems, though carefully planned and protected, suffer from unforeseen events triggering instability. Such events often include misoperations of relays that result in unintended line trips, load shedding and generation trips. Such misoperations are unchecked because global knowledge about the actual system condition is lacking. In the form of global knowledge related to tripping, the control centers simply acquire relay trip flags, circuit breaker (CB) status flags, and sometimes line currents and voltages for more reliable interpretation of these flags. These signals in most cases do not convey whether the trip was as per design (correct) or it was a misoperation.

Blackout logs [69, 70, 71] have shown many instances of relay misoperations that either triggered or accelerated the blackouts. It is crucial to realize that there is no way for system operators to know in near-real-time if the tripping of a relay/CB was as per design (correctly responding to an event), or a misoperation (operating in absence of event, or responding to an event it was not designed to detect). Therefore, there is no way to reverse the misoperation and bring back the part of the system that could avert a catastrophic outcome. In many of the blackout events described in [69-71], there was enough time to reverse the triggering event, as well as load encroachment trips, which could have probably averted or at least significantly alleviated the blackout.

A survey was performed by IEEE Power System Relaying Committee (PSRC) to evaluate the performance of relay systems over four years (2000-2004) [72]. For four representative utilities, the yearly misoperations during that period were 15.4%, 9.5%, 52.6%, and 28.6% at 345 kV voltage levels. Comparable numbers were reported at other voltage levels. Even System Integrity Protection Schemes (SIPS), which are specifically designed to prevent the system from hurtling into blackout, suffer from misoperations [73].

From observations made above, it is evident that the power system can benefit from a global layer of knowledge that oversees the relay and CB operation. This knowledge will either corroborate the relay action, or invalidate it. In case the relay/CB action is invalidated, the resulting loss of system component(s) should be brought back in, and the corresponding relay blocked for the time being. This action can result in averting or significantly alleviating outage due to a potential blackout. It is important to mention here that in case the supervisory knowledge is inaccurate, and results in erroneous disabling of a relay, the backup relay will operate and remove the fault. This may result in some loss of selectivity, but the advantage of this approach certainly outweighs this unintended outcome.

To work towards such a system, disturbance signatures from Phasor Measurement Units (PMUs) can be utilized. Pattern recognition can be very useful to classify disturbances using features extracted from disturbance files. Some studies in event identification using pattern recognition and classification have already been reported in [74, 75, 76, 77]. Results in [74, 75] are based on computer simulations, whereas study described in [76, 77] use real world PMU data from four PMUs for pattern recognition and classification.

6.3 Time Synchronization Based Protection and Control

Examples of protection and control applications that require time synchronization vary. Generally, any applications that use digital samples of measured analog values sourced from different locations require that these samples are time synchronized, with high accuracy.

Line current differential protection, commonly implemented today, exchanges time synchronized digital samples for the current measurement at local and remote ends of the line. An example of a line current differential application using a multiplexed channel using IEEE C37.94 is shown in Figure 47. Time synchronization to a relative time, i.e. common time for the devices located at each line end, is generally used for this application, while synchronization to absolute time is preferable. Proprietary data exchange protocols and time synchronization methods are used today. Both can be carried over to IEEE C37.94 data format. GPS time synchronization is also common using IRIG-B interfaces.

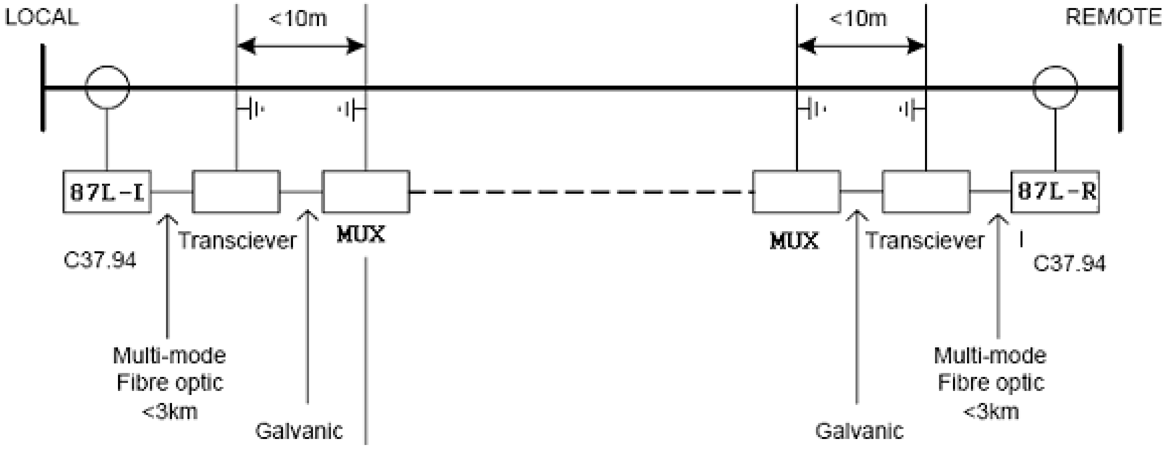


Figure 47. Example of line current differential application.

Protection and control applications using digital samples provided by IEC 61850 Merging Units (MU) also require time synchronization. Again, relative time synchronization among MUs may be used, while synchronization to absolute time is preferable. The IEC 61850-9-2LE UCA Implementation Guidelines specifies the use of 1PPS signal for MU time synchronization.

Emerging time synchronization uses IEEE 1588 Ethernet-based time synchronization for merging units based upon IEEE C37.238, with harmonization underway as IEC 61850-9-3.

Emerging fault locator applications using traveling wave technology also require accurate time synchronization. Relative time synchronization among two or more line terminals is sufficient, but time synchronization to absolute time using GPS is commonly used. For these applications the accuracy of time synchronization defines the accuracy of resulting fault location.

Protection and control applications that use synchrophasor measurements require time synchronization to an absolute time. These systems are typically deployed over a wide area, so time synchronization to GPS is commonly used. Synchrophasor has been successfully used for interconnection protection of distributed generation sites (anti-islanding protection), automatic generation shedding schemes (separate or as a part of remedial action schemes), wide-area control of FACTs, wide-area fault locator, etc. Example of wide-area synchrophasor-based Static Var Compensator (SVC) control is shown in Figure 48.

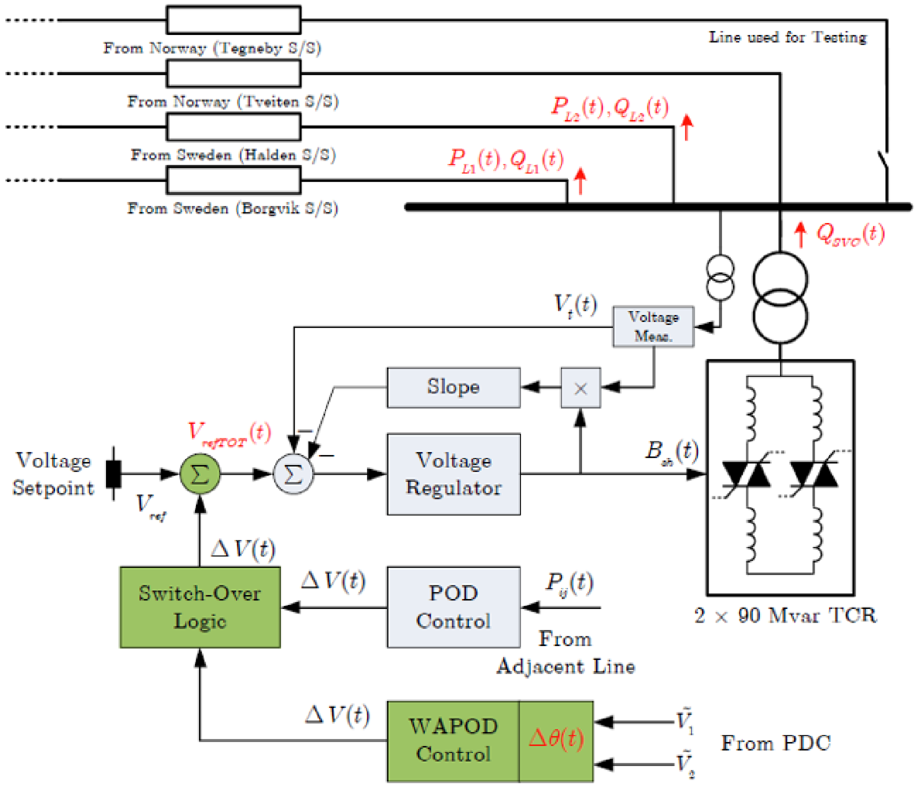


Figure 48. Wide-area control of SVC using synchrophasor measurements.

7. Conclusions and Recommendations

Advancements in protection and control technologies related to centralized protection and control (CPC) systems, within a substation, have been reviewed in this report. The evolution of protection and control systems with specific emphasis to CPC has been presented. It has been shown that existing technologies are mature enough to support the deployment of CPC. Advancements in sensor, merging units, and remote I/O technologies enable convenient collection of power system data at any location within a substation, independent of the location of protection and control devices due to the availability of standardized communication technology. The convenience is mainly due to the large reduction in number of cables and their interconnections. Communication technology based on PRP and HSR provides a standardized option for streaming sampled value data with a high degree of reliability from the IMU to the CPC. The same physical communication link using optical fibers can be used for sending GOOSE commands from CPC to the IMU for closing and opening of switching devices or changing taps in a transformer. Receiving GOOSE messages provides switching devices statuses using the same link between IMU and CPC.

Use of optical fiber is critical for communication between IMU and CPC and enables the use of off-the-shelf hardware for protection and control systems exploiting the optical isolation provided by the communication link. The availability of high-performance computing systems using server technology shows promise for the CPC systems hardware. One of the main advantages of this approach is the efficient management of end-of-life of hardware. Since the server technology is used by many sectors other than the power, the availability of next generation of hardware appears to be guaranteed at a competitive price and users will have much wider choices for hardware supplier. In many cases, selection of hardware and software can be decoupled; allowing users to select hardware systems based on their experience in other areas of their enterprise. It will also be liberating for IED suppliers who spent considerable cost, time and effort in managing component obsolescence and eventually has to pass on the expenses to the users to be competitive. IED manufacturer has little control over the component suppliers, due to low volume, unlike the control exercised by server manufacturers on their suppliers. CPC have to meet applicable standards for substation environment.

The report did not specifically discuss the software environment of CPC systems. However, one such example is available in the demonstrated project discussed in the report. The software environment of CPC systems should be discussed while proposing a recommended practice/guide for CPC systems to meet the requirements and challenges of implementing CPC software.

This report proposes possible architectures for the application of CPC systems using the emerging technologies. An example of the application of a CPC system in a typical substation was presented. Further, reliability and cost analysis examples are presented for comparison among the architectures. Testing and maintenance aspects for a substation with a CPC system are also discussed. As shown by the pilot project discussed in the report the CPC technology is ready for application in the distribution system now. Development of a recommended practice guideline in the use of CPC systems may accelerate the deployment of such systems for distribution networks. These systems will be helpful for advancing distribution automation that can accommodate high penetration of distributed energy resources. There are more opportunities to apply CPC systems in distribution networks as these systems are continuously upgraded and/or expanded. Based on the experience in the distribution system, the CPC technology can then be applied to other parts of the power system.

Promising emerging and future applications that can exploit the CPC approach have also been briefly reviewed in the report. These novel applications, when appropriately applied, significantly improve the reliability of protection and control systems and the power grid at an affordable cost - with enhanced capability and maintainability for both hardware replacement and software upgrade. The implementation of CPC approach will require a paradigm shift in the way we design, manufacture, install, test, operate and maintain a protection and control system as highlighted in the report.

8. Bibliography

1 A. Wright and P.G. Newbery, Electric Fuses, Institute of Electrical Engineers, Power Series 2, 1982, ISBN 0-*906048-78.*

2 B. Lundqvist, "100 years of relay protection, the Swedish ABB relay history," ABB Automation Products, Substation Automation Division, [Online]. Available: http://www05.abb.com/global/scot/scot296.nsf/veritydisplay/c1256d32004634bac1256e19006fd705/$File/PAPER_2001_08_en_100_Years_of_Relay_Protection__the_Swedish_ABB_Relay_History.pdf

3 *Substation Control and Protection System – System Requirements Specification*, Prepared by Westinghouse Electric Corporation for EPRI Research Project RP-1359-1, April 1980.

4 *Integrated Protection System for Rural Substations – SIPSUR,* GE Protection & Control and Union Electrica Fenosa (Spain) under a PIE research project, 1990.

5 P. Norberg, A. Fogelberg and A. Johnsson, "Field Experiences From Using PC Software for Protection and Control of AC Substations," B3-208, CIGRE 2006 General Session.

6 M.S. Sachdev (Coordinator), et al., Computer Relaying, Tutorial Course Text, Institute of Electrical and Electronic Engineers, New York, N.Y., U.S.A., Pub No. 79 EH0148-7-PWR, 1979.

7 M.S. Sachdev (Coordinator), et al. Microprocessor Relays and Protection Systems, Tutorial Course Text, Institute of Electrical and Electronics Engineers, Piscataway, N.J. U.S.A., Pub No. 88EH0269-1-PWR, 1988.

8 M.S. Sachdev (Coordinator), et al, Advancements in Microprocessor Based Protection and Communication, IEEE Tutorial Course, Institute of Electrical and Electronics Engineers, Piscataway, N.J. U.S.A., Pub No. 97TP120-0, 1997.

9 *Understanding microprocessor-based technology applied to relaying*, IEEE Power System Relaying Committee WG I16 Report, 2009, Available at: http://www.pes-psrc.org/Reports/Apublications_new_format.htm.

10 F.H. Last and A. Stalewski, "Protective Relay Gear as a Part of Automatic Power System Control," IEE Conference Publication 16, Part I, March 1966.

11 *Glossary of Some Telemetering Terms*, Electrical Engineering, vol. 74, issue: 2, pp. 156, February 1955.

12 *Supervisory Control and Data Acquisition (SCADA) in Liquid Pipelines*, PB2005-917005, National Transportation Safety Board.

13 *Communications technology for protection systems*, IEEE Power System Relaying Committee Report by WG H9, 2013, Available at: http://www.pes-psrc.org/Reports/Apublications_new_format.htm.

14 IEEE Std C37.236™ - 2013 IEEE Guide for Power System Protective Relay Applications Over Digital Communication Channels.

15 G. D. Rockefeller, "Fault protection with a digital computer," IEEE Transactions on Power Apparatus and Systems, Volume: PAS-88, Issue 4, 1969, 438-464.

16 G.B. Gilcrest, G.D. Rockefeller and E.A. Udren, "High-Speed Distance Relaying Using a Digital Computer I - System Description," *IEEE Transactions on Power Apparatus and Systems*, Volume:PAS-91, no. 3, pp. 1235 – 1243, 1972.

17 G.D. Rockefeller and E.A. Udren, “High-Speed Distance Relaying Using a Digital Computer II-Test Results,” *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-91, no. 3, pp. 1244 – 1258, 1972.

18 J.S. Deliyannides, M. Kezunovic, T.H. Schwalenstocker, “An Integrated Microprocessor Based Substation Protection and Control System,” *Developments in Power System Monitoring and Control*, IEE, IEE Conference Publ. No. 187, London, England, April 1980.

19 J.S. Deliyannides and E.A. Udren, “Design Criteria for an Integrated Microprocessor-based Substation Protection and Control System,” *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-101, no.6, pp. 1664 – 1673, June 1982.

20 Nilsson et al., “Pros and cons of integrating protection and control in transmission substations,” IEEE Transactions on Power Apparatus and Systems, vol. PAS-104, no. 5, pp. 1207 – 1224, May 1985.

21 E.A. Udren and J.S. Deliyannides, “Integrated System for Substation Relaying and Control Shows Benefits,” IEEE Computer Application in Power, vol. PAS-101, no. 6, pp. 21 – 27, January 1989.

22 Madani et al., “Distribution Automation Strategies Challenges and Opportunities in a Changing Landscape,” in Proc. *IEEE Trans. Smart Grid*, doi:10.1109/TSG.2014.2368382, vol. 6, no. 4, pp. 2157-2165, July 2015.

23 Bollen et al., “CIGRE/CIRED/IEEE Working Group C4.24 – Power Quality in the Future Grid – Status Report,” in Proc. of the *CIRED 23rd Inter. Conf. Electricity Dist.*, Lyon, France, June 2015, Paper 0181.

24 Das et al., “Distribution Automation Strategies: Evolution of Technologies and the Business Case,” in Proc. *IEEE Trans. Smart Grid*, doi:10.1109/TSG.2014.2368393, vol. 6, no. 4, pp. 2166-2175, July 2015.

25 *End-Of-Life Assessment of P&C Devices*, IEEE Power System Relaying Committee WG I22 Report, 2015, Available at http://www.pes-psrc.org/Reports/Apublications_new_format.htm.

26 C.F. Henville, “Multifunctional Protection IEDs – How Much Functionality is Too Much? Presented to the PAC World Conference, Dublin, Ireland, June 21-24, 2010.

27 *Optical Voltage and Current Sensor, NxtPhase Incorporated, Phoenix, AZ, US.*

28 Lj. A. Kojovic, “Integration of Protection, Control, and Metering Functions,” 44th CIGRE Session, Paris, France, 2012.

29 A. dos Santos, J. Lourenço, J. F. Martins, P. Monteiro, J. Fitch, T. Rahman , Lj. A. Kojovic, “Relay Protection Solutions based on Non-Conventional Current Sensors in Actual Industrial/Utility Applications,” CIGRE Study Committee B5 Colloquium, Belo Horizonte, Brazil, August 25-31, 2013.

30 *Analog Inputs to Protective Relays from Electronic Voltage and Current Transducers*, IEEE Standard C37.92™-2005.

31 *Instrument transformers – Part 8: Electronic current transformers*, IEC Standard 60044-8™-2002.

32 *Communication networks and systems in substations*, IEC Standard 61850, 2004.

33 *Guide for the Application of Rogowski Coils used for Protective Relaying Purposes*, IEEE Standard C37.235™-2007.

34 IEC 61869-1 Edition 1.0 2007-10 Instrument transformers – Part 1: General requirements.

35 IEC 61850-9-2 Edition 2.0 2011-09 Communication networks and systems for power utility automation – Part 9-2: Specific communication service mapping (SCSM) – Sampled values over ISO/IEC 8802-3.

36 *High-availability Seamless Redundancy (HSR) and Parallel Redundancy Protocol (PRP),* IEC 62439-3 Ed 2.0, 2012.

37 Official U.S. Government information about the Global Positioning System (GPS) and related topics http://www.gps.gov/policy/legislation/loran-c/

38 Proposal for U.S. eLoran Service Gains Ground http://www.insidegnss.com/node/3853.

39 Inter Range Instrumentation Group (IRIG) mod B standard. [Online]. Available: http://irigb.com, May 1998.

40. *IEEE Std. 1588 – 2008, IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems*, IEEE Std 1588-2008.

41 IEEE Std C37.238™-2011, Standard Profile for Use of IEEE Std. 1588™ Precision Time Protocol in Power System Applications.

42 IEC/IEEE 61850-9-3 Draft CDV Communication networks and systems for power utility automation - Part 9-3: Precision time protocol profile for power utility automation. April 2015.

43 *Communication networks and systems for power utility automation – Part 90-4: Network engineering guideline*, IEC/TR 61850-90-4 (2013-08) Ed. 1.0.

44 M. Kanabar, "Investigating Performance and Reliability of Process Bus Networks for Digital Protective Relaying," (2011). University of Western Ontario - Electronic Thesis and Dissertation Repository, Paper 272.

45 R. O. Billinton, and R. N. Allan, Reliability Evaluations of Engineering Systems, 2nd ed., New York: Plenum Press, 1992.

46 K. P. Brand, V. Lohmann, W. Wimmer, Substation Automation Handbook, Utility Automation Consulting, 2003.

47 B. Kasztenny, J. Whatley, E. A. Udren, J. Burger, D. Finney and M. Adamiak, "Unanswered Questions about IEC 61850 - What Needs to Happen to Realize the Vision?," in Proc. 32nd Annual Western Protective Relay Conf., 2005.

48 M. J. Thompson, "The power of modern relays enables fundamental changes in protection and control system design," in 60th Annual Conference for Protective Relay Engineers, Texas A&M University, College Station, TX, March 27–29, 2007.

49 *Reducing outage durationss through improved protection and autorestoration in distribution substations*, IEEE Power System Relaying Committee Report by WG K3, 2009, Available at: http://www.pes-psrc.org/Reports/Apublications_new_format.htm.

50 B. Pickett, M. Signo-Diaz, A. Baker, J. Schaefer, J. Meinardi, B. Kasztenny, I. Voloh, A. Depew and J. Wolete, "Restrike and Breaker Failure Conditions for Circuit Breakers Connection Capacitor Banks," *TAMU 2008 Protective Relay Conference*.

51 *Distribution Fault Anticipation: Phase III System Integration and Library Enhancement*, Final Report prepared for the Electric Power Research Institute (EPRI), Palo Alto, CA, EPRI Publication #1016036, July 2009.

52 C. L. Benner and B. D. Russell, "Intelligent Systems for Improved Reliability and Failure Diagnosis in Distribution Systems," *IEEE Transactions on Smart Grid*, Vol. 1, No. 1, pp. 48-56, June 2010.

53 J. Sottile, F.C.Trutt and A.W.Leedy; "Condition Monitoring of Brushless Three-Phase Synchronous Generators With Stator Winding or Rotor Circuit Deterioration," *IEEE Transactions on Industry Applications*, Vol. 42, no. 5, Sept.-Oct. 2006, pp. 1209 – 1215.

54 C.L. Benner and B.D. Russell, "Incipient Fault Detection Through On-line Monitoring," *Proceedings of the 9th Annual Fault and Disturbance Analysis Conference*, Georgia Institute of Technology, Atlanta, GA, May 1-2, 2006.

55 *IEEE Guide for Determining Fault Location on AC Transmission and Distribution Lines*, IEEE Std C37.114™ - 2014.

56 M. M. Saha, J. Izykowski, and E. Rosolowski, Fault Location on Power Networks, Springer-Verlag London Limited, London, 2009.

57 R. Das, M.S. Sachdev and T.S. Sidhu, "A fault locator for radial sub-transmission and distribution lines," *IEEE Power Eng. Society Summer Meeting*, Seattle, Washington, USA, Jul. 2000.

58 Y. Liao, "Fault location for single-circuit line based on bus impedance matrix utilizing voltage measurements," *IEEE Transactions on Power Delivery*, vol. 23, no. 2, pp. 609-617, April 2008.

59 M. Kezunovic and B. Perunicic, Fault Location, Wiley Encyclopedia of Electrical and Electronics Terminology, Vol. 7, pp 276-285, John Wiley, 1999.

60 S.M. Brahma, “Fault location scheme for a multi-terminal transmission line using synchronized voltage measurements,**”** IEEE Transactions on Power Delivery, Vol. 20, No. 2, pp. 1325 – 1331, April 2005.

61 T. Nguyen and Y. Liao, “Power quality disturbance classification based on adaptive neuro-fuzzy system,” *International Journal of Emerging Electric Power Systems*, vol. 10, no. 3, Article 4, June 2009.

62 I. Dorofeyev, “First deployment of fully digital software-based PAC system on substation 110/10 kV - Basic points of experience and first results,” PAC World Conference 2015, Glasgow, UK, June 29 –July 2, 2015.

63 Meliopoulos et al., “Setting-less Protection: Feasibility Study,” in Proc. of the 46th Annual Hawaii International Conference on System Sciences, Maui, HI, USA, January 7-10, 2013.

64 M. Kezunovic, “Translational knowledge: From collecting data to making decisions in a Smart Grid,” *IEEE Proceedings*, April 2011.

65 S. Vasilić, M. Kezunović, “Fuzzy ART neural network algorithm for classifying the power system faults,” *IEEE Transactions on Power Delivery*, Vol. 20, No. 2, pp 1306-1314, April 2005.

66 M. Kezunović, I. Rikalo, “Detect and classify faults using neural nets,” *IEEE Computer Applications in Power*, Vol. 9, No. 4, pp 42-47, October 1996.

67 N. Zhang and M. Kezunović, “Transmission line boundary protection using wavelet transform and neural network,” *IEEE Transactions on Power Delivery*, Vol. 22, No. 2, pp 859-869, April 2007.

68 N. Zhang and M. Kezunović, “A Real Time Fault Analysis Tool for Monitoring Operation of Transmission Line Protective Relay,” Electric Power Systems Research Journal, Vol. 77, No. 3-4, pp 361-370, March 2007.

69 North American Electric Reliability Council, *1996 system disturbances: Review of selected 1996 electric system disturbances in North America*. [Online]. Available: http://www.nerc.com/pa/rrm/ea/System%20Disturbance%20Reports%20DL/1996SystemDisturbance.pdf.

70 North American Electric Reliability Council, *Technical analysis of the August 14, 2003, blackout: What happened, why, and what did we learn?* [Online]. Available: http://www.nerc.com/docs/docs/blackout/NERC_Final_Blackout_Report_07_13_04.pdf.

71 North American Electric Reliability Council and Federal Energy Regulatory Commission, *Arizona - southern California outages on September 8, 2011: Causes and recommendations.* [Online]. Available: http://www.ferc.gov/legal/staff-reports/04-27-2012-ferc-nerc-report.pdf.

72 *Transmission relay systems performance comparison*, IEEE Power System Relaying Committee Report by WG I17, 2005, Available at: http://www.pes-psrc.org/Reports/Apublications_new_format.htm.

73 D. C. E. de la Garza, Masters Thesis, *Hidden Failures in Protection Systems and its Impact on Power System Wide-area Disturbances*, Virginia Polytechnic Institute and State University, 2000.

74 W. Gao and J. Ning, “Wavelet-based disturbance analysis for power system wide-area monitoring,” *IEEE Transactions on Smart Grid*, vol. 2, no. 1, pp. 121 –130, March 2011.

75 J. Ma, Y. V. Makarov, R. Diao, P. V. Etingov, J. E. Dagle, and E. De Tuglie, “The characteristic ellipsoid methodology and its application in power systems,” *IEEE Transactions on Power Systems*, vol. 27, no. 4, pp. 2206 –2214, Nov. 2012.

76 O. P. Dahal, S. M. Brahma and H. Cao, “Comprehensive clustering of disturbance events recorded by phasor measurement units,” *IEEE Trans. on Power Delivery*, vol. 29, no. 3, pp. 1390 – 1397, 2014.

77 O. P. Dahal, H. Cao, S. M. Brahma, “Evaluating performance of classifiers for supervisory protection using disturbance data from phasor measurement units”, *in Proc. ISGT Europe*, Istanbul, Turkey, October 2014.