Adaptive Protection and Control of Power Systems Incorporating IEC 61850

Saad Umer Khan, MSc

Institute for Sustainable Industries & Liveable Cities (ISILC)
College of Engineering and Science

Submitted in fulfilment of the requirements of the degree of Master of Applied Research

October 2022

This page has been intentionally left blank.

In the name of The God,
The Lord of mercy,
The Giver of mercy.

Abstract

Smart grids are referred to as electrical power networks that employ digital technology to coordinate the needs and capabilities of various stakeholders for power delivery. Application of IEC Standard 61850 enabled adaptive protection and control techniques increase reliability, add to self-healing features, and bring us closer to the realization of a smart grid. This research encompasses the implementation of adaptive protection and control based on existing systems and IEC 61850 data model implementation as a communication standard.

As the electrical power infrastructure has been developed and modernized in steps, so the current installations comprise of legacy components and new elements. The composite nature of protection and control system add complexity to the adoption of adaptive protection. Any automation project must be managed with in the policies of the utility and the policies need to evolve in order to accommodate a smart infrastructure. Substations design has a direct impact on the broader grid architecture where a smart substation will eventuate a smart grid, which in essence is adaptable to achieve an optimize state at any given time.

An optimized state of the grid can extract the maximum benefits out of the existing infrastructure and in the meanwhile, utilities can progressively add smart grid features to elevate the optimized state. The main adaptable actions are in the domain of power systems control and power systems protection that have numerous overlaps and cross linkages. Adaptive control and adaptive protection cannot be realized without a modern information and communication system in place. In addition to the enabling technologies and technology enablers, a standardized approach is needed for which the industry is already moving in the that direction.

Mainly the IEC Standard 61850 facilitates the standardized approach in a substation context, and this has helped to realize the smart grid objectives on a substation level. Although the standard deals with issues on a micro level, still its alignment with the smart grid policy has helped deal with issues on a macro level. This work covers the adaptable actions in context with the international standardized approached for current and future trends in power system configuration for transmission, distribution and generation with an intent of consolidation.

Student Declaration

"I, Saad Umer Khan, declare that the Master of Applied Research thesis entitled Adaptive Protection and Control of Power Systems Incorporating IEC 61850 is no more than 50,000 words in length including quotes and exclusive of tables, figures, appendices, bibliography, references and footnotes. This thesis contains no material that has been submitted previously, in whole or in part, for the award of any other academic degree or diploma. Except where otherwise indicated, this thesis is my own work".

"I have conducted my research in alignment with the Australian Code for the Responsible Conduct of Research and Victoria University's Higher Degree by Research Policy and Procedures.

Signature: 

Date 24/10/2022

Dedication

Dedication to friends and family for their support and patience.

Acknowledgements

I am thankful to The God for bestowing this and countless other opportunities on me despite my numerous shortcomings and enabling me to progress through this endeavour despite the challenging circumstances.

I would also like to acknowledge the guidance and support of Professor Dr. Akhtar Kalam, who is one of the very few good human beings I have come across during my career. He has been a mentor to me in both personal, professional, and academic endeavours. I would like to thank Professor Dr. Aladin Zayegh for his help and support.

In addition to that, I would like to thank Victoria University for their excellent program and facilities. Especially the purpose build IEC Standard 61850 substation automation lab established by Processor Dr. Akhtar Kalam is one of very few of its kind globally. The lab hosts the best and state-of-the-art available resources with continuous international collaborations, helping researchers like me to be inspired and educated on the latest trends.

Preface

Chapter 1 - Managing IEC 61850 Implementation for Smart Substation's protection and control

The majority basis of this century's paradigm shifts is based on information systems and power systems is no exception. The concept of electrical substation automation is not nearly just the automation of individual plants and components; but is a fragment of a bigger plan to a smart system that is self-healing, reliable, responsive, has provisions for augmentation, and supports operative maintenance. Automation is required not just for the sake of automation; it enables an information-based operation as opposed to design based. This chapter deals with systems engineering and project management related aspects of automation projects for which one of the functional requirements is adaptive protection and control.

Like IEC Standard 61850, there is considerable resistance to use adaptive protection philosophy and schemes in a meaningful way as these solutions are not proven in terms of testing or value vs risks is not fully understood. Adoption of IEC 61850 has different barriers, but adaptive protection can be an important technology enabler for smart grids combined with the ICT and SAS standards. This chapter will investigate the functional requirements and their verification to evaluate its implementation possibilities

Chapter 2 - Reviewing Adaptive protection for a wide-area power system

The structure of the traditional transmission and distribution system has undergone through a fundamental change because of market changes. This local energy flows between the source and the load fashions an impression of subsystems. These subsystems come with their own issues and considerations of which needs to be made for power system protection and control effecting the broader system. The theme of this chapter is the understanding that solution of these challenges lies in the IEC 61850 standard used in the context of adaptive protection and control.

Since power system protection causes much of the disturbances due to distributed agent-based architecture, it is natural to go towards an integrated approach with the availability of enabling technologies. This chapter will focus on the communication and protection architecture for wide area power system that in essence is integrated and adaptable.

Chapter 3 - Development of adaptive protection for intelligent power systems

Availability of reserve capacity has made protection engineers complacent. In the context of energy sustainability, it is vital to increase system utilization without compromising security and dependability. Real-time relay parametrization is the target for these smart grids and these concepts will be further explored in this chapter. Industrial distribution system relies on onsite central or distributed generation in addition to utility supply. In this section, the focus is on multi settings of overcurrent relays for industrial power systems adapting to the prevalent dynamic system state in terms of source and load.

Bringing energy generation closer to consumption reduces losses and this is realized with the use of DG (Distributed Generation) and Micro-grid. Where micro-grid is a subset of overall network that can work as its own system during islanding. During islanding or gird, disconnected mode the system should be capable to handle all the static and dynamic conditions which is challenging with conventional protection therefore adaptive protection comes into picture. This chapter will deal with the issues pertaining to adaptation of adaptive protection and control of system in the micro-grid context.

Chapter 4 - Adaptive protection and control based on IEC 61850 Standard

Lines distance protection and Generation out of step protection have coordination requirements during system design. There are scenarios where system protection requirements cannot be satisfied with fixed or even variable settings and adaptability to system state is required to keep system stable that is discussed in this chapter. In this chapter, different scenarios of micro-grid operation are evaluated for reliability. The discussion also included international standards for micro-grid operation and operational implications on power system protection.

This chapter will look into DER Penetration by building from the physics of fault and implications of DER on those fault conditions with possible solutions by taking a holistic approach to the combined AC and DC system. The solutions offered by adaptive protection are discussed form the enabling technologies perspective. Radial power distribution network is configured for a source such as zone substations but with increased DG, this has changed and so has the parameters of fault states. Variable DG availability, equivalent impedance and direction of current flow cannot be serviced by fixed setting. In this chapter a communication, based adaptive protection is discussed for distribution system both for islanded/connected system and for centralized/decentralized protection.

Table of Contents

List of Tables

List of Figures and Illustrations

List of Abbreviations

AI	Artificial Intelligence
ANN	Artificial Neural Networks
CB	Circuit Breaker
CDC	Common Data Classes
CT	Current Transformer
DER	Distributed Energy Resource
DG	Distributed Generation
DMS	Distributed Management System
DNP	Distributed Network Protocol
DO	Data Object
EMC	Electro Magnetic Compatibility
EMS	Energy Management System
ESS	Energy Storage System
FACTS	Flexible AC Transmission System
FFT	Fast Fourier Transform
FL	Fuzzy Logic
GOOSE	Generic Object-Oriented Substation Event
GPS	Global Positioning System
HMI	Human Machine Interface
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
IEEE	Institute of Electrical and Electronics Engineers
IDMT	Inverse Definite Minimum Time Characteristic
LAN	Local Area Network
LC	Local Controller
LD	Logical Device
LN	Logical Node
MAS	Multi-Agent System
MMS	Manufacturing Message Specification
MV	Medium Voltage

OC	Overcurrent
OLTC	On Load Tap Changer
PCC	Point of Common Coupling
PF	Power Factor
PG	Power Grid
PV	Photovoltaic
RMS	Root Mean Square
SAS	Substation Automation System
SCADA	Supervisory Control and Data Acquisition
SG	Smart Grid
SS	Substation
SV	Sampled Value
THD	Total Harmonic Distortion
TMS	Time Multiplier Settings
UML	Unified Modelling Language
VT	Voltage Transformer
WAM	Wide Area Measurement
WAN	Wide Area Network

List of Symbols

E	Primary Line to Neutral Voltage
I_P	Maximum Fault Current
S	Conductor Spacing
V_S	Source Voltage
ω	Radial Frequency of Source

List of Publications

[1] Khan, S. & Kalam, A. (2020). Seamless Engineering Process to Adapt IEC 61850 Standard for Substation Automation Through Requirements Specification. IOP Conference Series: Materials Science and Engineering. 937. 012043. 10.1088/1757-899X/937/1/012043.

[2] Khan, S. & Kalam, A. (2021). A Holistic Review of Smart Grid Contribution Toward Energy Sustainability. 10.1007/978-981-33-6456-1_6.

This page has been intentionally left blank.

Chapter 1: Managing IEC 61850 Implementation for Smart Substation's protection and control

1.1. Background

The majority basis of this century's paradigm shifts is based on information systems and power systems is no exception [1]. The concept of electrical substation automation is not nearly just the automation of individual plants and components; but is a fragment of a bigger plan to a smart system that is self-healing, reliable, responsive, has provisions for augmentation, and supports operative maintenance [2,3,4]. Automation is required not just for the sake of automation; it enables an information-based operation as opposed to design based. These days' utilities manage dual infrastructure that is of power systems and information systems. Enabling technologies has made substation automation possible that was not feasible a couple of decades before due to bandwidth constraints. Standards like IEC Standard 61850 have provided solution to structural issues by employing object-based model. The combined power systems structure is shown in figure 1.1.

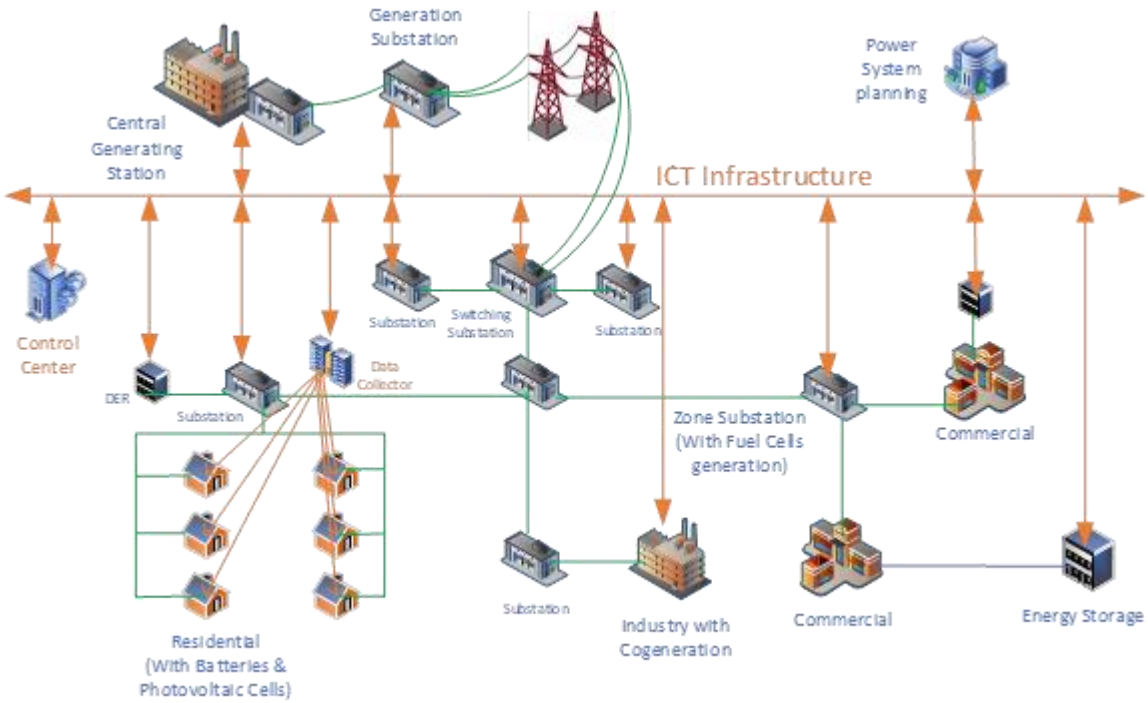


Figure 1.1 - Combined Power System Infrastructure

1.2. Power Management Solutions

As the automation aspect is more customized than traditional installations, a different management style is required to bring these into realization [5,6]. Each function of the utility-based organization must adopt their information flows to suit for these types of automation project. Most utilities have a hybrid asset base comprising of legacy systems and systems conforming to new standard requirements. The main driver is consideration for requirements and constraints related to information systems in addition to electrical systems.

After a decision is made to implement a SAS solution, it is essential to undertake effective requirements management. This includes development of functional requirements and system management requirements. Subsequently, a higher-level technical specification is developed for the systems as per IEC Standard 61850 object model. A useful tool for ICT functional requirement management can be the Intelli-grid Architecture and refer to Appendix B.

1.3. Requirement management for automation

Automation components and systems are specified functionally different to conventional equipment due to varying stakeholder requirements. RML (Requirement modelling languages) can help in understanding the question “what is required?” before moving to “how to fulfil that requirement?” RML is intuitive and accelerates the stakeholder review process to finalize the functional requirements [7]. The same tool can incorporate information flows and organization structure resulting in development of functional requirements for both automation and communication. Operators, maintainers, and asset owners must closely collaborate with the vendor executing the automation project to develop procedures on top of standard requirements.

Utilities do not leverage the full extent of available data and this need to change due to increasing network complexity or to support nontechnical business functions. Current technologies can already provide the entire functionality of a smart substation and smart grid that can go beyond local automation to system wide capability resulting optimized safe utilization. Although substation automation is the first step towards smart grid, still it incorporates most of the smart grid functionality at the substation level and aligns the efforts of all electric utility departments towards a common goal. Electric utilities must work in the direction of the general industry trend, which is digitization, digitalization and digital transformation summed up as industry 4.0. IEC 61850 contributes to this overall goal by

making information available in the right time, place, and format for system consumption. The decomposition of IEC Standard 61850 is shown in figure 1.2.

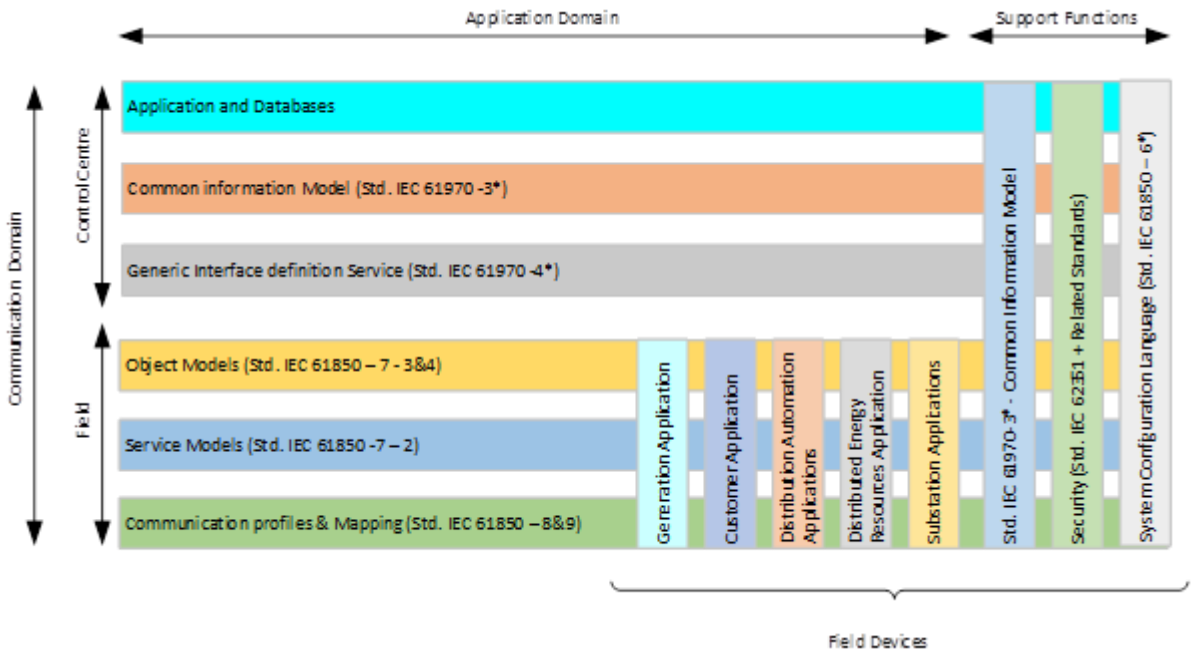


Figure 1.2 - Composition of IEC Standard 61850

1.4. Enabling technologies for adaptive protection and control

There has been a revolution in the capabilities of ICT (Information and Communication Technologies) and most automation capabilities are leveraging on this revolution because of their high depended on ICT [8]. Cross industry, learning is aiding electrical utilities in this new era in areas like management and security of information or software/hardware maintenance practices. Refer to appendix A.

Hardware and software for modelling, protection, communication, instrumentation, and HMI are developed under separate objectives, which has created compatibility issues. IEC 61850 framework is an essential tool to consolidate these product development efforts to get a truly integrated supply chain while maintaining the technical edge for different vendor's R&D processes.

1.5. Advantages of automation

Automation is not justified for the sake of automation. There should be economically justifiable perceived benefit for any automation initiatives and for substation; there are a magnitude of benefits for both physical and conceptual systems [8]. Nevertheless, automation leads to more automation possibilities that is we can only build on certain capabilities [9].

In short automation provide benefits to the physical system like reduce material/hardware requirement, make use of reliable media, integrate different functionalities, increases penetration of digital devices, provides new capabilities, and modernize human machine interface [10]. Conceptual systems gain benefits like self-diagnosis, increased statistical analysis capabilities, empower operational planning, provides greater customizable annunciation features, more real time information is available, ease of device configuration, manageable database, live system modelling, automated fault finding/response and many more. ICT can no longer be viewed as a support functionality and protection-engineering roles need to evolve with the object-oriented model of SAS.

1.6. System modelling leading to adaptive protection of system

Power system functionality needs to go through the requirement engineering process to determine the true system requirement [10]. Modelling of the information system and information flow is critical to analyse the overall system and complex interactions.

IEC Standard 10746 provides an important tool to create a system breakdown structure to be modelled via Unified Modelling language that is software engineering practice that can streamline the requirement management for substation automation systems [11]. Within the same model, information model can be incorporated that are defined by various standards such as IEC Standard 61970 and IEC Standard 61850 based on their respected scope. This model can be further developed to include functionality, actions, and naming convention.

Interoperability that is technology or vendor independence and plug & play functionality is going to be central tenants of adaptive ICT systems for future smart grids.

Table 1.1 - Actions required for plug & play functionality

S/No	System plug & play actions
1	Detection of new field device
2	Power System (e.g. Substation) register updated
3	Communication (e.g. SCADA) register updated
4	Initiation of data exchange
5	Communication and Power system model updated
6	Verification of system requirements

1.7. System Management

In the current environment ICT, security management is one of the most important management issues and it needs more attention than ever before [11]. The security interactions need detailed modelling and assessment as part of the requirement management process that includes:

- Security failure mode and criticality for the combined power and ICT system
- Implementation requirements out of the above assessment
- Selected solutions based on identified requirements
- Contingency requirements and associated plan in an adverse event
- Audit and assessment plan for routine check and security event

The second important aspect of communication/automation system management is data administration to meet the overall system's functional requirements. Following process, apply for power systems data management:

- Modelling of data related requirement that include storage, discover, accessibility, recovery, and validation
- User requirements both human and machine
- Design of data related systems
- Development of policies and procedures

Management of applications across functions and complying with desired metrics such as reliability, availability, maintainability, cost etc. can stretch to external parties. Application management process includes following aspects:

- Requirement management of applications while considering all the interfaces
- Short term, midterm, and long-term implementation planning which covers technology selection both hardware and software. This includes all aspects to reach the end goal.
- Implementation realization and testing
- Internal and external process/system integration
- Application performance, error, and failure management
- Preventive and reactive maintenance of applications including internal and external after sale support
- Workflow and business object management

Next is the management of networks for power systems. Power system reliability is directly linked to information system reliability and network management encompasses the business requirement engineering for networks, networks planning and network's design. Subsequently the processes like network monitoring, network performance management and network general management becomes relevant.

Finally, the management of telecommunications infrastructure involves the asset management of telecommunication physical systems and its interactions with internal/external stakeholders. A utility in some cases provide services to telecommunication companies that is an important revenue stream but adds to management requirements. The management processes for telecommunications are like network management.

1.8. Managing projects for power systems automation

Automation project managers in the current environment are required to develop awareness in the unique aspects of automation projects and the future only looks more demanding. Organization specific standards developers must understand the current new paradigm and take in to account the future trends considering organization's objectives that are not bound by previous constraints and underlying assumptions or simply the previous requirements are not feasible anymore.

Smart substations and in turn smart grid have benefits both in infrastructure construction and in operation in terms of cost and capability [12,13,14]. There is a need to evaluate if this is an isolated automation project or program of works to manage the implications. Program of works (projects) usually starts with a proof of concept via pilot project followed by system wide implementation to reduce the unpredictability of automation scope, but each automation project will add to the organizational learning reducing project risk further.

Strategic objectives vary across utilities that determines the placement of automation system in the overall objectives and subsequently the implementation plan [15]. A utility may decide to neglect an option, only evaluate options at the end of the asset life (either replacement or upgrade options), assess alternatives with the industry, and identify the areas requiring change or combination of these. Technology for the sake of technology is a bad idea for businesses as there should always be a business reason to justify an automation project or a program that even includes aspects like reliability. Another strategic element to contemplate is the migration strategy after a strategic object is identified. This component of strategy will enable the realization of the objective or challenging the objective if flawed.

The most important element of project management is the people managing the automation or any other project or program. Especially for automation projects, we need a supporter in the upper management who will the champion the cause until the completion of work. Afterwards an appropriate project manager is selected, stakeholders are identified, and a project team is setup. There are some unique traits required for an automation project and program managers that go beyond the usual project management domain. The joint project management team structure is shown in figure 1.3.

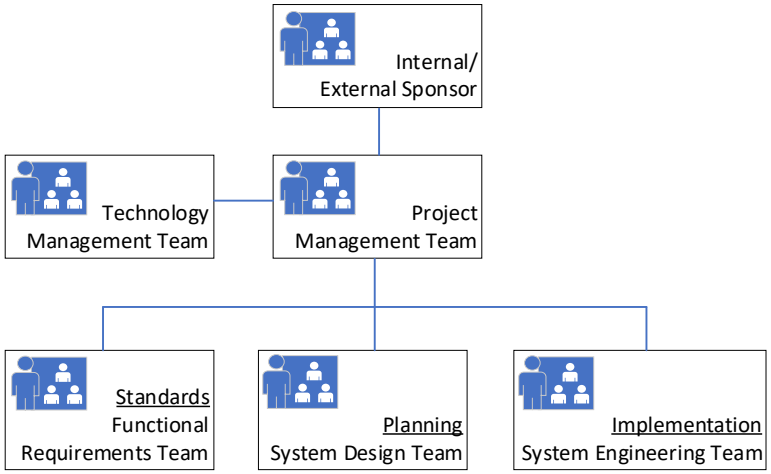


Figure 1.3 - Joint Project Management Team

The function of each team is evident from its name in the JPT (Joint Project Team) chart, but it should be noted that this arrangement might change from organization to organization. It is worthwhile noting that planning function will register all logical nodes and this listing will aid in the finalization of modes of communication like multicasting vs polling.

Appropriate stakeholder involvement is required for automation project success that will include staff from both operations and maintenance. A typical utility stakeholder matrix includes sections such as distribution operation, transmission operations, substation operations, transmission planning, distribution planning, facilities planning, communication planning, asset management, engineering & design, engineering planning, engineering standards, protection engineering, procurement, metering, accounting & finance, corporate departments, and energy market operations. Project needs to account for man hours required for total stakeholder engagement till the completion of the endeavour as personal from both sides are going to book their time on the project in hand. This will create efficiency in engagement and ensure accountability.

1.9. Automation project team

The preferred industry practice is to divide the project teams in the core project, requirements management, system engineering & design and technology management where the core team will take lead of the project [16,17]. The core team will have project ownership and will have continuous presence on the project whereas the other sections will be scheduled on the job when required.

As any project, the project manager ensures the project is executed within time, technical & nontechnical requirements, and financial constraints. The requirement management team can have specialized resources, but it is best to have people who can set aside their predispositions and aim to record the actual requirements for which they will consult with all stakeholders. Requirements team will review the integrated system, document undocumented process or variation in implemented processes, record undocumented client access practices, record undocumented or incorrect contingencies/constraints, record operational needs, maintenance needs and security requirements.

The design team covers activities in concept, planning, and execution stages of the project. A staged approach provides engineering assurance, change management, and streamlines management approvals. The stakeholder interactions for design team will include protection,

communication, automation, SCADA (Control), engineering, service vendors, and suppliers. This team reviews existing design, reviews existing requirements, provides preliminary / concept design, initiate type approvals, resolves contingencies/constrains, list all IEC 61850 Standard logical nodes, prepares project technical scope/specifications and review substation configurations.

The engineering team carries out detailed design (including time sync, hardwired elements, auxiliary power demand and local communication ports), procurement, configuration, and bench testing. The system testing will itself include IEC Standard 61850 conformance evaluation and verification of network operation / logical connections / electromechanical interfaces/functional interfaces/application behaviour/operational performance needs/mode of operations (including contingency) which is covered in project test plans. Site execution and engineering & design are grouped here under a single umbrella. Other project and site activities include factory acceptance testing, equipment installation & integration, site testing & commissioning, and setup for O&M provisions/tools.

The technology team will have interdisciplinary responsibilities such as requirement engineering for test data, self-description, and system management statistics. The main responsibility of the technology team is to provide engineering assurance for IEC Standard 61850 and hence the team member should be highly proficient with the standard along with all interdisciplinary topics.

1.10. Management game plan

Automation project management itself is a skilled based instead of qualification-based discipline that in the real-world deals with multidisciplinary issues [18]. The coordinated activities formalized as processes originally standardized in mature organizations are revisited based on lessons learned during the automation project.

During the initiation phase the automation project charter is agreed which defines the aim, pathway and constraints. The draft gives at a higher level the expectations while excluding the individual methodologies; this includes critical objectives, location of pilot/production deployments, anticipate benefits and constraints.

Organizational culture plays an important role in automation management as it embodies the collective behaviour of the workforce when adapting new or existing technologies as part of a

project. Effective communication, teamwork and appropriate delegation are the main topics effected by organizational culture. Other topics effected by organizational culture are document management, reporting, training requirements, assurance, and mediation.

Table 1.2 – Distribution of responsibility

- In House	- Supplier
• Introductory • Planning and implementation • Integration and testing • Functional IEC Standard 61850 communication capabilities	• Equipment specification and configuration • Equipment installation and testing • PLC and IEC Standard 61850 • HMI and IEC Standard 61850

1.11. Automation Project Assessment

Structuring and option analysis for a project or prioritization between projects is mainly conducted via cost to benefit assessment on a comparable quantifiable basis and risk analysis [19]. This analysis is conducted via economic analysis plan/program and achieves objectives such as: a) report costing b) return status at a point in time c) present worth of items d) risk and sensitivity analysis outcomes.

Cost & benefit analysis can be an important tool throughout the life cycle of the project and is especially relevant to substation automation project with gate-based approach. To allocate monitory value to IEC Standard 61850 application benefits is heavily associated in non-material savings such as simplification, novel capabilities and improved management etc. However, a cost to benefit analysis is a periodic process that can introduce new dimensions, limit scope, freeze or stop an automation project during its life cycle. The above also applies to risk management.

An automation project can have nontechnical risks such as scope creep, poor requirements management, supplier lead times, unstipulated product performance, staff scheduling issues, change in stakeholders and project resources. Afterwards any change management should have a holistic impact assessment. Contingency communication requirement planning to avoid mission critical communication failures is included in the functional requirements function.

Within the risk management, process the initial step is risk identification and classification followed by mitigation and alternatives comparison. Formally, the process after identification would be assignment of severity/probability, allocation of priority, delegation and verification. There are off the shelf software products available that have both cost-to-benefit and risk assessment process integrated with output dashboards.

1.12. Design process to design a substation with Substation Automation System

Functional requirement entails the system expectations from user, implications of these expectations, and presenting the requirements to ensure correct interpretation/implementation. Afterwards the functional requirements personal will define the standards. A system design engineer will be complying with the requirements via solution that is most practical and favourable. The combined memory of the organization would create an outcome comprising of best components in current enabling technology regime. Some of the basic concepts for design include interoperability, primary & secondary systems, substation automation and distribution applications.

Mapping of business processes is good starting point to develop secondary systems functional requirements. Business process would include official & casual lines of interaction, company cultural norms, role mandates, legal & regulatory requirements, technical flows, security authorizations and procedures/standards. By definition, a business process is an automated or manual action sequence architected to realize a business objective executed by specified actors sometimes drawn in the form of flow diagram.

1.13. Business process documentation for Power Automation System:

The project & business processes are formally documented by first defining the intent of the process followed by a process flow that include the sequence, the actors/actions, constraints/interlocks, coordination and the decisions. Afterwards, it is required to mention the primary system interactions only and generic secondary system interactions only where unavoidable. Specific secondary system descriptions should be avoided until the business process is not affected and the most important is to not rely on existing process as a reference.

It is useful the divide the documentation process in to five hierarchical levels that are:

- Layer/Level – One: Substation objectives

- Layer/Level – Two: Activities
- Layer/Level – Three: Functional Capabilities
- Layer/Level – Four: Substation Functions
- Layer/Level – Five: Affected Entities

The first layer will support the goals set by the utility inclusive of mission supportive, important and critical aspects. Content at this layer should be kept at the management and strategic level including distant goals. Layer 2 will include the activities required to achieve layer 1 and can be either broad or definite in nature. The layer 3 will elaborate on the definite capabilities to be supportive of the activities. For example, a protection-based activity can have capabilities of differential, distance and/or breaker failure protection. The last two layers/levels would cover the substation function (L4, trip, close, lockout etc.) and substation entities (L5, Feeder number, bay number, breaker number etc.) supporting the L3 Capabilities.

The group managing the functional requirements has the influence to tilt the final system and the significance of this group should be understood resulting in an increased focus on their work. The rationale behind the five layers/levels is to establish a group of replicable substation functions that are product independent and explain the functionality of a substation, which is quite like IEC Standard 61850. Substation functions are subset of business process that are of a technical nature but still recording human behaviour and interacts.

Within the documentation, there are sections for software application modules, application functions, logical notes and information flows. The software component can be either component of the shelf available separately or bundled with hardware or a custom development, but the main requirement is to be IEC Standard 61850 communication compatible without exposing the proprietary linkages.

Functionality or functions at its inception are concepts used as a modelling tool to mimic a designed ability where a function has an intended action, cross-dimensional interface and an application. A mix of software, hardware and signalling elements implements these abstracts, which can be a key component of model, based system engineering. It should be noted that application functions provide a bigger behavioural picture and substation functions are relate to a specific electrical utility role.

IEC Standard 61850 defines over 75 specialized logical nodes, which is the building block of application functions (For example XCBR – represents CB functions). A communication system would only see logical notes and not the application functions. A logical node definition has a data component and a capability (method) component accessible by the communication system boosting interoperability.

There are various project DMS (document management systems) in the market facilitating review and approval process which provide achieving, communication and distribution. Other than technical documentation, project has various administrative, progress and tracking documentation of which one of the most important is the project charter dictating the success of the project.

1.14. Substation Automation Functional Requirements

It is important to manage future functions in addition to current functional requirements driving competencies. Each user has different functional requirements for present and future trends, but planners should be aware of the possibilities to carve out their needs.

Substation automation is driven by holistic utility requirements considering futuristic functionality for which the list provided by IntelliGrid® architecture program can be a good point for reference. Although dynamic but functions have varied information intervals which are instantaneous or intermittent (millisecond, seconds, or statistical periodic durations). One of the main features of protection settings are an offline activity that will become online and automatic in the future, hence critical for adaptive settings. Refer to appendix D for further details.

Concurrent power systems information is critical for operational needs and the systems is managed by simultaneous control instructions or with established parameterization and applications can access this via various types of distributed data acquisition and control functionality. The same data acquisition and control functionality is accessed by other systems like SCADA, Automation, EMS and protection systems. The four distinct environments as defined by the IntelliModel® are depicted in figure 1.4.

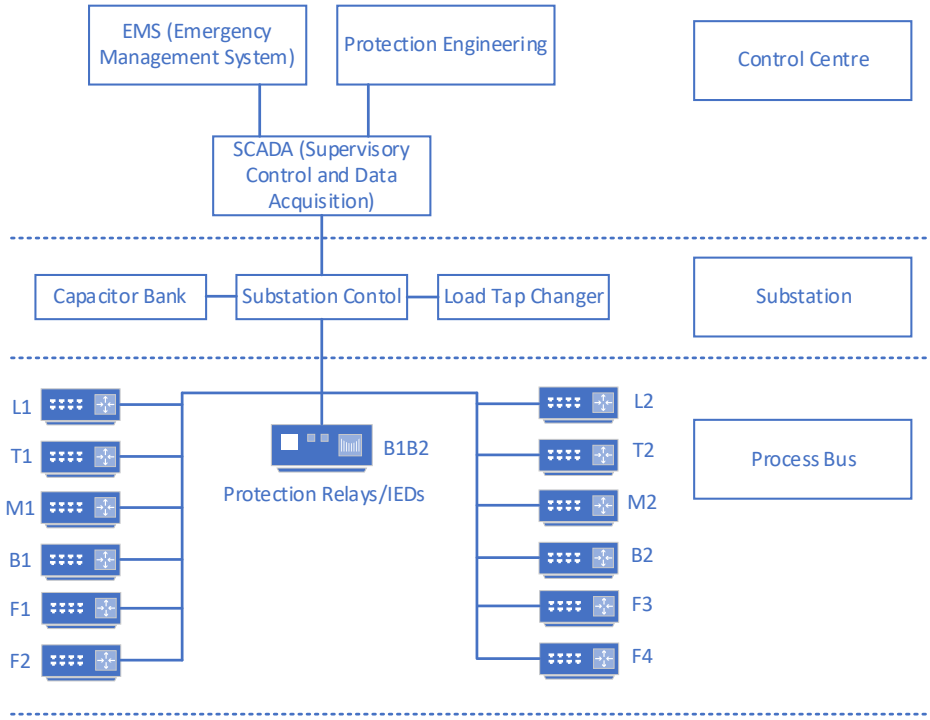


Figure 1.4 - Case of Inteli-grid® environment

1.15. Model Based Substation Automation Planning

Automation planning cannot rely on traditional substation planning function, as it requires information engineering in addition to existing design needs. Conceptual modelling is the best practice for information engineering (Definitions, Requirements, and Specifications) conceptual or abstract modelling involves system decomposition for requirements capture and integration back to final system.

Proprietary protocols require a plethora of protocol converters and different protocols have varying strengths/weaknesses. Some protocols like DNP3 do not have complete requirements capture like validation difficulties due to lack of consideration in data description. In addition to that, the data handling methodology is counterproductive where the central SCADA interface tries to handle most information.

Due to an object-oriented philosophy IEC Standard 61850 can provide superior standardized capabilities with fast-paced adoption across vendors. Standardized nomenclature provides a magnitude of benefits to asset owners from O&M (Operation and Maintenance) perspective. Data handling is as per requirements that means that the SCAD system is used when required and not as a default.

Information abstraction provide nomenclature and structure to physical and virtual handlers of information that in turn facilitates protocol mapping. An implementation approach is to move from proprietary to interoperability to interwork-ability to interchangeability.

Modelling via abstraction is a ground-breaking technique employed for a holistic top-down comprehension of the system. It also provides techniques to implement a programming code from the abstract model. It is possible to visualize a system in different dimensions or details while supressing other aspects yet via modelling, we can develop interrelated multidimensional views.

It is possible to visualize a system in different dimensions or details while supressing some aspects and highlighting others yet producing interrelated multidimensional views. A system can be viewed via multidimensional models that can contain varying level of details but in essence reflect the real world. UML is the go-to standard for majority of software system's visualization and documentation which can broadly be stated as business analysis and requirement engineering. UML in turn supports object-oriented approach for objectify items conceptual behaviours incorporating best practices. This is scalable and increases productivity by directly connecting to code.

Among the UML modelling tools a use case diagram focuses on function interactions from one of the perspectives. A basic unit focus of these diagrams are "Actors" which can be animate or inanimate objects for which requirements are recorded. Use case functions can be decomposed into individual use cases but each will contain following:

- Communication
- Use Cases
- Actors
- Classes
- Interfaces
- Associations (Relationships)
- Generalization (Relationships)
- Dependency (Relationships).

The advantage of user cases is that it records often-neglected items, user requirements are recorded, user involvement is ensured, it's a good tool for information modelling, provides an

overview of requirements, facilitates implementation staging, facilitates requirements tracking, facilities testing, facilitates documentation, facilitates documentation, facilities reporting and improves quality by coverage. An example UML model is shown in figure 1.5.

A UML technique involves:

- Use case development by process selection, actor identification, function identification, recording performance requirements and recording interactions.
- Class diagram development by data type identification and recording data type requirements.
- Class translation into models, definitions and code.
- Creating registries for accessibility.

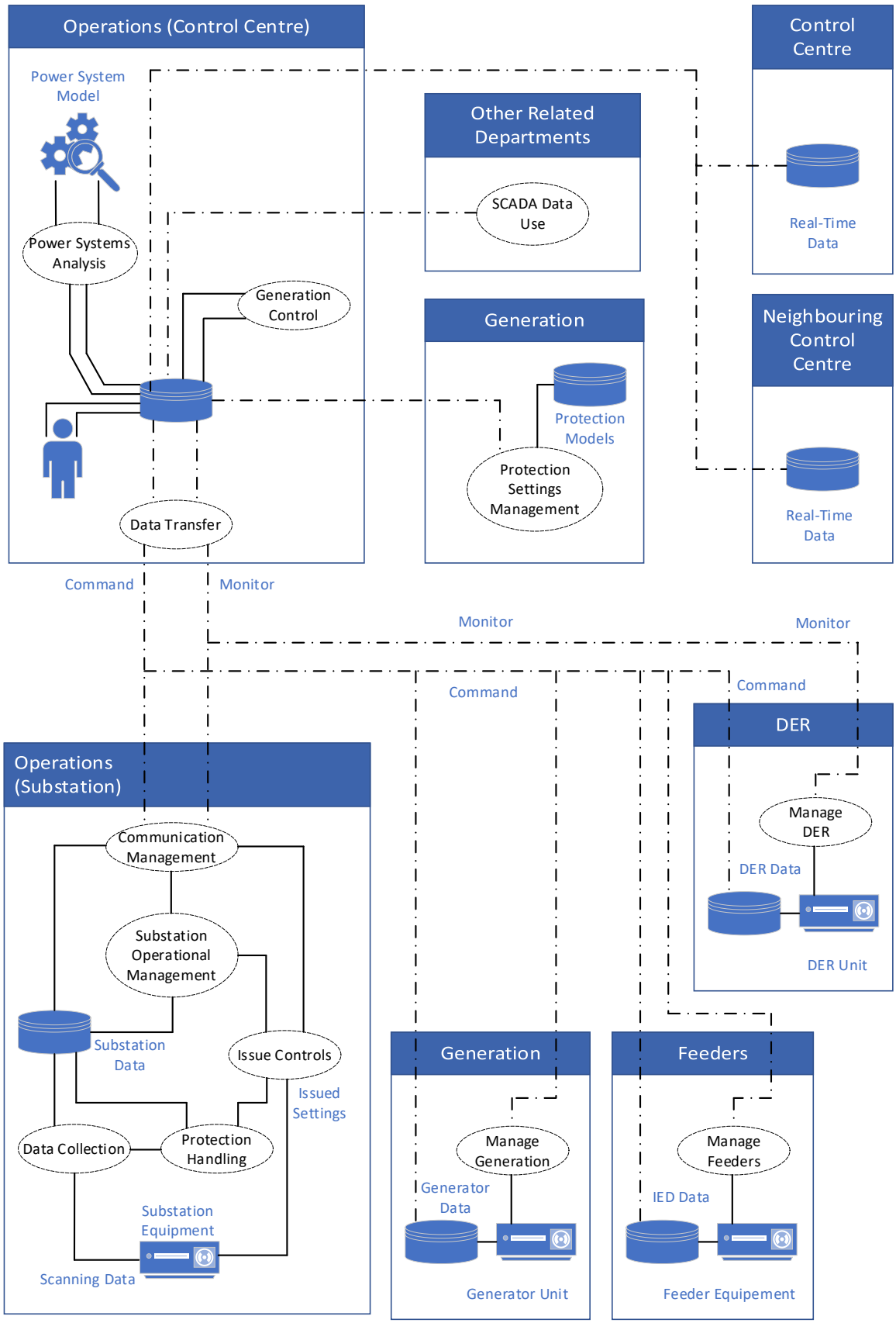


Figure 1.5 – Control and Data Acquisition Model

In the IEC Standard 61850 reference model, nouns such as exchanged data are termed as object models. These includes standardized data types, preassigned attributes, standard data classes, standard data associations, standard & augmentable data object grouping and standardized device models. This is depicted in figure - 1.6.

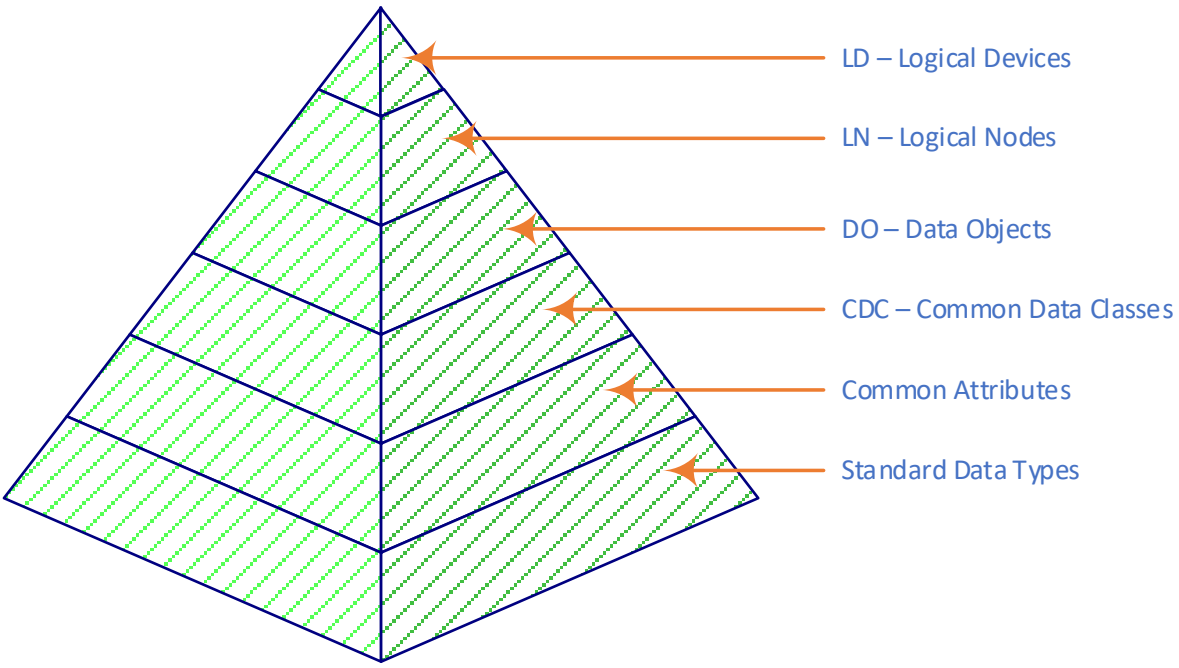


Figure 1.6 – Hierarchy of OM (Object Model)

IEC Standard 61850 LD (Logical Device) server/hardware contain one or more LD (Logical Device) model/software imitating hardware and component information. LD model/software constitute of several LN (Logical Node)/functional modules that are standardized function specific DO (Data Object) grouping. This is illustrated in figure 1.7.

Verbs to the object models are data related communication services providing transmission, reporting, logging, etc. that are either mapped abstract services ACSI (Abstract Communication Services Interface) or inter-LN (PICOM – Piece of Information for Communication) services.

ACIS includes services such as logical connectivity, information sent requests, information write services, data value grouping, data set reporting, information logging, value updating, high-speed messaging operational selection controls, time sync and file exchange. The predefined data sets can be updated based on requirements. PICOM includes inter LN (Logical

Node) data transfer, its definition, and its performance requirements. Although provided by vendor still protection engineer should define triggered requirements.

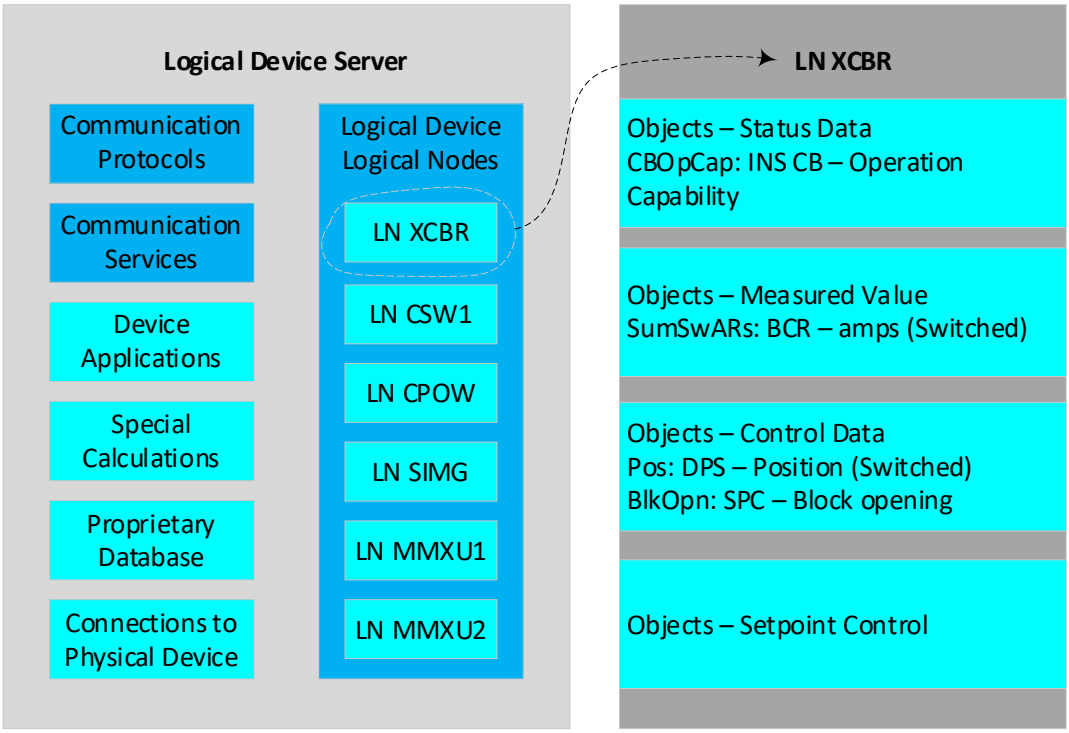


Figure 1.7 – Relationship illustration between LD, LN, DO and CDC

Abstract communication needs to be mapped to real world protocols as per IEC Standard 61850 such as GSE (High Speed), MMS (TCP/IP) or even MMS and XML (Which require communication service). To give applications visibility of actual substation layout/orientation, a configuration language is used such as CFL (Substation configuration language) or CIM (Common info model).

1.16. Power Automation System Specification

As discussed before the specification process includes managing functional requirements, Logical notes, inter-substation data exchange, intra-substation data exchange, stipulate testing and stipulate configuration tools. The conceptual model for basic communication services is shown in figure 1.8.

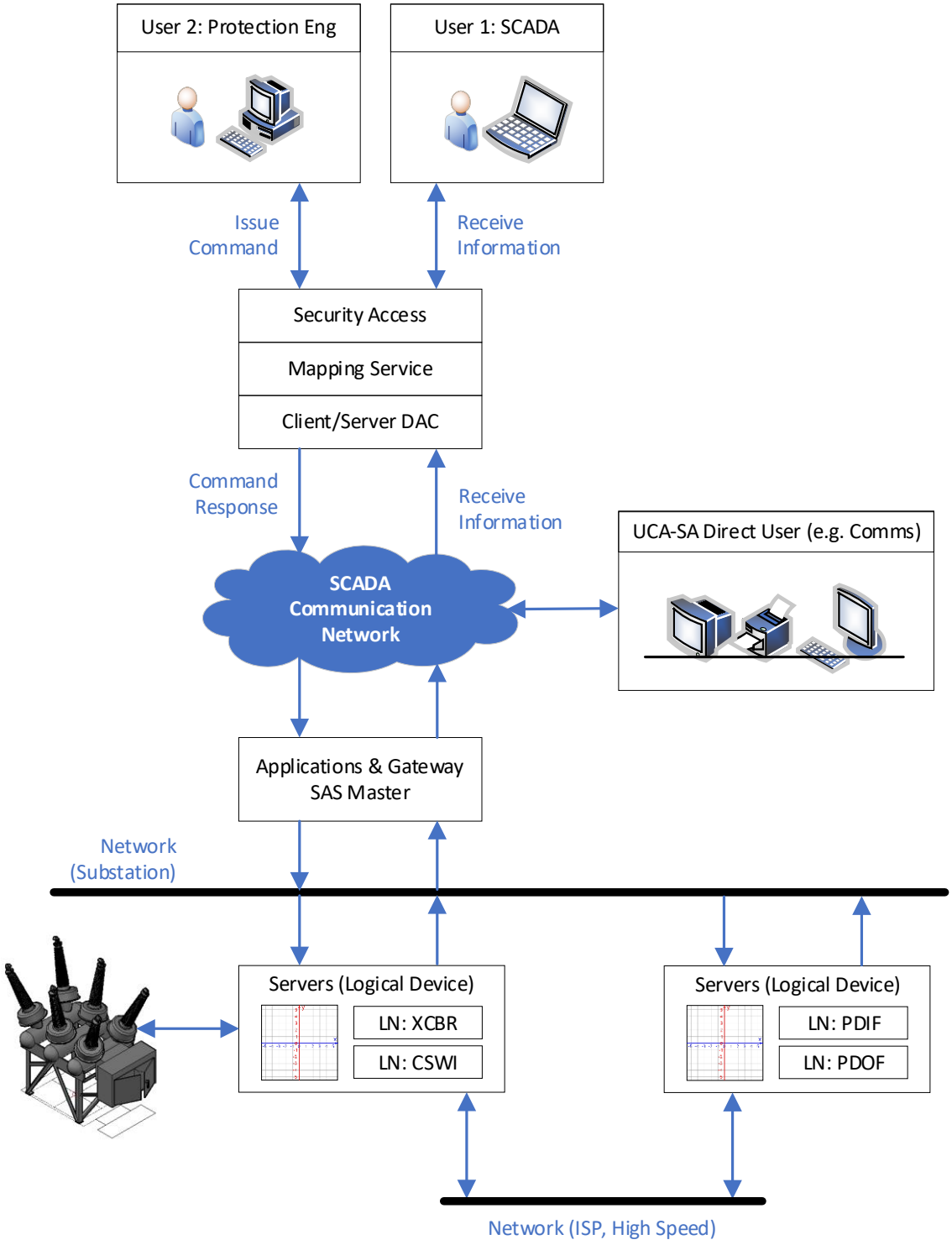


Figure 1.8 – Conceptual Model for Basic Communication Services

An independent conformance testing is required to cover all data objects and services in relation to a recognized reference. This will serve as verification and validation activity for the product under question. An open conformance testing process is shown in figure 1.9. Refer to appendix E.

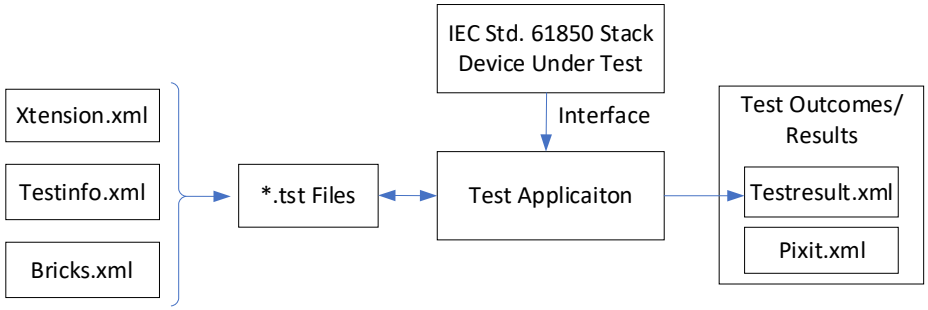


Figure 1.9 - An open conformance testing process

1.17. Developing the communications standard:

Purpose build (Organization specific) or vendor specific adaptations of latest ICT trends has created fragmented body of knowledge. This fragmented execution precedence has created communication challenges and interoperability issues. To solve this problem, a utility collaboration program was initiated in 1988 known as Integrated Utility Communication Program (IUC) and under this program; the Utility Communication Architecture Project (UCA) was undertaken.

After communication requirements analysis and finalizing requirements definition, a list of standards was selected through standards review of which MMS was adopted for real time communication. The UCA version 1.0 could not solve the interoperability issues, as detailed specifications for MMS were not created which left space for diverse adaptations.

Deregulation and limited adoption of version 1 led to the recognition of the need of a standardized approach culminating to version 2 or the preamble to IEC Standard 61850. Refer to appendix F for vendor information.

1.18. Conclusion:

This takes us to the conclusion that the basis of this century's paradigm shifts is based on information systems and power systems has been no exception. It is also clear that the concept of electrical substation automation is not nearly just the automation of individual plants and components; but is a fragment of a bigger plan to a smart system that is self-healing, reliable, responsive, has provisions for augmentation, and supports operative maintenance. It is also concluded that the automation is required not just for the sake of automation; it enables an

information-based operation as opposed to design based. The discussion around systems engineering and project management aspects of automation projects is important for which one of the functional requirements is adaptive protection and control.

It was found that like IEC Standard 61850, there is considerable resistance to use adaptive protection philosophy and schemes in a meaningful way as these solutions are not proven in terms of testing or value vs risks is not fully understood. Adoption of IEC 61850 has different barriers, but adaptive protection can be an important technology enabler for smart grids combined with the ICT and SAS standards. It was beneficial to investigate the functional requirements and their verification to evaluate its implementation possibilities

Chapter 2: Reviewing Adaptive protection for a wide-area power system

2.1. Background

Power systems have grown to its present state of large wide area interconnected system from a humble beginning of a few installations. After privatization, each investment decision is more scrutinized and regulation compliance cost has increased exponentially leading to a similar trend like many industries that is optimization. Supported system protection is required for each optimization decision and here is when adaptability comes in to play. Protection departments favour dependability over security which is acceptable in an over designed system. Dependable protection system will identity and clear all faults which at instances cause nuisance tripping. Whereas secure protection system would not perform any unwanted trips but might be unresponsive on some fault conditions.

Even the simplest of protection device selection that is a fuse have a security vs dependability decision where a wire size is based on the outcome. A combined protection system can have more complex decision-making process [20]. In adaptive protection, the security by dependability figure will change with system state. System is getting more capable as it shifts form hard logic to soft logic and in addition to settings, the scheme can also modify itself with the system requirements and that will be a true adaptive protection. Modern relays are already providing proven solutions to issues like CT mismatch or tap changer error etc.

Because of its relative complexity, Distribution system is more prone to fault as compared to transmission system. Electrification is the basis of much of human achievements. Power grids being the central piece of infrastructure manned by dedicated human resources contributes immensely to all aspects of modern cities [21,22].

2.2. Aims and objectives

The main aim of the research is to develop IEC Standard 61850 based implementations for adaptive protection/control of power transmission and distribution systems. Different scenarios and configurations of a typical installation will be assessed to determine the best structure. Several OEMs (Original Equipment Manufacturers) offering product and system solutions are considered in this study.

At present, relay manufacturers normally do not permit remote access to individual protection settings via IEC 61850. This is one of the main limitations encountered during the implementation and it restricts the adaptive protection system in that it can only use protection setting groups. This is the primary limitation for a real adaptive system implementation. The only provision in the existing products is use of protection settings groups which generally range from four to eight but the network scenarios for a particular power system can be more. Although this problem can be solved using IEC Standard 61850 standard in an ideal manner, still a practical way around needs to be explored until industry wide change. Several adaptive protection and control applications can be realized with the use of IEC 61850 object model. The main application under consideration is "Relay setting co-ordination checks". Other applications which are a subject of interest but will only be discussed briefly are as follows:

2.3. Contributions

The impact of power electronic based system components on an adaptive protection and control elements is little understood due to absence of work on the subject. Power electronic based components in a network serve a protection feature as well.

A portion of this work contributed towards a simplistic concept of supervisory zone of protection can provide an adaptable solution which can distinguish between heavy loaded and fault conditions. Also, possibilities around the implementation of a pseudo-adaptive protection system while utilizing the multi-settings available in IEDs available as COTS (Component/Commercial of The Shelf) reacting to the system situations based on the calculated pre-setting conditions are assessed. The same mechanism can cater for protection challenges posed by DG such as protection blinding, sympathetic trip and coordination issues. As this offline multi-setting adaptive technique is flexible, we can incorporate it both as distributed and centralized protection regimes.

This study strives to provides a simple protection solution to different complex microgrid structures being encountered with increased DG penetration. The solution entails the introduction of a simplified adaptive protection system which relies of matching tables for different microgrid scenarios while utilizing multi-setting overcurrent IEDs which select the settings relevant to the prevailing grid state. This solution although simple yet covers all the necessary requirements of protection through an MCC.

The IEC 61850 has not been implemented for the entire utility infrastructure and currently in Australia only limited test installations exist. Predominantly, most of the industry is working with legacy standards which are in the process of upgrade. Under these circumstances particular scenario-based studies are required to cover all the aspects of future installations with possible pros and cons.

2.4. Research Gap

Even after understanding the benefits of an adaptive protection and control system, the industry is not using these methods and the usual approach is to rely on conservative protection settings. This study will lay the groundwork while highlighting the inherent advantage of the technology. Other practical contributions associated with the research are:

- Practical models for different cases
- Comparison between vendors

2.5. Adaptive protection review

The review of power system protection philosophy is motivated by the contribution of protection towards undesired events including cascaded failures discussed by Phadke [23] and the study in [24] suggests that close to 30 percent of events are false trips. Further to this, [25] advises that up to 70% events are connected to system protection. Current outdated prevalent philosophy is to isolate the fault and protect the equipment that starts to show its drawbacks if the system is overloaded. Hence, the requirement to balance reliability vs security gets challenging specially in a smart grid context. Begovic in [26] made application specific use of system level protection as opposed to component level integrating control and protection but this so-called system protection scheme introduced further issues and complexity. Other protection design issues include hidden system/component defects and obsolete organizational/market structure basis. The current industry focus is towards latest development in IEDs and ICT, but this work has the intention to explore feasibility of adaptive protection and control in a wide area setting from an architectural perspective as opposed to technology.

In theory protection, settings can be altered to disable or modified reach or change delay settings to optimize as per system state. In late 1980s and early 1990s, there have been tests to validate the concept in stages that IEDs or previously relays could be set in real time to align with system changing condition. Starting with a small IEEE 38 bus system [27].

Definitions are import and adaptive protection has been consistently defined as following:

- Ability – Automatic change/adjust operational characteristics/parameters
- Event – Changing/prevailing system conditions
- Objective – Optimal performance

This automatically implies the provision of robust (Secure and dependable) communication system, decision-making process and adaptable hardware/software at IED level. Review of work on the subject is illustrated in Table 2.1 and Figure 2.1.

Table 2.1 - Review Summary

Contribution Timeline and Summarization	**Period**	
Adaptive Protection, Initial Models	1988	1990
Fast Calculation Coordination Experimentation	=Do=	=Do=
Sectionalized Subsystems Studies	=Do=	=Do=
Digitized Relaying Architecture	1991	1993
Detailed Adaptive Relaying Demonstrations	=Do=	=Do=
Synchronized Phasor Capacities Utilization	=Do=	=Do=
Industry Wide Survey of Requirements	=Do=	=Do=
Relay's Contribution Identification towards Blackouts	1994	1996
Customized Adaptive Applications	=Do=	=Do=
Concept Identification of Concealed Failures	=Do=	=Do=
Online Protection Coordination Dialog	=Do=	=Do=
Further Application Development e.g. Transformer	1997	1999
More Implementation Methods e.g. Decision Tree	=Do=	=Do=
Wide-Area Models Experimentation	=Do=	=Do=
Concealed Failure Method Classification	2000	2002
New Localized Back-up Protection Methodology Experimentation	=Do=	=Do=

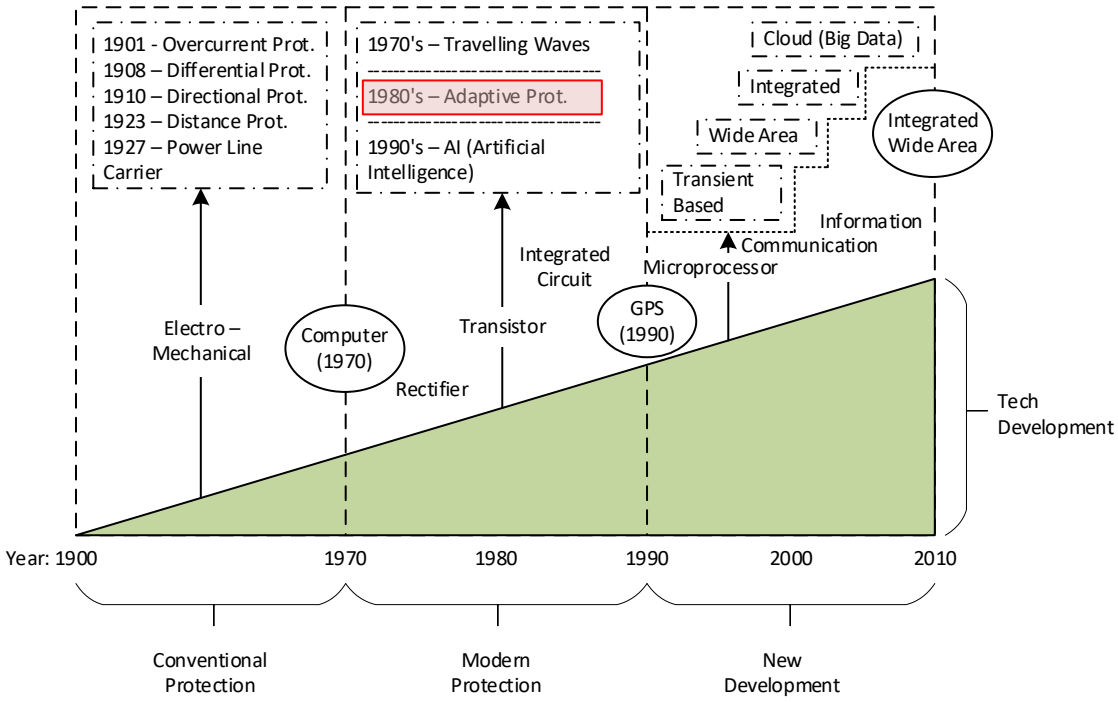


Figure 2.1 - Development towards an integrated wide area adaptive protection and control system.

The protection system inherently relies on interrelated measurements from a greater geographic area and the reaction is based on the operating state that is adaptive in nature [28,29]. Phasor measurements for a wide area network collection on a central location increasing the communication system requirements can alleviate the instabilities by a combination of tripping (Source and Load) and change in power flow. Locally the same issue can be resolved with load modulation that still puts high duties on the communication system. Another technique is area isolation within a short window from a central control centre which translates into fast reaction time involving communication and control. To maintain synchronism the above techniques, require reaction time within 1 to 0.1 Seconds depending on the size of the network and modern communication systems can achieve a reaction time of 150 milliseconds [30]. In a post-contemporary protection regime, an adaptive protection feature at local level would include adaptive automatic-reclosure, component protection and automated protection coordination. More contemporary adaptive protection techniques would include concepts like intelligent measurements/sensors/algorithms, artificial intelligence, adaptive control and communication. Dynamic system studies including but not limited to voltage and angular stability studies have a role to play [31,32].

2.6. System Design

Based on response type an adaptive protection scheme can either be reactive or preventive like maintenance regimes. In a reactive adaptive protection system, a component failure is isolated to stop instability propagation to broader system for example by islanding a stable portion [33,34]. While in a preventive protection, system architecture a critical section is parameterized to absorb the risk of component failure. This chapter will focus on the reactive adaptive as criticality of response time is significant as compared to preventive adaptive which will be studied via IEEE 179 bus system. The concept of an adaptive wide area network is shown in figure 2.2.

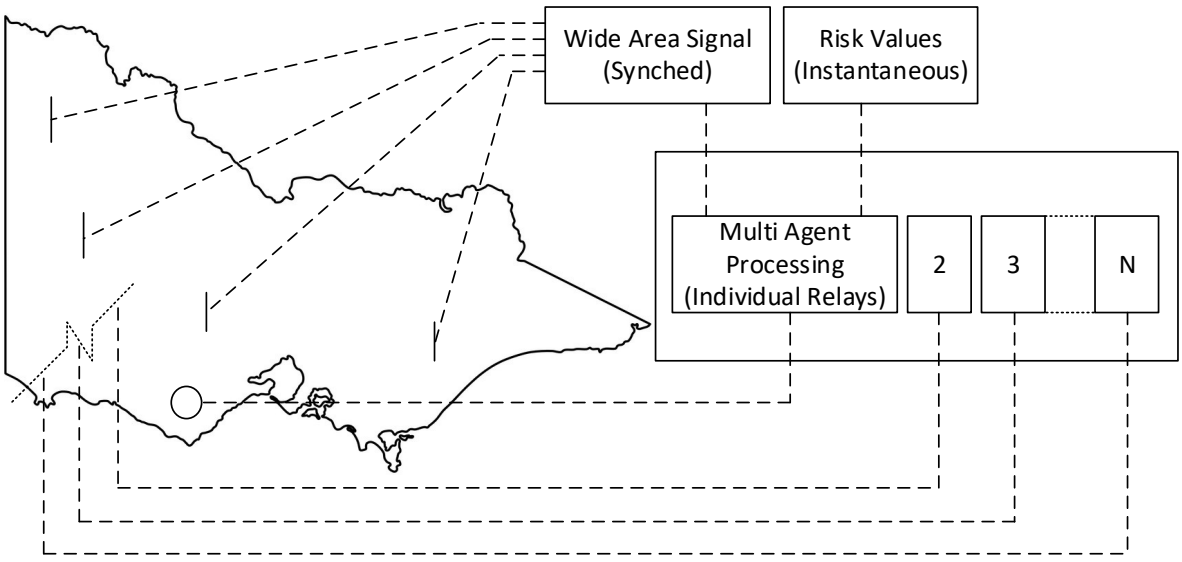


Figure 2.2 - Adaptive Protection (WAN) Concept

The case between security vs dependability is to be studied in system context rather in a unit context defining security to operate only when intended (unsecure system will cause false tripping) and dependability is not to fail in that instance (undependable system will case failure to trip). Device sensitivity setting is one way to change the preference between dependability and security, but the most important factor would be availability of designed contingency. Impact assessment is an important tool used to establish a philosophy that include the consideration for size and value of area effected while using backup protection. Numerical risk assessment will translate to following equation:

Acceptable Overall Risk = Cost of Relay Miss Tripping x Probability of Relay Miss Tripping + Cost of Relay Failure x Probability of Relay Failure

A basic comparison of parallel and series arrangement of two relays depicting a parallel protection scheme and series scheme would still indicate that overall risk could vary depending on the individual effect and probability. Another example is of a synchronous generator if offline will incur the fraction of the cost compared to an event in which it is damaged which may only be true with the availability of sufficient reserve. In the absence of a reserve or already stressed network, we are going to witness a more expensive or even disastrous blackout event and hence the overall risk is the only relevant criteria. Based on the grid stress value (GSV) it is expected that an adaptable system will adjust based on the live risk values. For higher GSV the protection should tilt towards security and for lower values, the protection should tilt towards dependability.

Another case is risk assessment between two different assets such as a transformer and a transmission line. Considering these two varying assets type's protection is assessed under two schemes that is two parallel relay (Dependable Scheme) or two series relays (Secure Scheme). The common element in the two schemes is both operate under readings in proximity to the asset. Among the N-2, N-1 and N network conditions, the dependability inclined scheme will be favoured for overall risk when continence is available whereas security inclined scheme will be favoured when operating close to the network limits.

It is also studied that in cases where the two assets are not independently protected or system state effect both assets then the overall risk will vary. It is also assumed in the previous section that the risk of relay failure is constant which may not be the case as this value changes for different operating conditions for example increases for a stressed network state. Protection philosophy is designed to circumvent protection failure and network burden. Phase comparison and differential protection failure is unsusceptible to line burden whereas distance and overcurrent protection failure is susceptible to line/asset burden.

As for some relays the failure risk increases with a stressed network which increases the overall risk further and the decision makers hence opt for a security inclined or focused scheme. Exploring the protection basics and its nature we arrive at two subsets that is micro layer agenda for relay/IED itself and macro layer agenda is at the scheme level.

Micro level deals with input/output relationships, studies relationship with settings, and internal mechanisms while macro level deals with protection coordination, black boxed micro-level and tries to reconcile the subjective/artistic aspects of design. A focus is required in the macro-level to bring standard solutions to this space. Reliability metrics can be studied further after this decoupling of protection space while understanding that IED's are susceptible to failure, self-contained, backup manages failure to operate, supervisory relay manages false tripping, coordination is time dependent, and margins manage noise-based uncertainty.

Figure 2.3 depicts a primitive but prevalent scheme that needs to be improved considering available enabling technologies. A shift in protection philosophy is noticed by virtue of dependable micro layer shifting the focus to secure macro layer and the basic unit of protection is also extended. The philosophy now caters for system level approach as opposed to a component level approach as protection now in addition to isolation may also change system conditions. Terminology has also changed from custom/special to system in a SPS (Special System Protection Scheme), still each SPS is unique due to specificities.

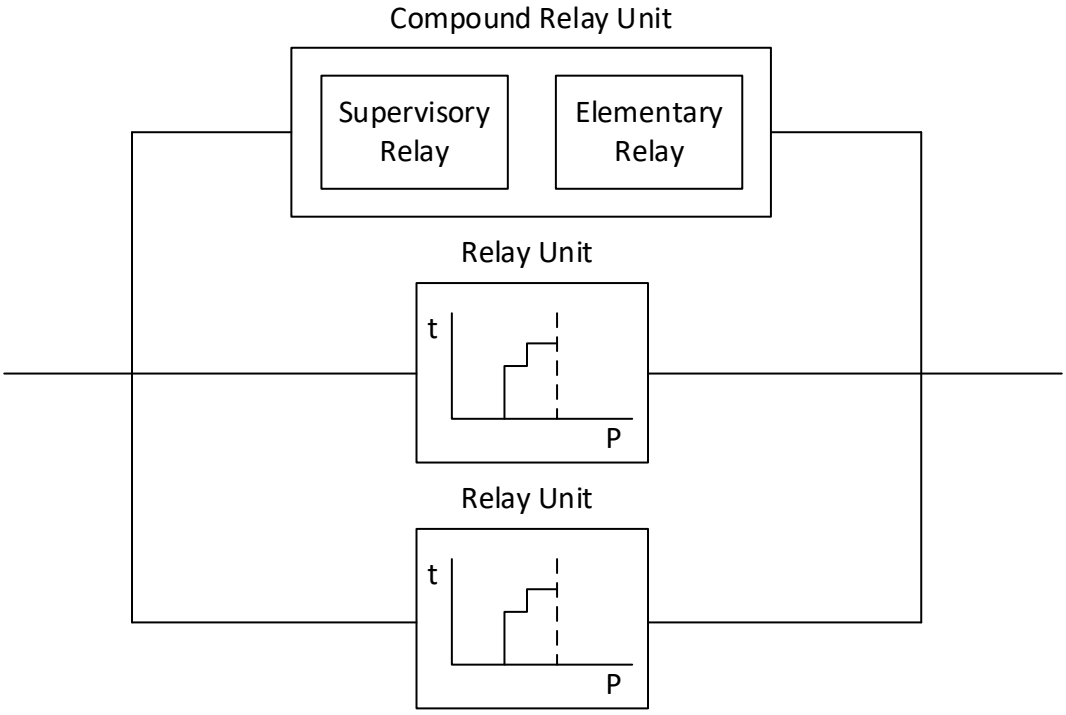


Figure 2.3 - Prevalent protection scheme's logical diagram

Broad Classifications of SPS exist such as centralized vs decentralized, and event-based vs response based. Infrequent nuisance tripping during infrequent requirement is a concern. System expansion was a challenge before but has been simplified due to availability of future

proofed standard, yet legacy SPS still pose a challenge. This challenge can be resolved by reconciliation of system level and component level.

Current research indicates that flexible adjustment and calibration of micro and macro layered protection is practical, but reconciliation of micro and macro layers would resolve the coordination issue. Based on the operational state the system settings inclination can fluctuate between dependable or secure considerations based on local and remote system values. In the absence of a smart grid a temporary SPS can be proposed unit a standardized smart solution is available.

2.7. Methodology

A three-level hierarchical decision tree is required in which the first level is the substation interconnection, the second level is the substation itself and the third level is the individual components. Figure 2.4 shows the arrangement for a wide area protection system.

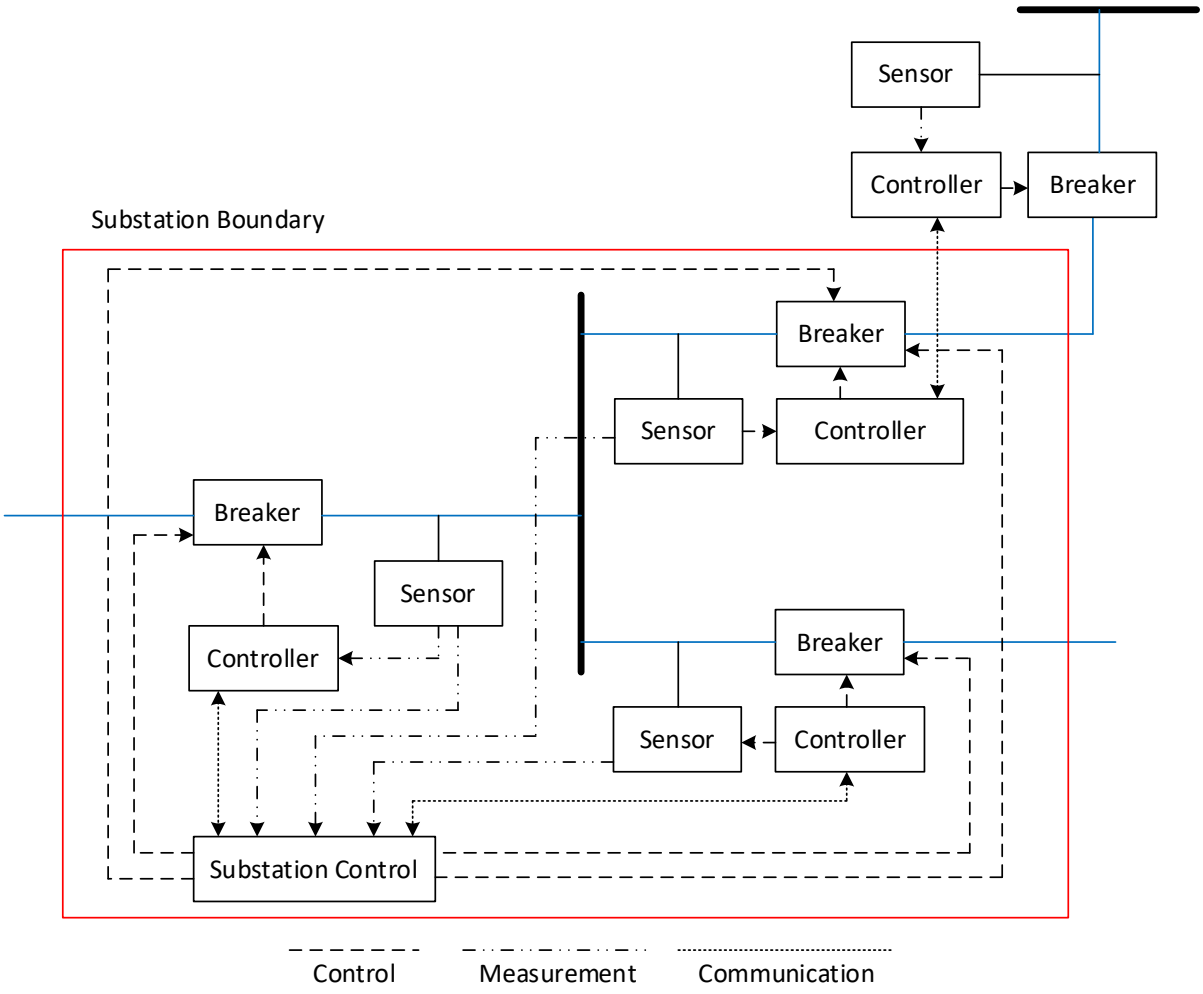


Figure 2.4 – Integrated Protection System (WAN)

Three level of controller are required to realize an adaptive architecture and all three levels have access to sensor data and can issue tripping command. These are central controller, substation controller and bay controller. In addition to control, this arrangement will also monitor all switching devices, have an update on failures and maintain up to date coordinated settings in either emergency or preventive modes of operation. This will include automatic lead shedding or isolation of supposed faulty section before congestion.

A coordinated response is possible for hidden failure, adverse system states, environmental and natural phenomena. Functionally an IED will perform the primary function independently, backup function will be coordinated instead of time delayed, parallel protection function will be communication based, IED risk is incorporated in settings and emergency mode of top two controllers will be data intensive.

The architecture considers a radial and non-radial communication and data intensive reliance to manage instrument noise and unidentified failure modes. System susceptibility values have a possibility of inclusion in system stability in a maintenance regime. The backup time delay consideration is swapped with the communication latency. The following assumptions are included in the proposal.

- No change in primary protection
- Backup communication channel needs to be addressed
- Architecture is technology & structure independent with the possibility of new devices and technology integration.

This work is focused on protection philosophy and system stability is not the intention but only a by-product. It is recognized that adapted protection entails real time modification of relay settings which can only happen in preventive regime as there is little time to calibrate in an emergency scenario. The suggestion here is the implementation of the concept on the IED level for a fast response.

The fast response requirement translates into manageable duty on the IED when defining the criteria for real time relay setting manipulation encompassing most system states and conditions. Existing devices allow for either a single or a multi criteria process. Although less powerful yet simple single criteria process or function has low or high out based on the input or its offshoots. Figure 2.5 shows a single criteria three-zone distance protection.

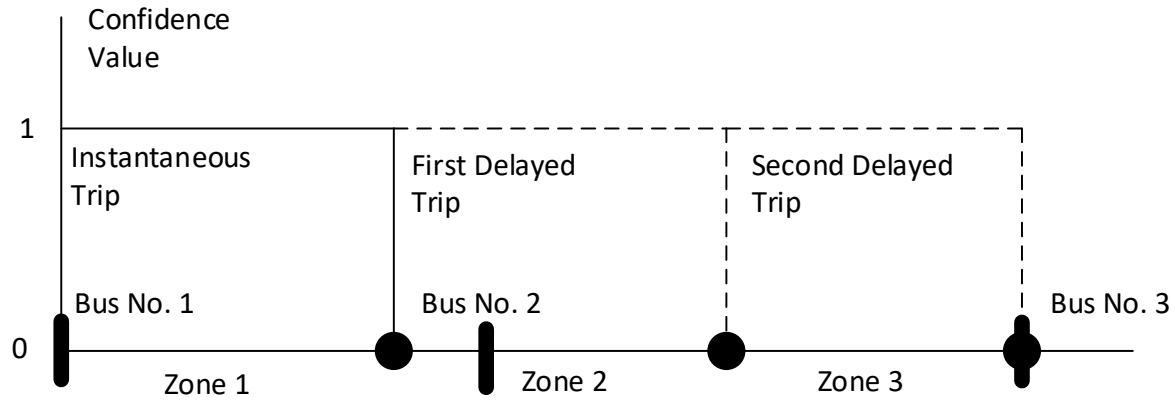


Figure 2.5 – Existing criteria of distance protection.

Multi criteria process as the name suggests incorporates multiple criteria while deciding protection-relying on multiple device's contribution such as synonymous yet different criteria functionality of main and redundant relay using a simple or weighted voting scheme. Additional investment in hardwired logic can provide AND/OR decisions between functionality of two or more relays such as the case with main and redundant devices. As two different functionalities can have different accuracy, a fixed weight is usually used to establish the overall criteria of operation after multiplication and comparison to a threshold.

Uncertainty and reality go hand in hand. Uncertainties exist in protection scheme that can be attributed to elements, calculations and communication. Much research has been contributed to standardize the uncertainties in the protection model and sources are identified such as operational conditions, system configurations, varying fault states, measurement inaccuracies, failed communication, calculation short sightedness, trade-off considerations and silent protection failure modes. The prevalent practice is to divide the system into subsystems to isolate and identify the source. Existing devices have limitations in terms of uncertainty considerations.

Most of the uncertainties are attributed towards knowledge gaps or holistic oversights. Objectifying the subjectivities in protection engineering is possible when uncertainty is captured and catered for in design. Currently practice is (1) monitor system readings against margined (2) threshold and modelled uncertainty can add tremendous value to this approach.

Engineering judgements can be modelled via a fuzzy set theory while the mathematical framework of probability theory can used to model objective uncertainty data. FL (Fuzzy logic)

can give a varying degree of impression for AI (Artificial Intelligence) in a protection system which is data error resistant, easy comprehension, and can account for non-linear functions while mapping input/output data. Due to layering, there is still a degree of human involvement based on the stipulated requirement. Other possessing intensive AI methodologies are ANN (Artificial Neural Network) and ES (Expert System) which will be implemented for real time applications in the future with the enabling technologies of the time. Other limitation of ANN is the network can have a non-standard operation and ES is domain specific that makes FL the most appropriate AI tool.

An example of a fussy distance protection is shown in figure 2.6. Each protection IED issues several outcomes with associated confidence value that goes through a voting system taking an instantaneous tripping decision against an adjustable threshold and subsequently informing peer agents.

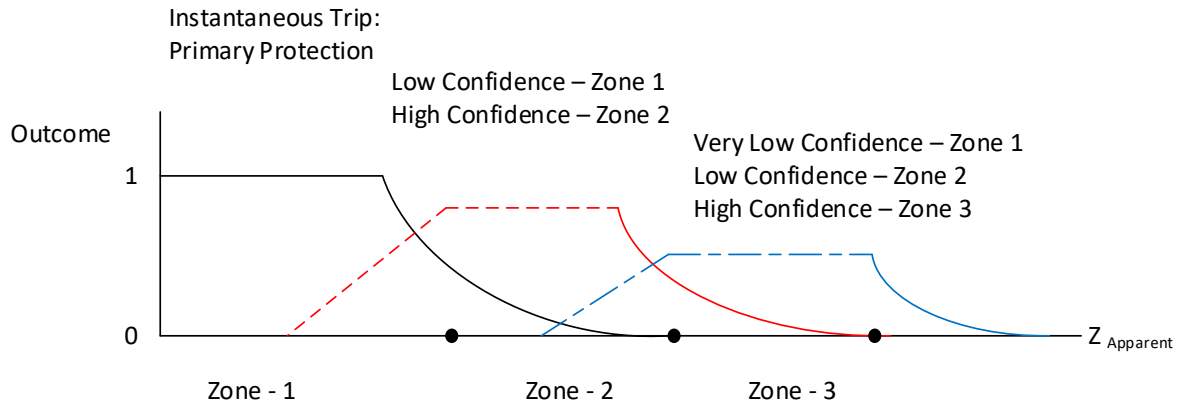


Figure 2.6 – A fuzzy distance charateristc function

Primary protection having the higher than threshold confidence value will operate instantaneously while low confidence value backup protection will rely on more informed decision and any intentional time delay is replaced with communication latency. The fuzzy logic can be implemented either by lookup tables or by functional calculation. The system is illustrated in figure 2.7.

Majority of transmission line faults are disproportionately temporary in nature, which are identified by a primitive trip and close cycle known as auto-reclosure posing safety and stability issues. Single or three phase temporary faults can be characterised to avoid the use of the primitive auto-reclosure scheme and in turn switching on to fault.

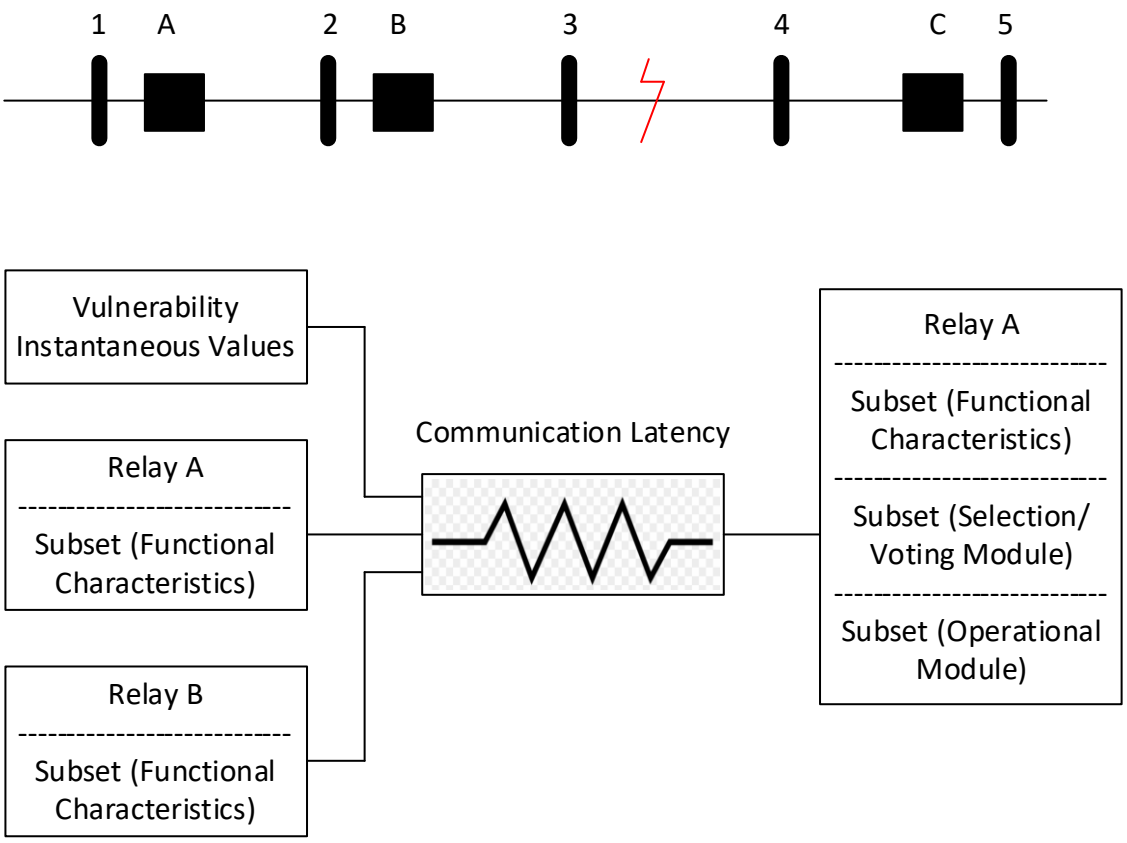


Figure 2.7 – Single proposed protection system's logical diagram

Adaptive auto-reclosure can be implemented by using ANN or a numerical technique by either utilizing the open circuit characteristic voltage waveform or high frequency transient fault components. Partial adaptability can be introduced by varying the reclosure time by arc extinguishing time calculation. It is suggested that a voting system can be implemented for auto-reclosure differentiating between temporary and permanent fault.

As stated before, communication is centre to adaptive protection system. Detailed review of review of required communication system has been introduced in Appendix 1-6. Adaptive protection operation speed is dependent on the speed of integrated communication system. A summary of stagged time calculation is included in the following table 2.3.

Table 2.2- Adaptive Protection Time estimate

S/No	Description of Activity	Time Estimate
1	Instrument Processing	4-5 ms
2	Communication With Central Controller	8-10 ms
3	Processing real time data	8-10 ms
4	Analysis with decision making	80-100 ms
5	Control Communication	8-10 ms
6	Breaker Operation	45-50 ms
	Total	145-185 ms

The time estimates are acceptable for preventive mode and backup protection, but emergency mode will require better IEDs. Protocols covered by IEC Standard 61850 are a logical choice for this adaptive protection and control system due to high degree of coordination requirements and the need for structured data. Legacy standards and associated protocols are not suited for adaptive protection because of inherent point list mechanisms, slow serial communication and master slave architecture.

GOOSE (Generic Object-Oriented Substation Event) covered under IEC Standard 61850 can support distributed decision making, counter latency via multicasting, ensure positive communication, support hold time and monitor IEDs. In addition to this GOOSE provides wide area applications and an object model is available through IEC Standard 61850.

2.8. Test System and Results

IEEE 179 Bus System is used to study the Victorian Power Grid and its interconnections in the context of adaptive protection and control system with a note that this does not essentially represent the real grid behaviour as the intension is to develop the prosed concept rather to study the grid itself.

A portion of the grid will be highlighted in the subsequent section to study the critical portion in a stressed system state where faults will cause instability of the overall grid of which an importance parameter is the X/R ratio showing the character of the grid impedance. The simulation is performed on PowerFactory® - DIgSILENT® software package and the system are depicted in the following figure 2.8.

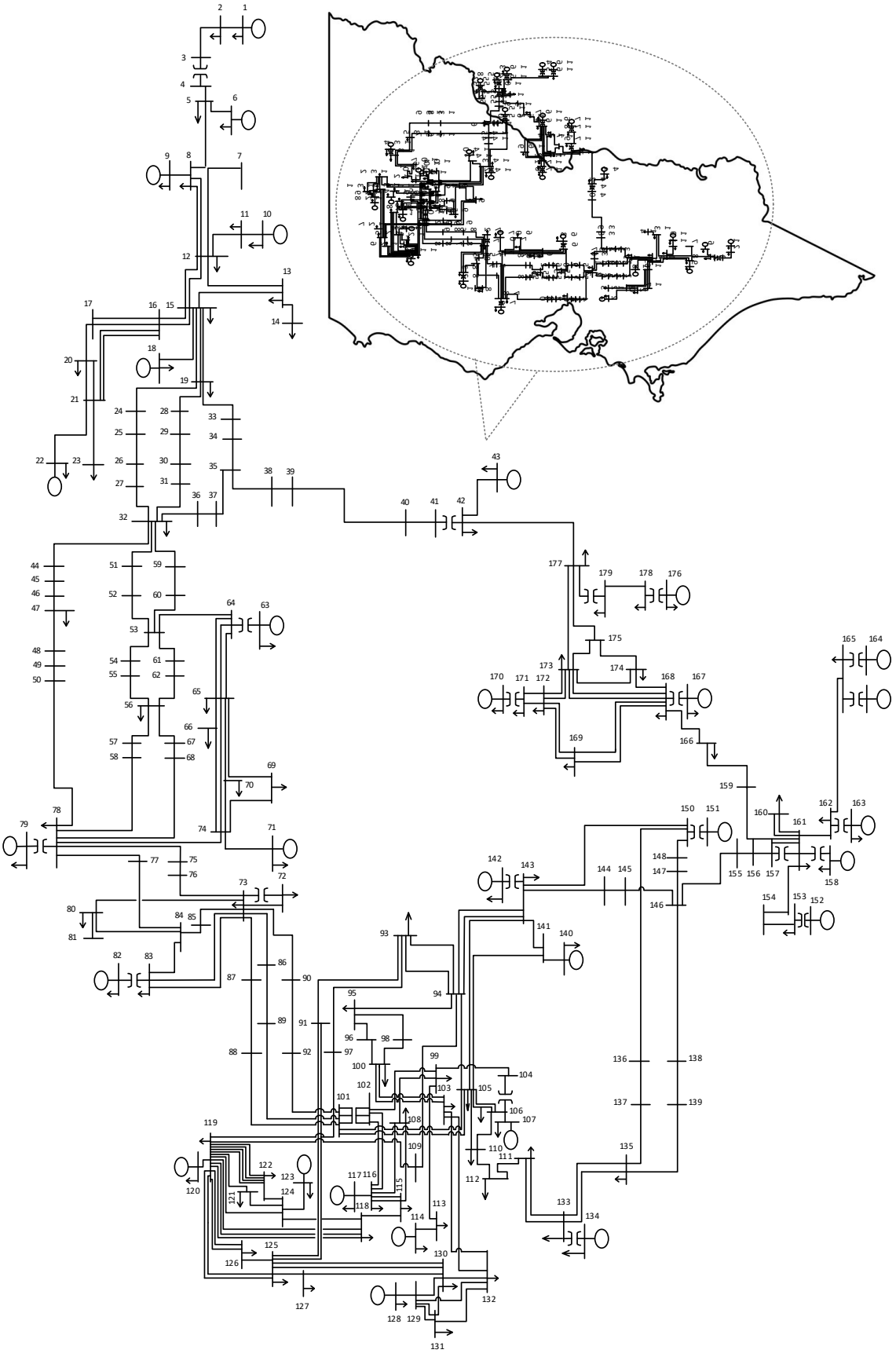


Figure 2.8 – Reference IEEE 179 Bus System overlayed on Victorian Power Grid

A usual operation (as shown in Figure 2.9) in case of three phase fault between bus eighty-three and one hundred and fourteen will trip both ends. A hidden failure may force the tripping of a parallel line causing the cascaded tripping of the critical portion of the system. An adaptive protection scheme can counter that by blocking the trip transfer function is stressed grid state, the adaptive protection could switch to preventive load shedding regime, or adaptive protection can rely to relay setting change in this scenario.

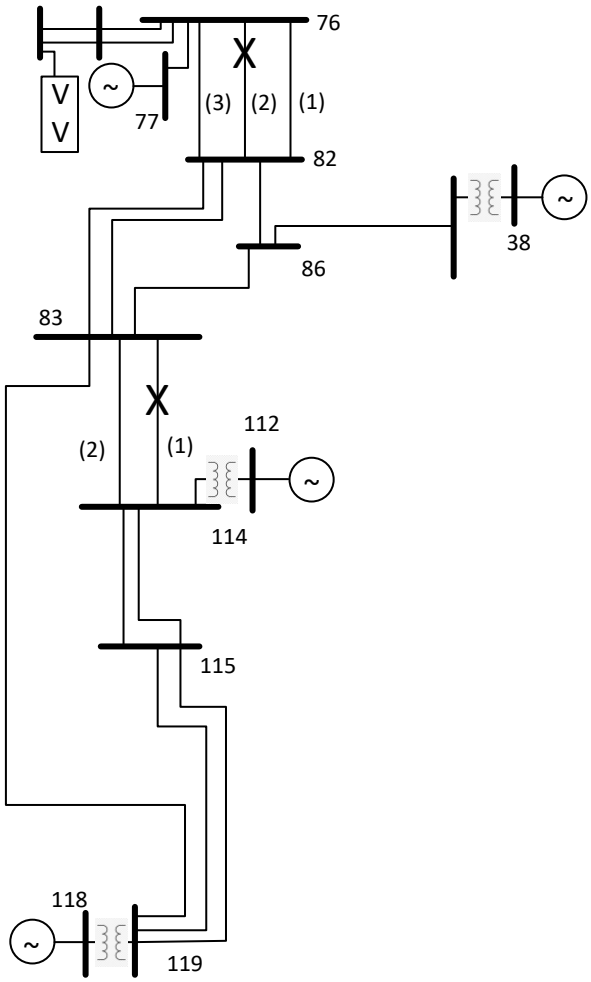


Figure 2.9 - Test system's critical section – Case 1

A usual operation (as shown in Figure 2.10) in case of a permanent three-phase fault between bus eighty-three and eighty-six will clear both ends of the line with a failure on breaker B will result in the tripping of all the other named breakers. This will lead to sever system instability and loss of synchronism. This situation can be avoided by preventive adaptive measures.

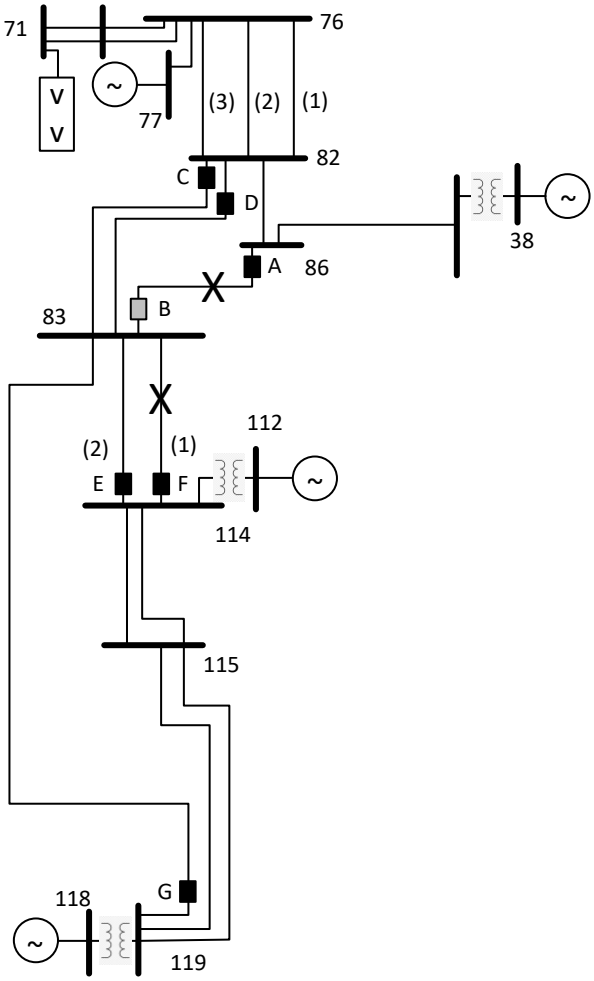


Figure 2.10 - Test system's critical section – Case 2

The adaptive mechanism will be implemented by a combination of adaptive reclosure, adaptive backup protection and adaptive load management.

In the following figure, the system is adaptive, and a fault occurs between buses eighty-three and eighty-six. Fuzzy logic is implemented on all Local/remote IED inputs via membership. The consequence would be a collective decision by all relevant agents rather than one element. After a holistic assessment, it will be identified that the fault is within agent A's area of influence with a faulty instrument transformer resulting in a tripping of only breaker A.

The same is depicted in figure 2.11.

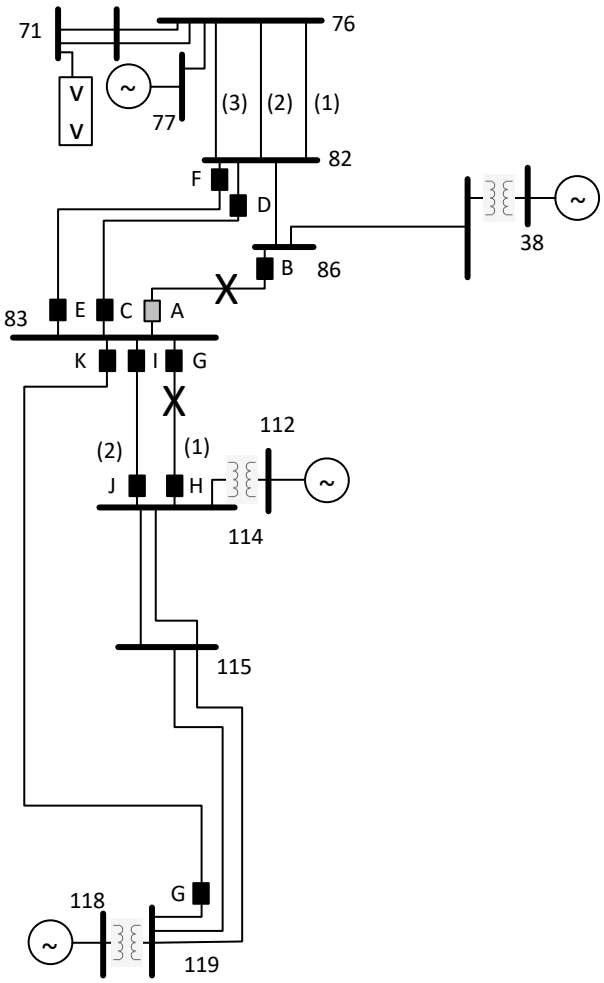


Figure 2.11 - Test system's critical section – Case 3

System insecurity increase with system loading and in a highly loaded system, the probability of instability and false tripping increases. A fault on a stressed grid can result in a non-recoverable voltage collapse. In addition, voltage dips in a highly loaded grid can cause false trips and lack of reactive power capacity can cause generator trips. This related loop will ultimately lead to total grid collapse.

Historically, it is recorded that protection system are blameable to initiate voltage collapse and unstable voltages will push the protection system towards failure. This cycle is shown in the following figure 2.12 and adaptive protection in essence endeavours to break this cycle. There is also room to the status of ancillaries.

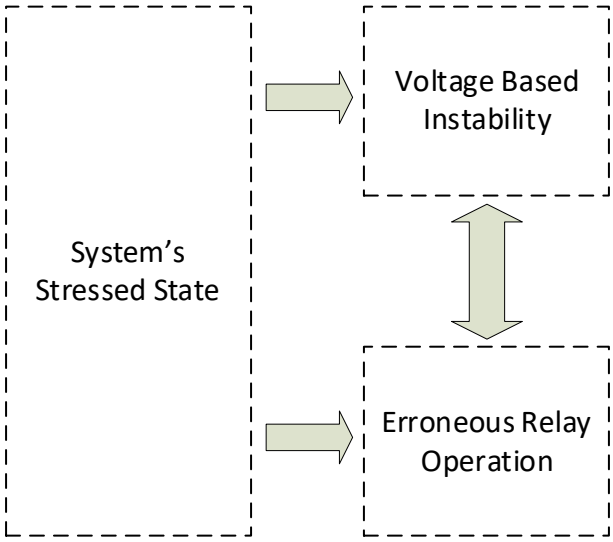


Figure 2.12 - Depiction of an exacerbation cycle

The protection system for SVC (Static VAR Compensators) are susceptible to false trips due high level of harmonics that nudges the inclination towards dependability as opposed to security with individual agent decisions as opposed to combined weighted decisions. Adaptive protection can consolidate the decision process as shown in figure 2.13.

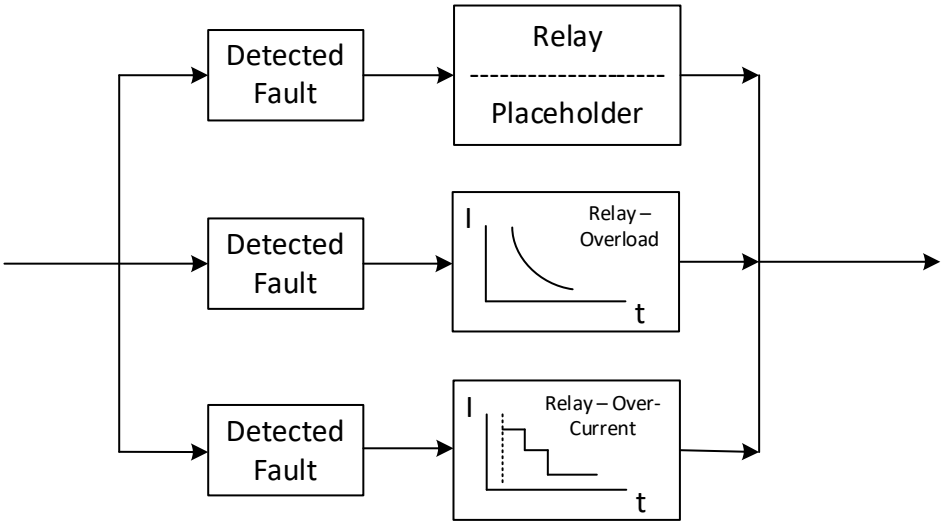


Figure 2.13 – Conventional SVC Protection Logic

2.9. Conclusion

We have seen that structure of the traditional transmission and distribution system has undergone through a fundamental change because of market changes. This local energy flows between the source and the load fashions an impression of subsystems. These subsystems come with their own issues and considerations of which needs to be made for power system protection and control effecting the broader system. This exercise has helped us to understand that the solution of these challenges lies in the IEC 61850 standard used in the context of adaptive protection and control.

As we know and have concluded in this section that the system protection causes much of the disturbances due to distributed agent-based architecture, it is a natural suggestion to go towards an integrated approach with the availability of enabling technologies. It is also suggested that there is a need of greater focus on the communication and protection architecture for wide area power system that in essence is integrated and adaptable system.

Chapter 3: Development of adaptive protection for intelligent power systems

3.1. Background

An increased living standard and GDP calls for a reliable grid which is challenged by security concerns environmental factors and commodity super cycles. To address these concerns a distributed generation setup can offer a few advantages which conflicts with the traditional grid design based on some set energy flow patterns. This is also in opposition to the designed fault flows [35].

The solution these issues is adjustable & coordinated protection of distribution system. Protection conventionally stives to timely isolate only the faulty section or shed only the right amount of load by means of primary and backup protection devices. This chapter will explore the adaptive overcurrent protection for commercial and industrial implementations operating in the form of a microgrid [36].

Traditional grids have a radial structure which is evolving due to distributed generation and microgrid capable to operate in an islanding mode. There is also possibility to move some DG components which are available as mobile systems [37,38]. With numerous advantages micro grids have a few technical issues for protection and control due to:

- Intermittent sources
- Varying level of fault current
- Bidirectional flows
- Variable DG numbers
- Variable topology

The system will require fit for purpose protection and adaptive protection fits the bill. The three main considerations for protection design are different system short circuit values for different modes of operation, direction of power flows and source availability [39]. Microgrid protection can be benefit from the use of communication based centrally coordinated protection scheme with a local backup protection philosophy in an event of communication failure.

Figure 3.1 illustrates a typical micro-grid with a mix of renewable and non-renewable DER (Distributed Energy Resources, energy storage, and utility grid connections. The industrial

terminology for utility grid connection point is PCC (Point of Common Coupling) which facilitates both grid connected and islanding mode connection/disconnections [40].

It was proposed in chapter 4 to utilize a traditional approach and take it a step further to introduce a decentralized offline adaptive overcurrent protection. In this chapter the concept is developed further to propose an online adaptive centralized protection scheme catering for the increased complexity of microgrids beyond a simple radial microgrid system [41].

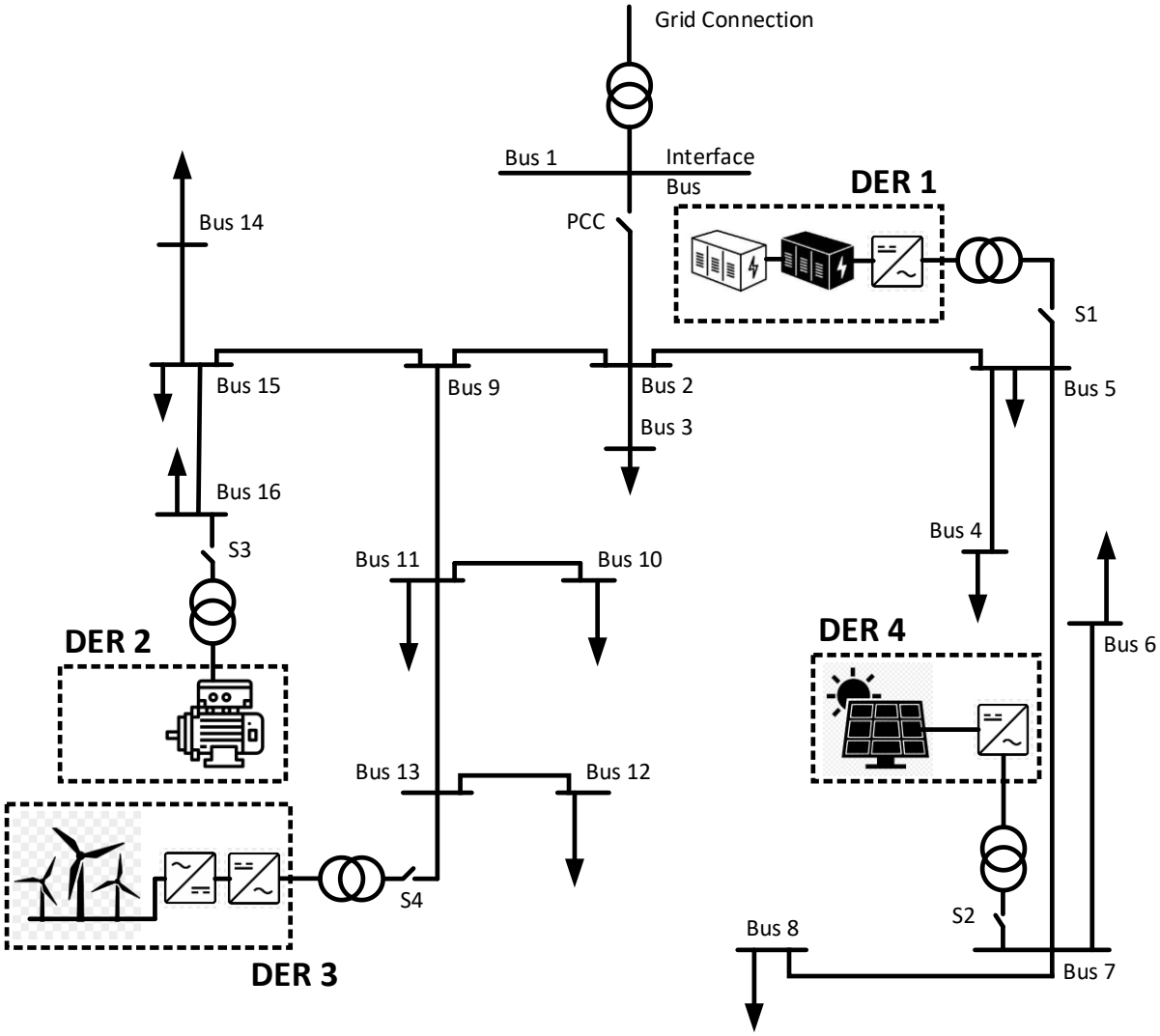


Figure 3.1 – Typical Microgrid

The above micro-gird usually has three configuration options shown in figure 3.2, 3.3 and 3.4.

- Radial Arrangement
- Ring Arrangement
- Mesh Arrangement

Protection strategy for these arrangements can be different and adaptive protection plan as multiple connections/paths can add to complexity for protection. For this reason, a centralized adaptive protection scheme can manage this complexity, as this will support a comprehensive reliable operation.

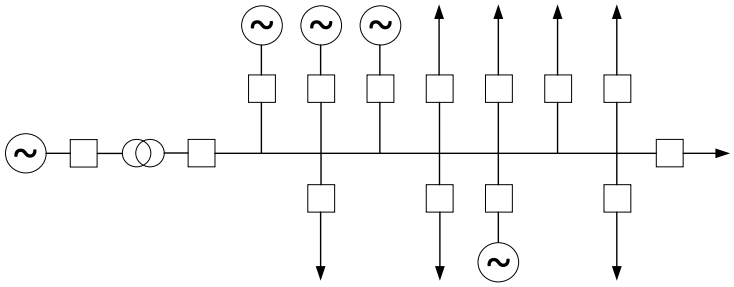


Figure 3.2 – Radial network configuration

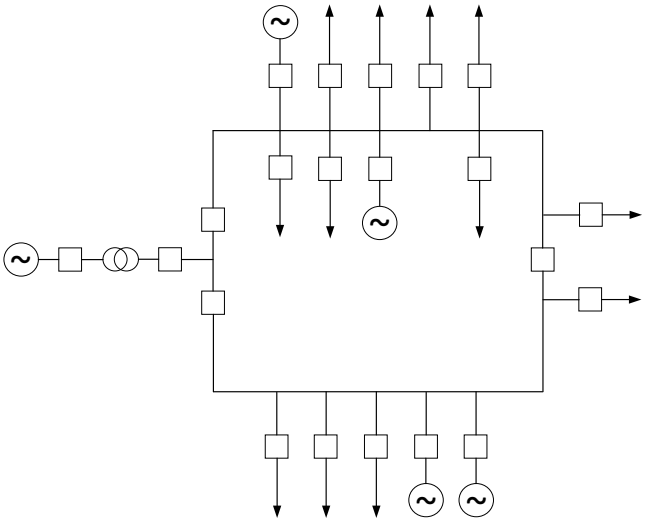


Figure 3.3 – Ring network configuration

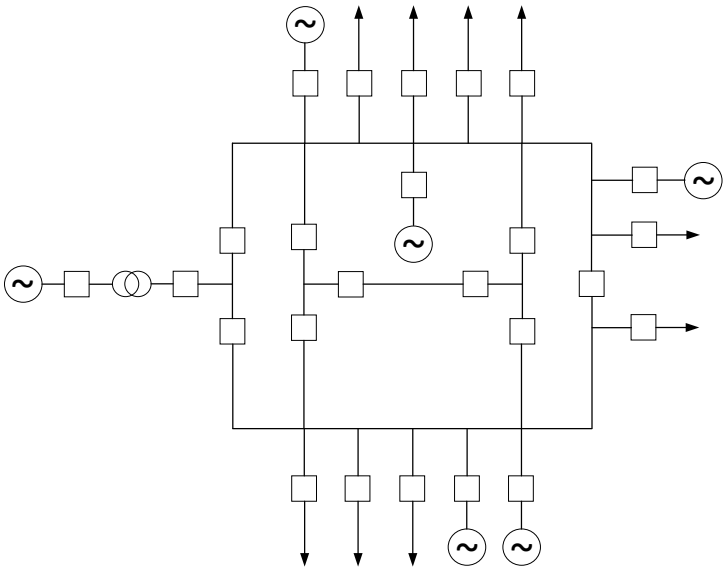


Figure 3.4 – Meshed network configuration

3.2. Incorporating an adaptable supervisory zone of protection concept

For a distance protection system, the IED responds to Voltage, Current and Phase Angle of the transmission line asset while computing the apparent impedance of the line. In a fault scenario the impedance will include the fault impedance. On a R-X plane we can plot the characteristic impedance of the transmission line where reactive impedance is along the x-plane while the resistive impedance is along the y-plane. A sample three step distance protection setting for a transmission line is shown in figure 3.5.

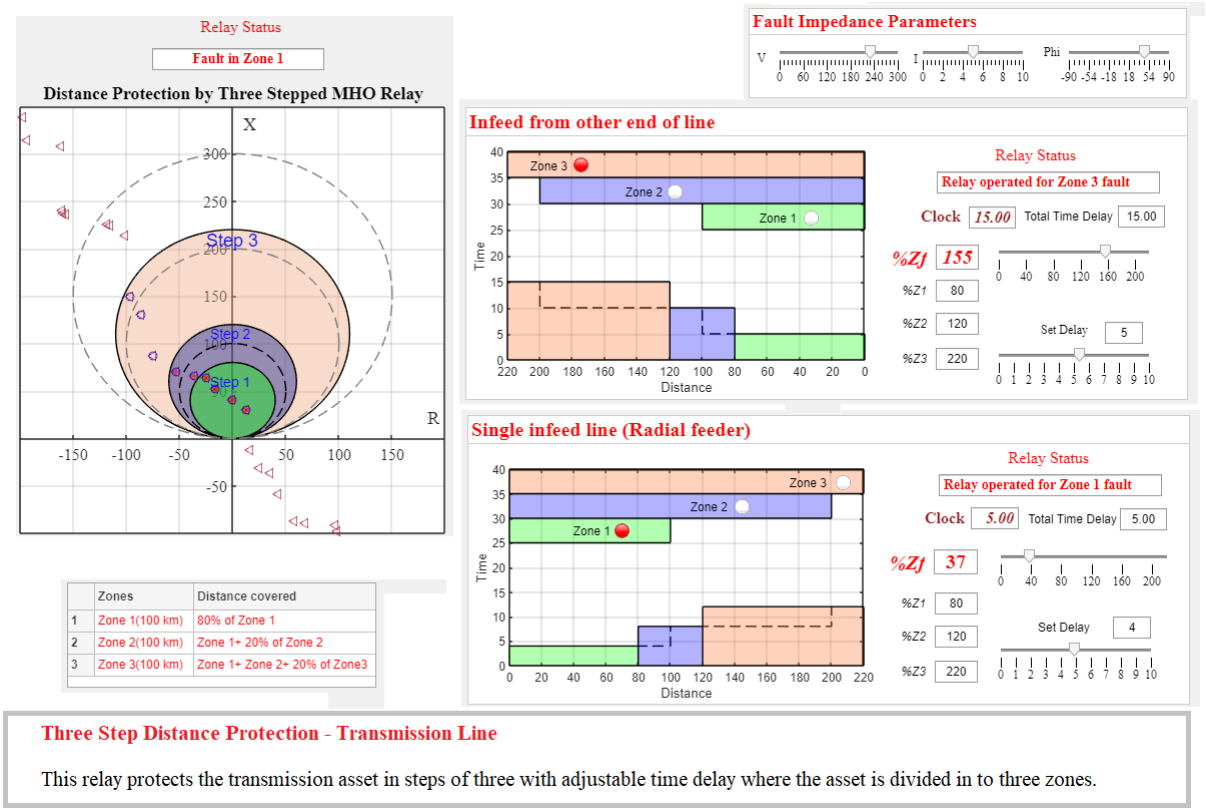


Figure 3.5 – Sample three step distance protection setting for a transmission line

The green circle indicates the first zone of protection, followed by second and third zone of protection encompassing 85%, 120% and 150% of line respectively. It is evident that second and third zone protects adjacent assets and adjacent protection will overlap with subject asset protection with time delay as the coordination mechanism.

It should be noted that this type of protection has a load-ability limit because an increase in load will reduce the apparent impedance due to increased current value and encroaching in to the third zone.

$$Simp = 3\frac{E^2 n_i}{Z_r n_v} \qquad \text{Eq. 1}$$

$$S_{moh} = \frac{E^2 n_i}{Z_r \cos(\theta + E_\varphi) n_v} \qquad \text{Eq. 2}$$

The above equations suggest load-ability based on an impedance and a mho relay. Load-ability can also be adjusted by changing the shape of the zone. Building on these concepts to develop an adaptable protection system, we can address the load-ability issue which has caused some historic blackouts.

Supervisory zone of protection is one of the mechanisms by which load-ability related cascaded tripping can be hindered as the breach of secondary zone of protection would require human intervention or automated decision-making. This is where we can adjust the preference between dependable and secure system avoiding catastrophic events. Supervisory zone is introduced on top of the three zones which will comfortably detect a slow-moving load increase scenario. The introduction of a basic timer between the impedance crossing of supervisory zone and third zone can measure the speed of movement. This allows to block the relay operation during a slow-moving load increase scenario.

This is an offline adaptable scheme at best when offline simulations would calculate the timer value to avoid online computation. The offline simulation would provide the necessary mechanism for fault characterization. One the relay is parameterized, the measured values of current, voltage and phase angle can be used to calculate the complex impedance for all phases. This value can have two condition outcomes that is normal or abnormal state. With a change in state from normal to abnormal will initiate the timer to determine two additional states of abnormal state that is fault or no-fault both for upstream and downstream locations.

This was implemented on a SEL-421 for high-speed distance and directional protection relay which allows a block-based programming. The simulation resulted in expected results.

3.3. Overcurrent protection of an adaptive microgrid

Distributed generation poses certain implementation issues even with its clear advantages. This is because renewables can have intermittent or unpredictable generation and may create stability concerns. Energy storage addresses some of the concerns posed by intermitted generation [42]. The per unit cost of DG is higher because of these allowances. Large DG switching can cause serious issues to overall health of the system such as challenges

to system protection, power quality issues, and equipment malfunction because of thermal reasons. Bidirectional power flow is also a challenge to protection and control as well as interlocking when the operator's intension is to provide a reliable supply. The overall acceptable risk equation discussed in chapter 2, changes with the insertion of DG. The duration of short circuit for DG is different to conventional generation and will also require a consideration such as inclusion of anti-islanding mode (based on active and reactive power capabilities).

Distribution network characteristics are modified with the introduction of DG which causing disruption for system protection. Magnitude and direction patterns of fault current is altered which may cause component failures. Figure 3.6 shows such condition. Introduction of DG may also cause system coordination errors which will result in tripping of unintended circuits as shown in figure 3.7.

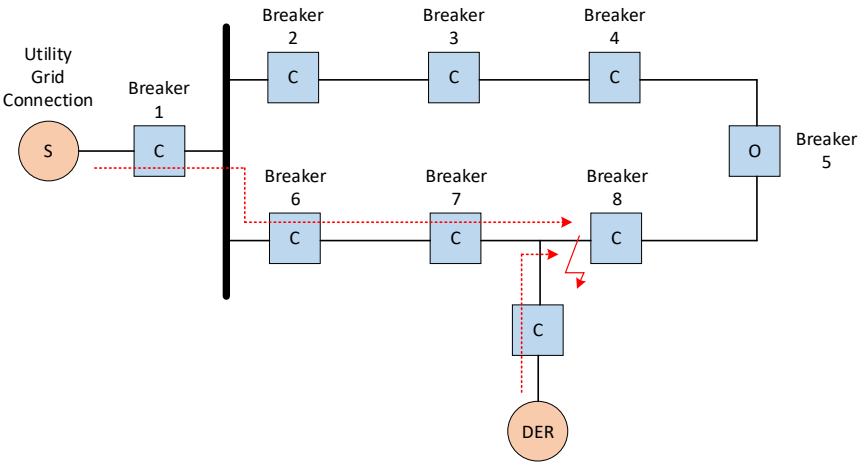


Figure 3.6 – Increased Fault level because of DG

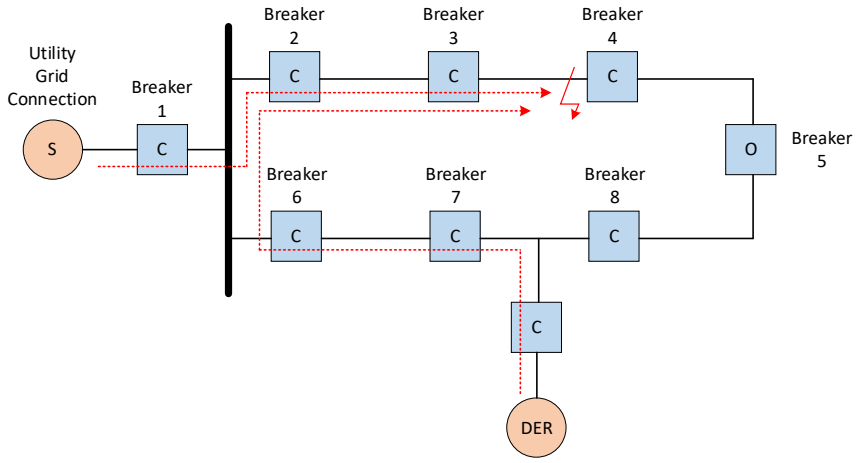


Figure 3.7 – Coordinaiton loss because of DG

Grid connected and islanding mode have different fault values and would require adaptable settings as per the system state. Figure 3.8 and 3.9 illustrates this difference in value and the contribution of two sources.

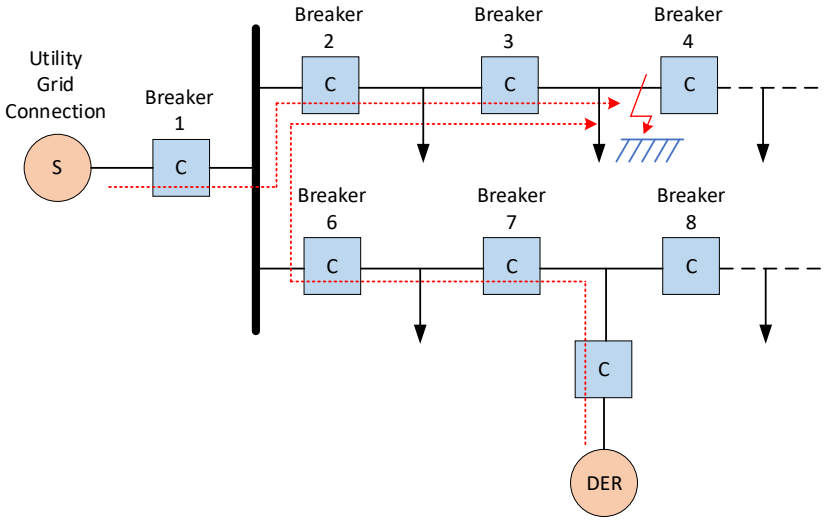


Figure 3.8 – DG introduction causing unintended Islanding (Schematic)

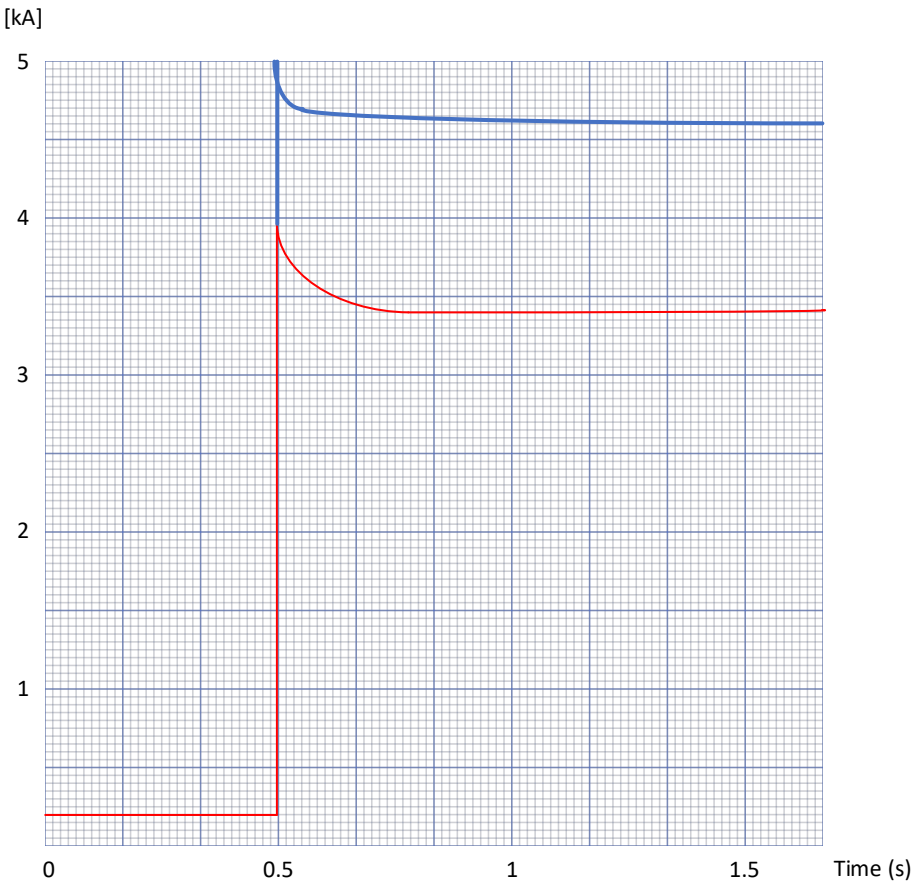


Figure 3.9 - DG introduction causing unintended Islanding (Fault level)

In a radial feeder setting the IED is configured to cover a specific distance and the reach is defined by the current pickup value. As the DG has a contribution to the total fault current and the resulting impedance, the responsiveness of the upstream protection is degraded and at times causes blinding of protection. Same is illustrated in figure 3.10.

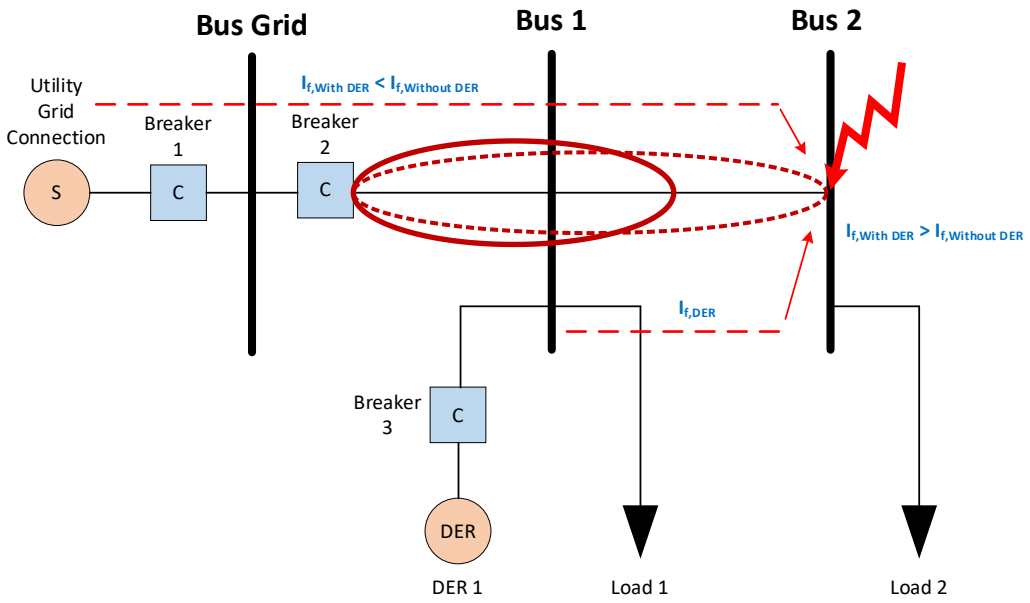


Figure 3.10 – DG Causing proteciton blinding

Another concern is that of nuisance trip such as sympathetic trip which is an undesirable trip initiated by a neighbouring circuit experiencing fault or overload. In a network configuration where the DG is supplying to a neighbouring connected circuit as shown in figure 3.11, the neighbouring circuit fault will be picked up by the DG connected circuit. This can be resolved by a communication based adaptive protection.

It is evident from these examples that we can no longer rely on the principal of designing the protection for the worst-case scenario. Also, time delayed coordination will not be feasible in certain network configurations and conditions. For the main power flow paths, a fuse won't be an acceptable choice. In addition to DG, we have REFCL (Rapid Earth Fault Current Limiter) implementations in Australia which also require coordinated protection in order to avoid nuisance tripping or asset failures such as cables.

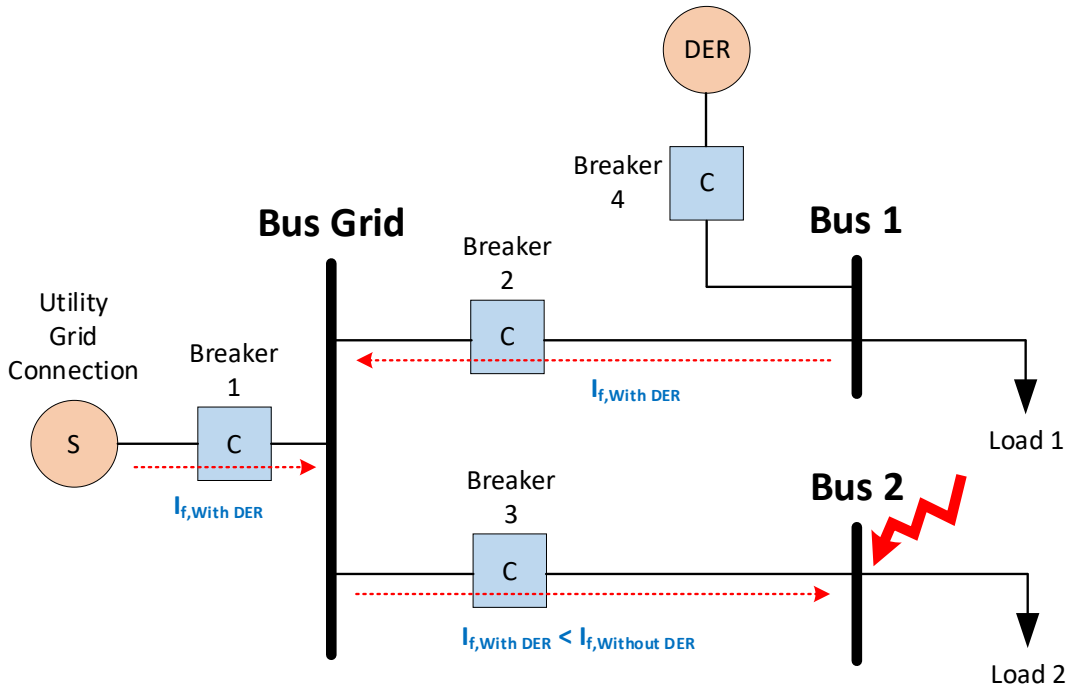


Figure 3.11 – DG causing supportive/sympathetic tripping

Figure 3.12 illustrates the structure of a typical IED which we can use to our advantage for adaptive overcurrent protection. The central controller or present values on the IED can change the settings such as operating time, pickup current or time dial settings based on the system configuration options.

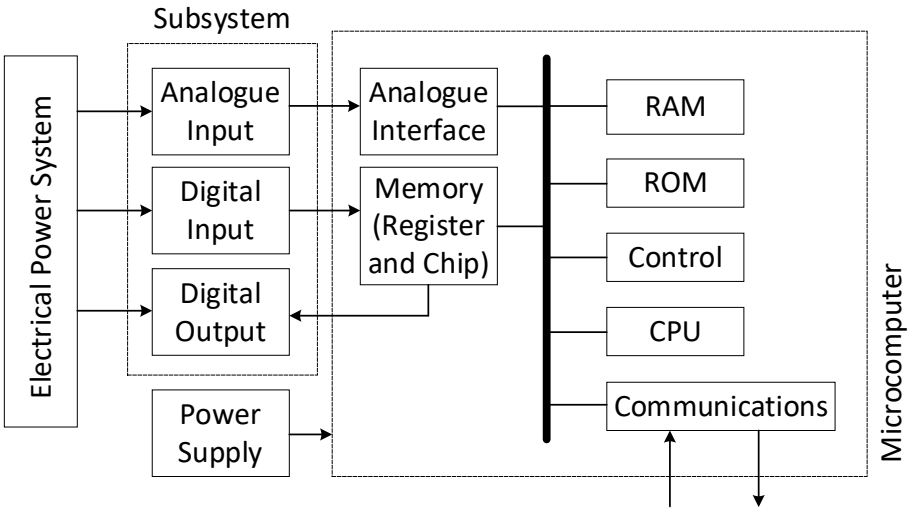


Figure 3.12 – Digitial relay structure

IEC Standard 60255

$$t = \frac{K}{\left(\frac{I}{I_s}\right)^{\alpha} - 1} \times TMS$$

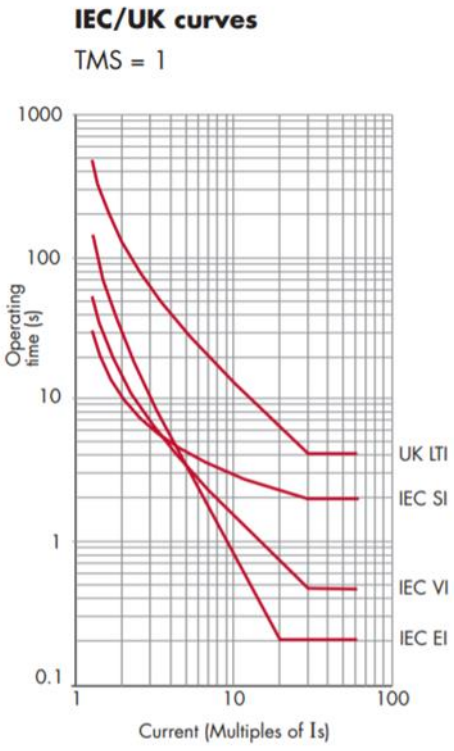
T = tripping time in (S)

I = fault secondary CT current (A)

Is = relay pick-up current setting

TMS = time multiplier setting

Characteristic	α	K
Standard Inverse	0.02	0.14
Very Inverse	1.0	13.5
Extremely Inverse	2.0	80
Long-time Inverse	1.0	120



IEEE Standard C37.112-1996

$$t = \frac{TD}{7} \times \left(\frac{K}{\left(\frac{I}{I_s}\right)^{\alpha} - 1} + \beta \right)$$

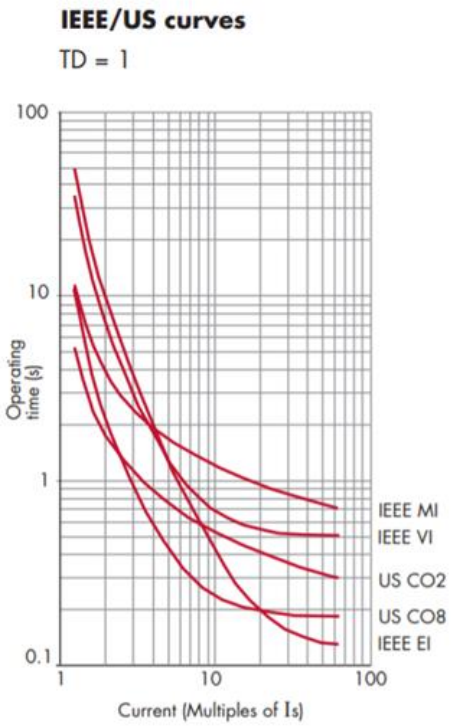
t = tripping time in (S)

I = fault secondary CT current (A)

Is = relay pick-up current setting

TD = time dial setting

Characteristic	α	β	K
IEEE Moderately Inverse	0.02	0.114	0.0515
IEEE Very Inverse	2.0	0.491	19.61
IEEE Extremely Inverse	2.0	0.1217	28.2
US CO_8 Inverse	2.0	0.18	5.95
US CO_2 Short Time Inverse	0.02	0.01694	0.02394



The adaptive protection settings evaluation for overcurrent IEDs can follow the following process shown in figure 3.13 to account for all topologies and configurations of the distribution system or sub system.

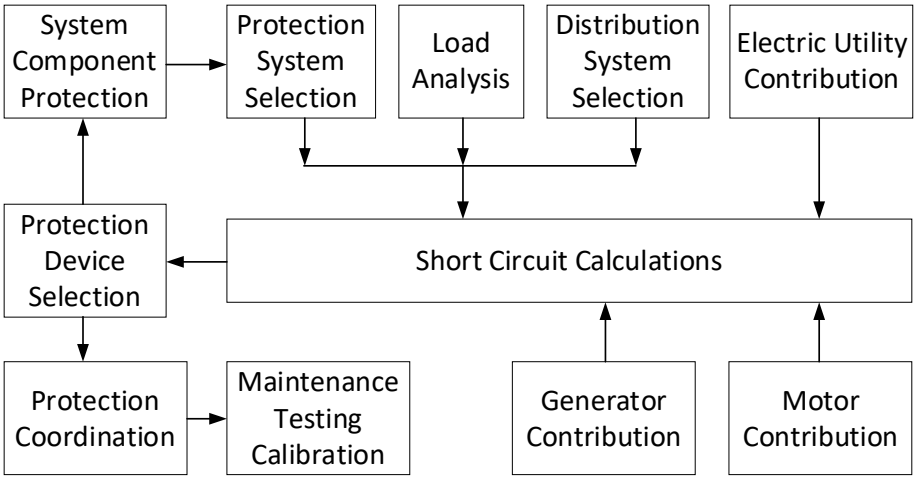


Figure 3.13 - Coordinated protection process

3.4. Centralized adaptive microgrid protection

As discussed, DG and network configuration contributes to fault current variation which requires dynamic restructuring of protection system. This chapter proposes an online adaptable system reconfiguring the protection response which requires:

- Directional and digital overcurrent IEDs
- Multi-setting IEDs
- IEC Standard 61850 based communication interface for protection coordination

Figure 3.14 shows a centrally controlled communication-based protection implementation where MCC (Microgrid Central Controller) is a controller equivalent to station controller. The communication lines indicated in the figure are station level IEC Standard 61850 based communication links capable of settings selection. The local device can check against two criteria of which one is local and the other is remote MCC. MCC can also close and open the breaker in case of false local trips.

MCC performs a monitoring function in addition to acting as a central controller. MCC will be maintaining an event table based on offline simulations and online operations will be supported

by this event table. The offline operations will be supported by this event table. The offline simulations will cover all fault and operational scenarios.

The multi-setting directional overcurrent IED will match the settings of the event table pre-emptively by means of an action table. The event table will respond to system state based on simulation which will select the action table which maintains the record of protection counter measures (Relay Settings) and ultimately performing relay setting selection.

In order to propose fail safe system, in case of communication failure the system will inhibit a change in system configuration and the protection system will maintain the last selected protection counter measure which will be up to date as per current system state as no further changes are permitted. With the communication recovery the system will permit control operations. Refer to appendix C for communication environment basics.

As there are redundant communication links a communication failure event is unlikely. Each communication site has a GPS receiver for time synchronization.

3.5. Case Study – Microgrid adaptive protection

The reference grid is shown in figure 3.15 which is a university campus supporting grid connected and islanding operations with renewable and thermal distributed generation. Each load and renewable source are connected via RMU (Ring Main Unit) creating 7 loops all around the campus which are mostly cable-based connections.

Protection philosophy has following main points:

- Islanded short-circuited values are balanced via generation control.
- Local directional overcurrent has a hierarchical settings control.

  (That is: Load Level < Loop Level < Feeder Level < Microgrid Level)
- Adaptable Settings (Event and Action Tables) are maintained on the microgrid level.
- Looped structure introduces an additional layer of reliability.

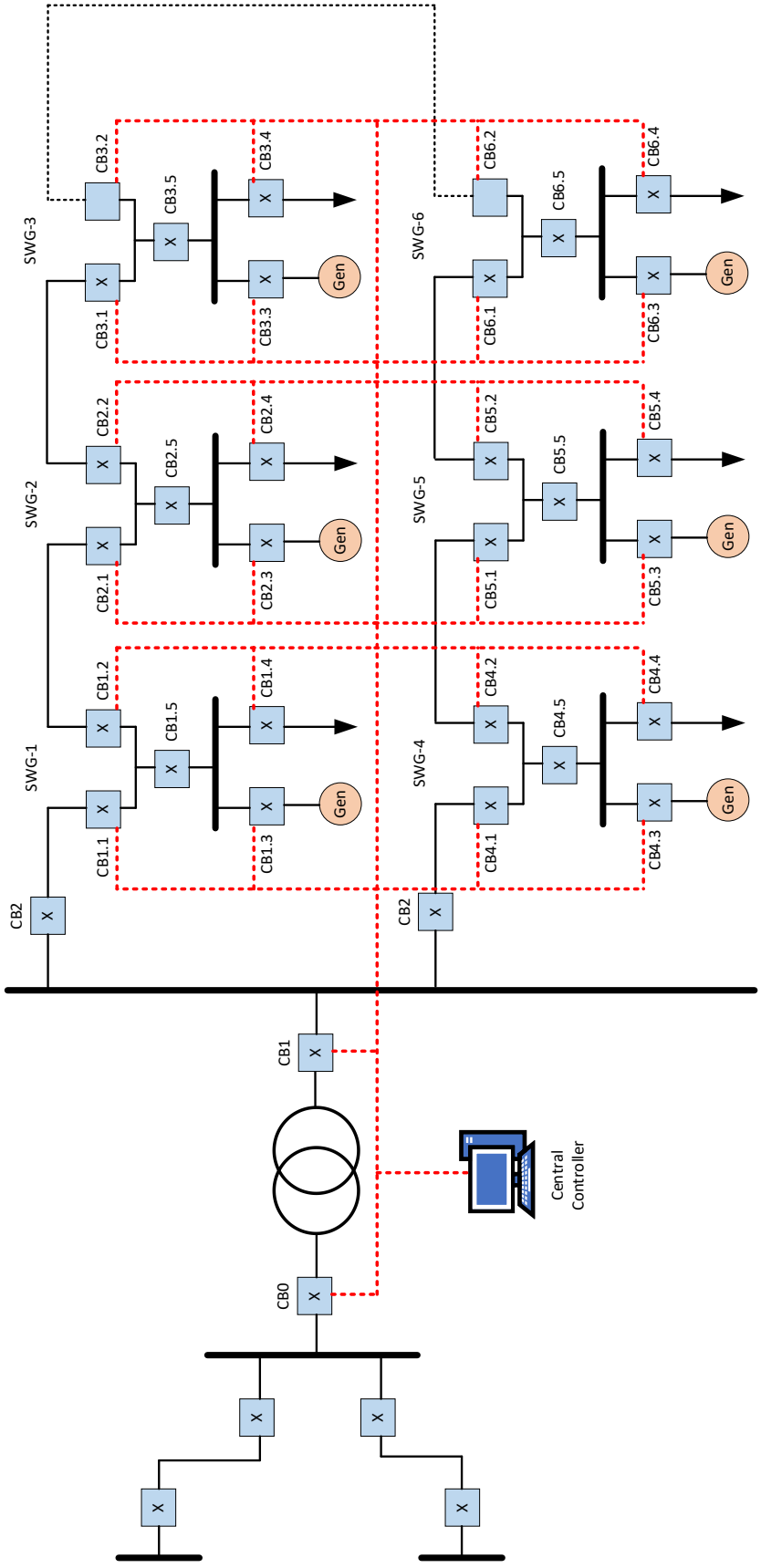


Figure 3.14 – Centralized Adaptive Protection Scheme

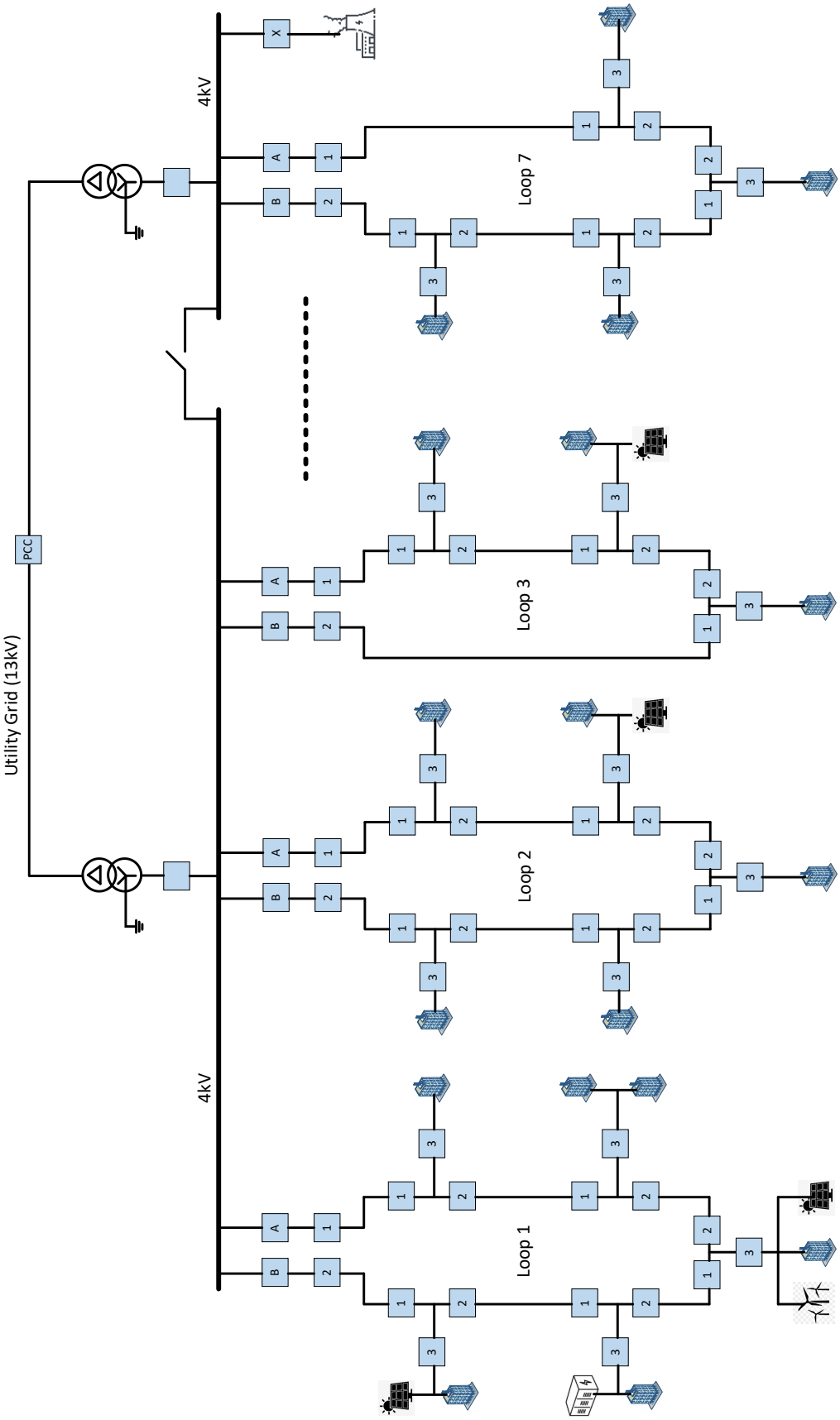


Figure 3.15 – Case Study for micro-grid

3.6. Conclusion

It in concluded that simplistic concept of supervisory zone of protection can provide an adaptable solution which can distinguish between heavy loaded and fault conditions. This concept can be easily implemented by transmission line companies to protect the system from major black out events for heavy loaded events or during bush fires.

It is possible to implement a pseudo-adaptive protection system while utilizing the multi-settings available in IEDs available as COTS (Component/Commercial of The Shelf) reacting to the system situations based on the calculated pre-setting conditions. The same mechanism can cater for protection challenges posed by DG such as protection blinding, sympathetic trip and coordination issues. As this offline multi-setting adaptive technique is flexible, we can incorporate it both as distributed and centralized protection regimes.

This chapter strives to provides a simple protection solution to different complex microgrid structures being encountered with increased DG penetration. The solution entails the introduction of a simplified adaptive protection system which relies of matching tables for different microgrid scenarios while utilizing multi-setting overcurrent IEDs which select the settings relevant to the prevailing grid state. This solution although simple yet covers all the necessary requirements of protection through an MCC.

Chapter 4: Adaptive protection and control based on IEC 61850 Standard

4.1. Background

Dormant faults due to otherwise nonoperational device and settings becomes relevant in an unfortunate operational state [44]. These dormant failures will further worsen the operational state in which it came into light and an intelligent adaptive system can identity these dormant faults via data analysis. The review in this chapter is intended towards novel philosophies introduced by digital relaying. A distance protection philosophy is based on the known unit apparent impedance which is varies from the desired relay characteristics for an undesired state of transient and bolted faults. An intelligent electronic device/relay can read the speed of shift in characteristic resulting in distinguishing the type of event.

Power systems starting from a humble beginning of a geographically limited DC generation and distribution have come a long way [45]. AC system moving to the concept of the grid has inclemently increased interconnections which itself has created challenges such as increased fault current and cascaded failures. The planning function thus has become complex covering a huge network of generation, transmission and distribution via a detailed yet fine balanced act. Increased nature scheduled type of distributed generation and combined generation/load elements cause complex power flows. The system at multiple points is fixed due to fixed plant specifications but a smart system of the future would be able to manipulate some of these parameters to drive efficiency [46]. Transformers realizing multiple voltage levels but also introduces the most rigidity to the system along with associated accessories. Increased transmission voltages reduce losses which are brought down for distribution which itself introduces dynamic requirements on the load end based on changing nature and value of the load. The load side management can introduce issues like varying harmonic levels and reactive power requirements [47]. This chapter will mostly deal with transmission side of the network.

Adaptive protection as already discussed in becoming increasingly relevant due to modern microprocessor-based relays and a realization from the utilities of its importance. The data storage capability by different agents in the system increases monitoring and subsequent automated actions. The next concept is automated setting correction that is a natural progression with the increase capabilities of the agents. The North American black out of 1965 is a prime example of obsolete relay settings and its widespread effects when a single line

perceived overload created a cascaded effect [48,49]. Periodic automated scans employing data mining is one the mechanisms that can identify and correct obsolete agent settings with notifications to protection team. In certain load conditions, the scheme itself will exhibit flaws that can be ratified rapidly for soft logic hence phasing out hard logic.

Differential protection philosophy that operates on the principle of evaluating instantaneous value differences has now limited limitation on time-sync due to availability of GPS. Other limitations in communication, CT mismatch and transformer ratios are not a consideration these days due to IED building features.

Other design considerations such as Transformer magnetization current, over excitation and instrument saturation are known concerns that makes the system less flexible but intelligent devices are increasingly incorporating features for situational management [50]. For example, these IEDs can scale CT mismatches, can ignore inrush values or detect different inrush value.

Although with security concerns, alternate mechanisms of power systems communication have increased the redundant possibilities in addition to conventional direct linked communication such as pilot wire, power line career, and microwave. Based on the employed scheme the alternate less secure means of communication are increasingly used as a backup channel.

Although higher data speed is available for power system still issues such as latency and security on the internet has limited its use as restricted backup communication while the intranet has increased the scope of differential protection from just transformer asset protection [51,52].

Time stamping has enabled wide area protection and even when using internet, the integrity of data/measurement can be checked via value comparison, for example an incorrect voltage value can be validated by phase angle [53]. Adaptive protection is relevant to most if not all sections of the network. Transmission line assets performance is governed by four basic electrical parameters that are also related to material attributes and physical design features in an AC system.

It is paramount to comprehend these parameters and associated characteristics as it relates to protection schemes such as distance protection and its reach. Although the consumer is unaware of backend system and broader network, much through goes into system design, operation and protection. Abnormal states can wreak havoc and for fast response time high

degree of automation is employed in system protection and control. Protection also has contingency in the form of main and backup.

Basic physics of the fault remains the same that is unintended flow of current, but the definitions or details may change based on assets involved [54]. The implication can also vary between different asset types and their utilization. The main intention after detection is isolation of faulty component and use of alternate asset for service if designed in the system. Protection schemes have come a long way from initial use of thermal to electro-mechanical components to solid state to intelligent devices. Although solid state relays provide various simplified opportunities, computerized relays or IEDs have opened an entire world of communication centric possibilities for commutation analysis [55].

The measurement circuit includes an instrument transformer and an analogue to digital time synchronized converter providing possibilities to implement communication-based protection philosophies.

4.2. Characteristics of microgrid

Energy sustainability policies are influencing increasing use of renewables that is challenging the traditional network structure [56]. Smaller renewable sources are by nature distributed and energy storage is increasingly becoming fragmented. Protection remains the main topic among other issues such as stability, power quality, energy management etc.

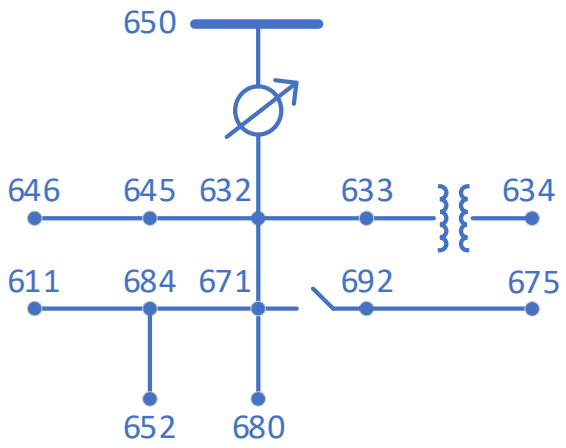


Figure 4.1 - IEEE-13 bus system

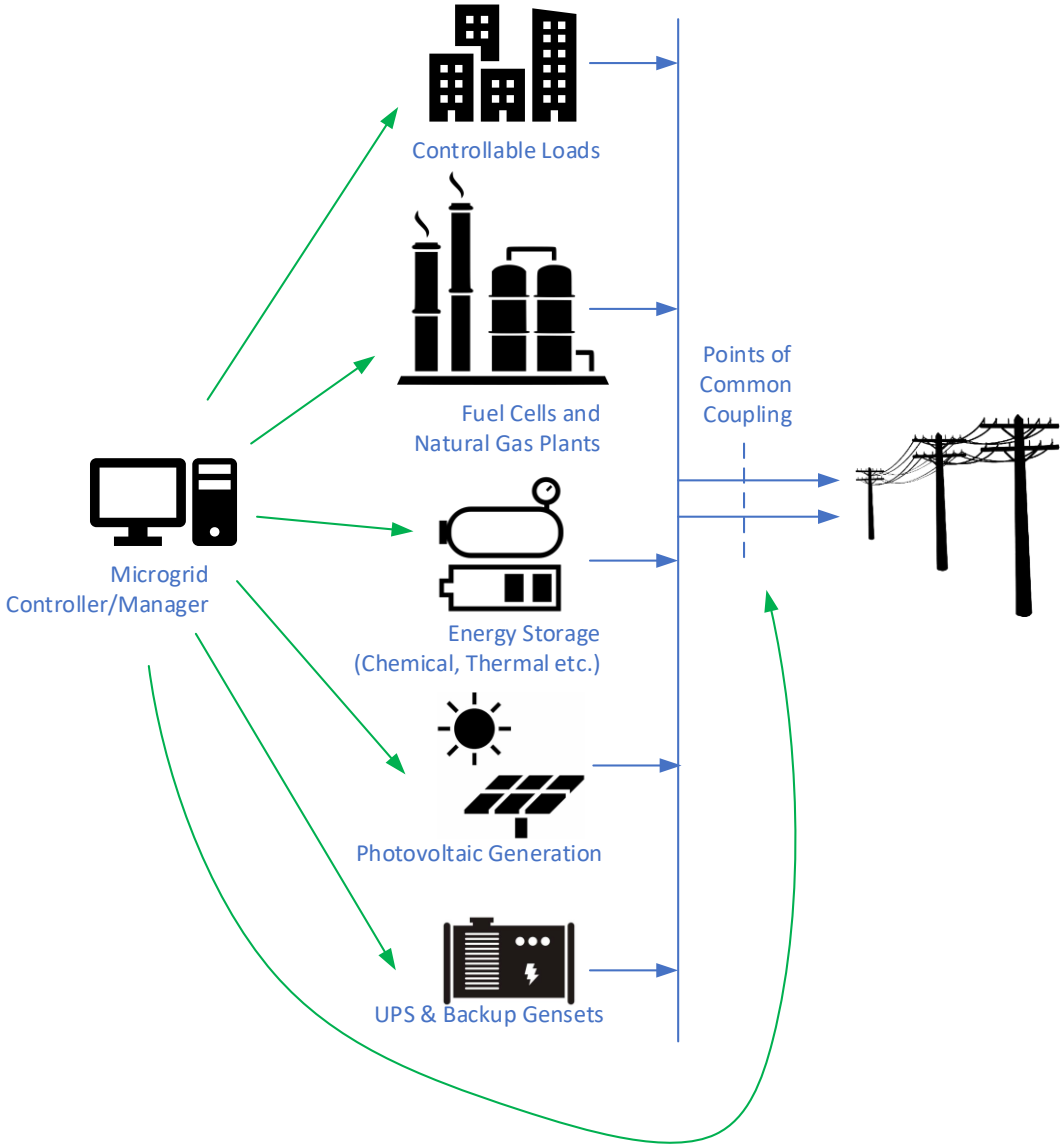


Figure 4.2 - Controllable elements of a micro-grid

This discussion will use 1992 Test Feeder Case of IEEE-13 (Shown in figure 4.1, 4.2, 4.3) Bus feeder modelled as micro-grid. The 13-bus system has a conversion of 480V to 4.18kV at the point of common coupling which is normally closed allowing two-way power transfer and lower fault current contribution from micro-grid (Intra-micro-grid power flow is also bidirectional facilitating distributed generation). The second mode of operation is islanding which in this case is limited to a fault scenario on the main grid and this mode operates in an adaptive system regime based on the availability of generation options.

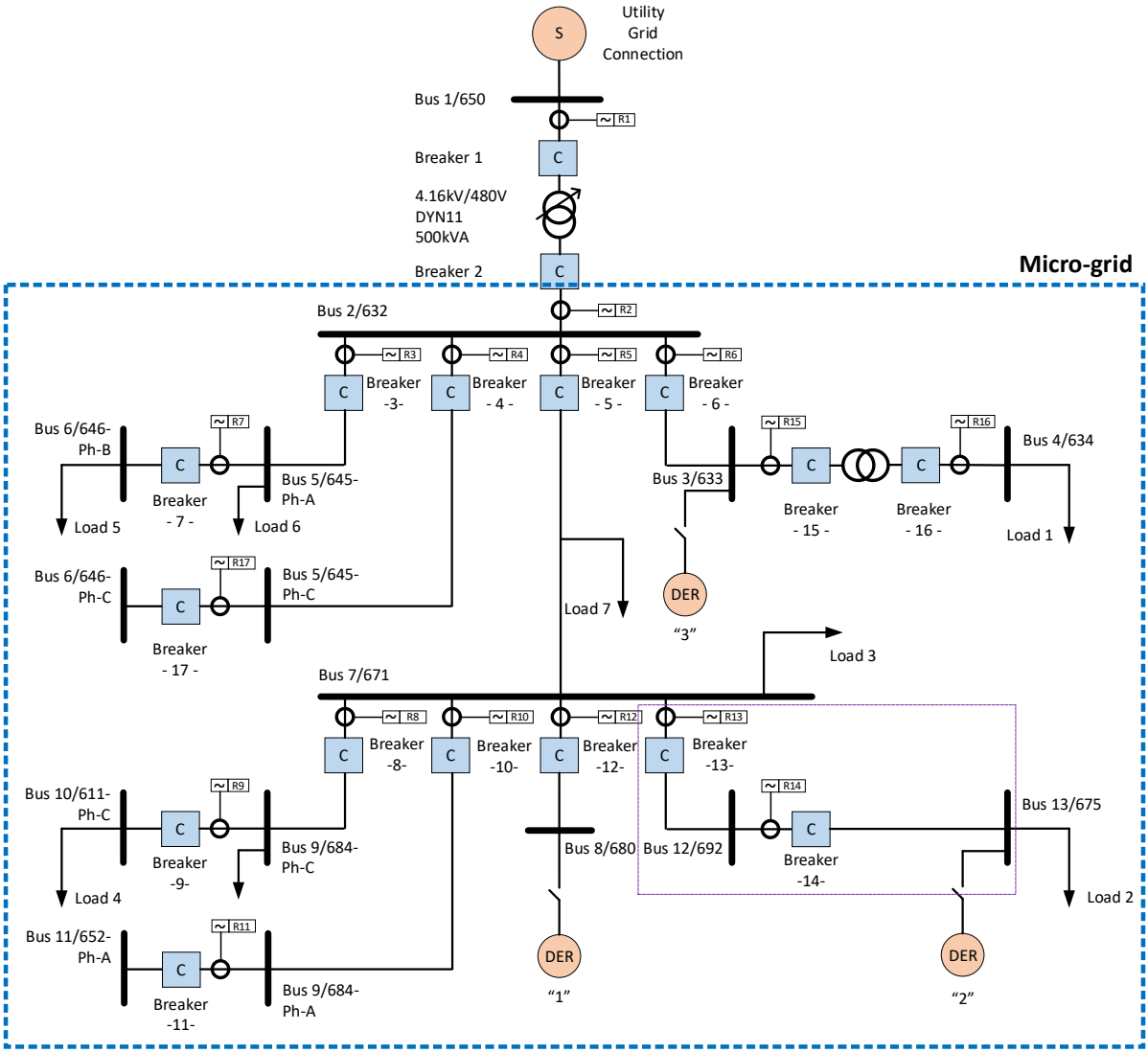


Figure 4.3 - Micro-grid based on IEEE-13

Micro-grid required specific protection philosophy that allows rapid isolation from utility faults, which ensures only the smallest subsection of the effected micro-grid section, is isolated and which allows for different settings for the two modes of operation. In the distribution context this in implemented while, using overcurrent protection that has limitations such as fixed settings and absence of directional element. Although there are many proposals in the market to use complex protection enabled by communication to circumvent these limitations, yet in this chapter I will be using overcurrent protection with IEC Standard 61850 to propose a micro-grid protection system. The locational and optimal advantage of DER placements is usually highlighted in the due diligence report.

Digital stakeholder requirement management in a smart grid setting can add value and optimize performance. IEC Standard 61850 can introduce new ways for DER management. IEC Standard 61850 can provide various benefits for transmission and distribution systems or specifically to utility installations. The main advantage is distributed automation for all protection and control agents facilitating automation, scalability and cost reductions. 5G based GOOSE messaging is the way forward in a power distributions system setting.

4.3. Protection behaviour and relevance of communication intensive system

One of the main attributes of current electrical power distribution system is the unidirectional flow of power and the same characteristic is reflected in the power system protection scheme [57]. The coordination and discrimination are structured according to upstream and downstream elements also shown in figure 4.4 and 4.5.

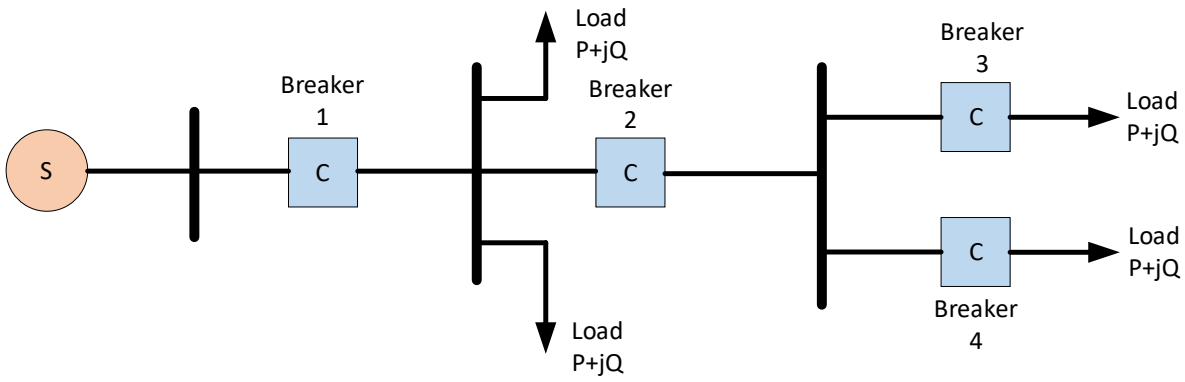


Figure 4.4 - Conventional power distribution system

Deregulation has paved way for DG which has changed the dynamics of network operation which include bidirectional power flow, decreased stress, and requirement of transmission system. The classification criteria of DG include the energy source, size/scale, and connection type [57,58,59,60].

Islanding in a deregulated energy environment can have implications on personal and system safety which has resulted in conservative measures for some operators. Although there are different protection settings for connected and islanded mode, still the operator must ensure if the DG complies system operating levels or there is an additional requirement for load sheading. In terms of protection considerations, the designer must consider the system parameters in both modes.

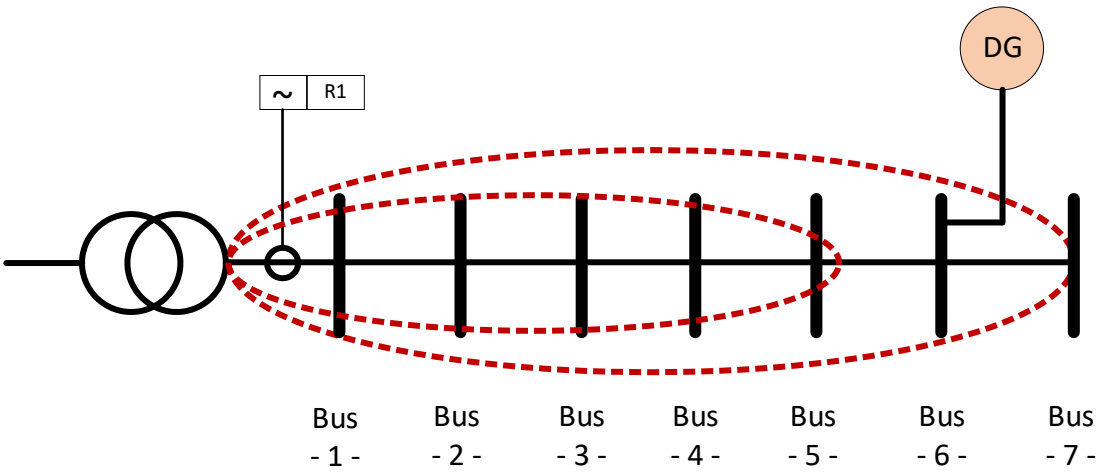


Figure 4.5 - Change in reach for two modes of operation

One of the most basic and low-cost protection devices is a fuse which has no instrumentation prerequisite. This device is based on its thermal characteristics because of which it has fixed value and single use per fault. A typical fuse characteristic curve is shown in figure 4.6

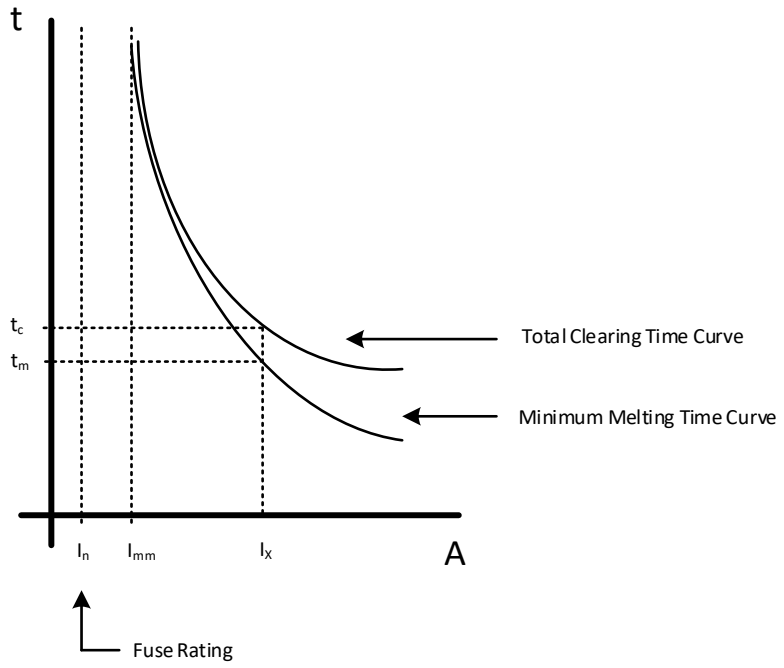


Figure 4.6 - Typical fuse characteristic curve

Usually beyond 0.6/1kV a protection relay or IED is required for circuit breaker control or protection operation and can be either unit or non-unit type. Differential protection principle is one of the options to protection a section by comparing the current of CTs and lacks the choice

to provide backup protection to adjacent section. Basic principle of differential protection is illustrated in figure 4.7.

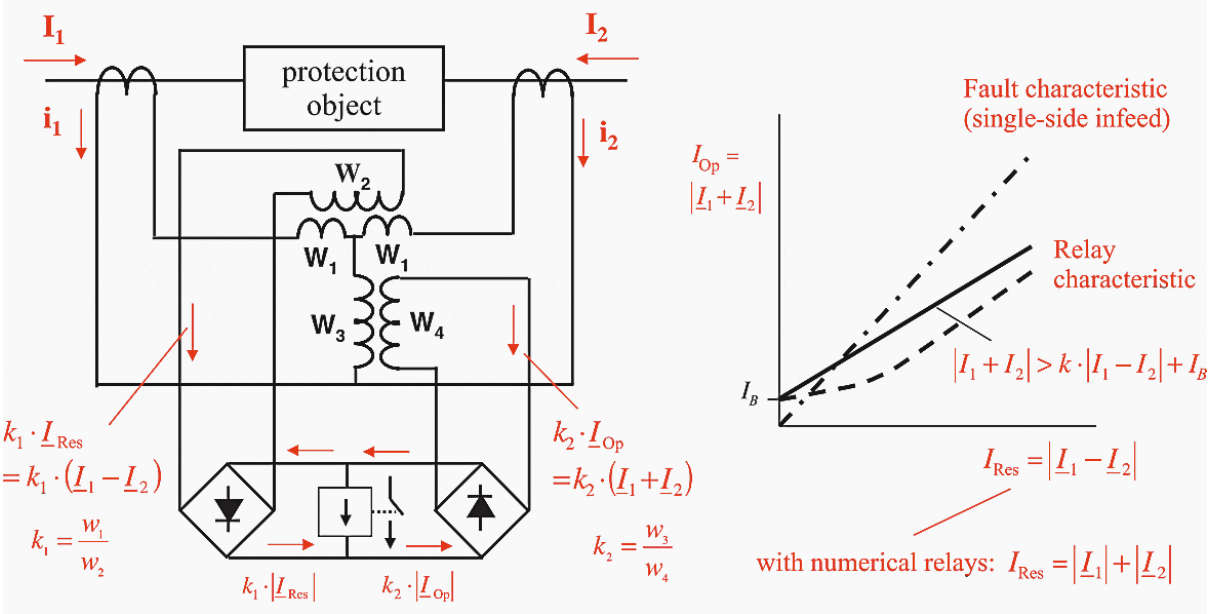


Figure 4.7 - Basic principle of differential protection

A line protection option is distance protection relying on apparent impedance ratios and the important device features is its Mho characteristics that has a possibility to over or under reach [61]. Overcurrent feature is the most basic, cost effective and widely used option in IEDs.

It is concluded form the protection review that the industry must move towards a communication intensive protection system developing the ICT systems along with the protection systems. The most prevalent protection system is the overcurrent protection and its offshoots, and the share number of these implementations requires an extensive yet secure communication network. “5G” communication systems are ideal for such application as they have higher immunity to EMC and related noise while providing large bandwidths and high data rates.

4.4. Analysing adaptive protection from the perspective of system stability

There is a constant effort to improve energy transport and protect key assets because electrical energy is the key aspect of modern living. One of the reasons it is of fault detection

and clearing of only the effected portion is of paramount importance is to maintain the network within its stability limit [62,63,64].

Distance protection is primarily used to protect and monitor transmission line assets whereas out of step protection is used primarily for generator assets in order to monitor for synchronization loss event which may happen due to an event on the power systems network [65]. With any such event there is also a possibility for generation units to face synchronization loss in relation to its peers. Which makes it logical to demarcate the whole system into regions or subsystems which can ensure stability while working together or in some events individually.

Unfortunately, even with these pre-emptive measures there have been some major events both locally and internationally such as 2016 South Australian blackout where protection IED operation in the third zone of distance protection covering the transmission line asset caused a major cascaded tripping event creating a wide area blackout effecting all spears of life.

It is proposed that an adaptive protection system for these asset and protection types be used that is:

- Adaptive distance protection for transmission assets
- Adaptive out of step projection for generator assets

With the ability to be adaptive the IED has a degree of situational awareness of the system and its operating state which gives this agent the ability to modify and calibrate its settings or parameters to suit the prevailing state or topology. It's a given that the device deceives its inputs from the wider system and in turn provide its status, condition and information related to its area of coverage to the wider system.

Keeping the above discussion in mind a new and improved distance protection is required and has been proposed. This is a merger of a Mho protection relay and a quadrilateral protection relay which is called a mushroom protection relay.

In addition to this a new measure is required to establish whether a post disturbance electrical power swing is unstable or within stability limits. Transmission line asset's distance protection holds high significance in the context of system countermeasures in the event of system disturbances and system faults. This makes distance protection a very common type of measure

around the world, but some limitations need to be addressed even if it provides excellent protection. Among other limitations an insufficient response is attributed towards the following critical limitations:

- Infeed effect during parallel line operations
- Limitations due to line load-ability

The protection scheme can benefit immensely from an adaptive distance protection IED because its settings can be managed and altered in line with the pre-fault and post-fault network conditions. This can be implemented with a merger of mho protection characteristics and quadrilateral protection characteristics to attain a mushroom form on a R/X plot. This new protection IED introduces greater reach yet has a reduced load-ability limitations. In the event of a major disturbance event, a generator can be out of step with load or suffer synchronization loss due to power imbalance between generation and load. In order to ensure supervision signals for distance protection, an out of step protection is necessary to alleviate the disturbance effects. For out of step identification for complex electrical power system, a novel R-X criterion is required. The proposed adaptive out of step protection will support in power swing identification with system monitoring and resulting adjustment in protection reach.

With the identification of an unstable power swing, the system control will separate the demarcated regional subsystems to maintain overall system stability while creating a regional balance between generation and load. Such an arrangement is well suited for regional Australia that already have a distributed generation and grid connectivity. It is proposed that the South Australian grid be operated with system and subsystem mindset that will enable the operator to disconnect and operate the subsystems individually in an instability event.

4.5. Improving power system reliability with adaptive protection techniques

Traditionally a protection relay and contemporarily an IED is an agent sending, measuring and comparing system values and issuing system commands. A protection agent has some key design considerations such as reliability (dependability/security) and selectivity. Dependability suggests on demand correct operation while security suggests no mal operation. Agent selectivity suggests operation for assigned areas and time [66,67].

Agent types discussed in this chapter are overcurrent (50/51), differential (87), directional (67), and distance (21). The simplest agent type is overcurrent with point current being the only

variable have the characteristic of inverse time variable and a fixed instantaneous characteristic portion with different applications. Differential agent type is used to cover major plant such as transformers generators and buses operating when the inflows and outflow difference between two or more gate points is more than the characteristic fault [68].

Automation and protection engineers will benefit from an automated creation of coordination tables as the amount of coordination requirements grows, resultantly staff can spend time on power system analysis rather than the laborious task of table creation. Utilization of engineering software for protection modelling and short circuit analysis can help the protection systems engineer to:

- Protection system coordination during and after faulty system state
- Simulation of diverse fault scenarios
- Simulation of different operational scenarios

Further, the protection systems engineers can sift out non-responsive protection system simulation cases via APSA (automated protection security assessment) which will allow them time and resources to identify hidden failures. They can also identify the causes of miss-coordination to address it in protection system settings or schematics. These fixes and redesigned portions can be validated by utilizing a power protection system coordination chart or by offline power system analysis.

Generation, utilization and availability landscape is evolving and so is the online protection systems which has a profound effect on electrical protection system speed, sensitivity and selectivity due to heightened dynamic implications. Simply put, this has a direct impact on electrical power system's responsiveness, security and dependability. This online electrical PSSA (Protection System Security Assessment) will have link with the following systems:

- In order to understand the operational and switched configurations of grid at current and future estimates the ADMS/EMS systems will have an interface.
- In order to understand the current arrangement and protection system's settings of protection elements the PAMS (Protection Asset Management System) will have an interface.

The aforementioned information is supplied via protection and network snapshots recurring update procedure within the agreed framework. In one of the reviewed projects an XML based

interface for protection and network snapshot was utilized. Further, these snapshots were utilized by automated tools to apprise the network reference model. The reviewed project workflows initiated from a reference network model and proceeded to appraise the network/protection snapshots to automatically produce PSA outcomes. It also indicated that the protection settings and system optimization should ideally be performed by an automatic adaptive protection system. Contractors have already utilized optimization routines for protection IED settings on projects. They have also demonstrated pilot adaptive rules for protection settings optimization of international projects which will become part of business rule engine. It should be noted that any adaptive protection rules will be selection by accredited protection systems engineer.

The adaptive optimization rules or routines are intended to fix the weaknesses in the subject protection system in order to avoid instances of uncleared fault or miss-coordination. A PSA check can validate and mitigate such weaknesses. Afterwards, the validated and optimized protection settings can be stored as optimized protection snapshot. Vendor specific and generic optimized protection settings are recorded in a protection repository. This will include IEDs with or without adaptive capabilities.

4.6. Performance proofing of the adaptive protection system

Due to some historic disruptions, power system protection is under inquiry for operational errors and verification/validation practices needs to be introduced to the power systems protection domain [69].

A V diagram representation of an automation project is shown in figure 4.8. Verification activity for power automation and protection scope will evaluate the quality of the protection and automation system as this will entail all the actions related to the attainment of high-quality power system while covering:

- Testing activities
- Inspection activities
- Design analysis activities
- Specification analysis activities

The main advantage of verification of the adaptive protection scope in the advanced stages of engineering and design there will be substantial reduction in the number of issues and defects

with which the engineers must contend with during testing or redesign. Verification of adaptive protection system or associated products at the early system or product development stage will facilitate the comprehension of the system or product in a more meaningful way creating value for the system user, operator and maintainer. This verification activity will also minimize the instance of adaptive protection system or project failure both in the software component and hardware topology. The main outcome of the verification cycle is the attainment of a system in accordance with the utility needs and existing system's requirements.

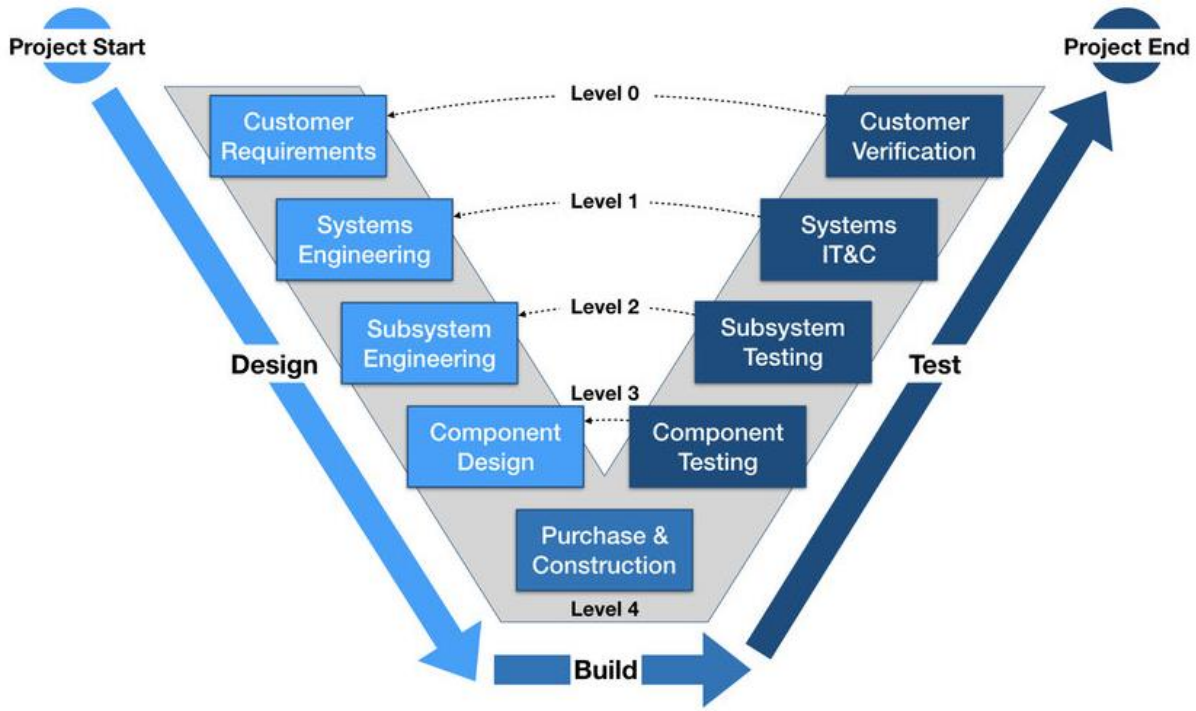


Figure 4.8 - V diagram representation of an automation project

Validation activities for power automation and protection scope will ensure that the adaptive system requirements are achieved by design and engineering outcome or application functionalities. System or product validation for adaptive protection will be done at the conclusion of the development cycle after the verification activities.

The central advantage of the adaptive protection verification activities is the capturing of failures that essentially are the shortcoming of the validation activities. In cases when there is misunderstanding of adaptive protection specification during the verification activities and resulting requirements have already been implemented then the gap between the delivered outcome and required outcome can be recognized though the validation activities in order to proceed with correction actions. Adaptive protection validation activities will usually include the following testing activities:

- System testing
- Load testing
- Stress testing
- Feature testing
- Compatibility testing
- Integration testing

Adaptive protection validation activities will facilitate the development of a fit for purpose system or desired product as per the industry or client requirements that eventually will satisfy the utility's business requirements.

The reason of divergence between verification and validation activities is mainly the intent of the requirement specifications. The validation activities for adaptive protection will ensure that the requirement specifications record the exact customer or system requirements whereas the verification activities for adaptive protection system will ensure that the final system/application/product meets the requirement specification.

Verification for adaptive protection system is completely an objective process as no engineering judgement or subjectivity is required to verify a system/application/product. Verification will include all the activities related with the attainment of a high-quality system. As discussed before, in opposition to verification, the validation process is highly subjective and requires much attention. It would require high attention to detail and subjective assessment to check if the resulting system will fulfil the actual requirement. Adaptive system validation activities will also include:

- User or system evaluation
- Concept and Prototyping
- Requirement modelling

4.7. Adaptive protection in context with inverter-based DER

This chapter discussed the effects of high inverter-based DER penetration and their mitigation with adaptive protection. Increased penetration of inverter-based DER has a negative effect on traditional protection [70]. Inverter based DER are unable to supply significant current during fault events that will cause:

- Overcurrent protection will be bypassed
- Fault could replicate the behaviour of inrush current or motor starting current
- Protection coordination is complicated by lower magnitude of fault which is susceptible to generation dispatch
- Inverter systems are unable to supply negative or zero sequence currents
- Subject to controls, the inverter systems have a variable transient response with no capability to provide inertia
- Inverter systems needs to be accounted for in the system analysis when its behaviour is that of a pre-fault state

It is essential to develop actual inverter system models for protection coordination, dynamic studies noting that the current limiter will define the steady state fault current, control actions will generate transients, and pre-fault state/system impedance/filter cap will define the initial fault spike. The main challenge during modelling is the product make and type differences. Hence, the best route towards inverter characterization is via testing.

With high PV penetration that is hundred percent inverter-based systems, the traditional protection design, simulation and modelling is not enough as following is required:

- Accurate short circuit models are required
- New electrical protection schemes are needed to handle faults

A holistic approach is required to address the challenges of micro-grid based distributed system design with increased inverter-based DER penetration that is demonstrable with inverters, IEDs and communication system.

4.8. Conclusion

It is concluded that lines distance protection and Generation out of step protection have coordination requirements during system design. Also, there are scenarios where system protection requirements cannot be satisfied with fixed or even variable settings and adaptability to system state is required to keep system stable. Different scenarios of micro-grid operation are evaluated for reliability in this section. The discussion also included international standards for micro-grid operation and operational implications on power system protection. The topic of DER penetration was explored from a different angle that is building from the physics of fault and implications of DER on those fault conditions with possible solutions by taking a

holistic approach to the combined AC and DC system. The solutions offered by adaptive protection were also discussed form the enabling technologies perspective.

It is found that Radial power distribution network is configured for a source such as zone substations but with increased DG, this has changed and so has the parameters of fault states. Variable DG availability, equivalent impedance and direction of current flow cannot be serviced by fixed setting. A communication based adaptive protection is suggested for distribution system both for islanded/connected system and for centralized/decentralized protection.

The impact of DG to system fault levels differs greatly with the technology used. In the matter of of directly linked synchronous machines the fault behaviour is well recognized; with synchronous machines providing greater fault quantities than the equivalent induction machines. The impact of inverter-based DG is the smallest due the ability of this equipment to demonstrate limited overload attributes. Still, the behaviour of this generation equipment under fault situations is defined by the used control methodology.

Conclusion and future scope of work

It is concluded that smart grids are represented as electrical power networks that employ digital technology to coordinate the needs and capabilities of various stakeholders for power delivery. It is also clear that Application of IEC Standard 61850 enabled adaptive protection and control techniques can increase reliability, add to self-healing features, and bring us closer to the realization of a smart grid. The study has explored the implementation of adaptive protection and control based on existing systems and IEC 61850 data model implementation as a communication standard.

Also, it is concluded that as the electrical power infrastructure has been developed and modernized in steps, so the current installations comprise of legacy components and new elements. The composite nature of protection and control system has added complexity to the adoption of adaptive protection. Any automation project must be managed with in the policies of the utility and the policies need to evolve in order to accommodate a smart infrastructure. It is stressed that a Substations design has a direct impact on the broader grid architecture where a smart substation will eventuate a smart grid, which in essence is adaptable to achieve an optimize state at any given time.

It is strongly advised that an optimized state of the grid can extract the maximum benefits out of the existing infrastructure and in the meanwhile, utilities can progressively add smart grid features to elevate the optimized state. It is understood that the main adaptable actions are in the domain of power systems control and power systems protection that have numerous overlaps and cross linkages. Adaptive control and adaptive protection cannot be realized without a modern information and communication system in place. It is suggested that in addition to the enabling technologies and technology enablers, a standardized approach is needed for which the industry is already moving in the that direction.

It is finally concluded that the IEC Standard 61850 facilitates the standardized approach in a substation context, and this has helped to realize the smart grid objectives on a substation level. Although the standard deals with issues on a micro level, still its alignment with the smart grid policy has helped deal with issues on a macro level. Future work will continue to cover the adaptable actions in context with the international standardized approached for current and future trends in power system configuration for transmission, distribution and generation with an intent of consolidation

References

[1] F. B. Costa, A. Monti, and S. C. Paiva, "Overcurrent protection in distribution systems with distributed generation based on the real-time boundary wavelet transform," IEEE Transactions on Power Delivery, vol. 32, no. 1, pp. 462-473, 2017.

[2] A. Rahmati and R. Adhami, "An accurate filtering technique to mitigate transient decaying DC offset," IEEE Transactions on Power Delivery, vol. 29, no. 2, pp. 966-968, 2014.

[3] N. I. Elkalashy, M. Lehtonen, H. A. Darwish, M. A. Izzularab, and I. T. Abdel-maksoud, "Modeling and experimental verification of high impedance arcing fault in medium voltage networks," IEEE Transactions on Dielectrics and Electrical Insulation, vol. 14, no. 2, 2007.

[4] W. Santos, F. Lopes, N. Brito, B. Souza, D. Fernandes Jr, and W. Neves, "High impedance fault detection and location based on electromagnetic transient analysis," in International Conference on Power Systems Transients (IPST2013) em Vancouver, Canadá, Julho 18, 2013, vol. 20.

[5] A. Sharaf and S. Abu-Azab, "A smart relaying scheme for high impedance faults in distribution and utilization networks," in Electrical and Computer Engineering, 2000 Canadian Conference on, 2000, vol. 2, pp. 740-744: IEEE.

[6] C.-L. Huang, H.-Y. Chu, and M.-T. Chen, "Algorithm comparison for high impedance fault detection based on staged fault test," IEEE transactions on power delivery, vol. 3, no. 4, pp. 1427-1435, 1988.

[7] I. Baqui, I. Zamora, J. Mazón, and G. Buigues, "High impedance fault detection methodology using wavelet transform and artificial neural networks," Electric Power Systems Research, vol. 81, no. 7, pp. 1325-1333, 2011.

[8] M.-R. Haghifam, A.-R. Sedighi, and O. Malik, "Development of a fuzzy inference system based on genetic algorithm for high-impedance fault detection," IEE Proceedings-Generation, Transmission and Distribution, vol. 153, no. 3, pp. 359-367, 2006.

[9] F. B. Costa, B. Souza, N. Brito, J. Silva, and W. Santos, "Real-time detection of transients induced by high-impedance faults based on the boundary wavelet transform," IEEE Transactions on Industry Applications, vol. 51, no. 6, pp. 5312-5323, 2015.

[10] T. Gammon and J. Matthews, "Instantaneous arcing-fault models developed for building system analysis," IEEE Transactions on Industry Applications, vol. 37, no. 1, pp. 197-203, 2001.

[11] M. Michalik, W. Rebizant, M. Lukowicz, S.-J. Lee, and S.-H. Kang, "High-impedance fault detection in distribution networks with use of wavelet-based algorithm," IEEE Transactions on Power Delivery, vol. 21, no. 4, pp. 1793-1802, 2006.

[12] M.-T. Yang, J.-C. Gu, J.-L. Guan, and C.-Y. Cheng, "Evaluation of algorithms for high impedance faults identification based on staged fault tests," in Power Engineering Society General Meeting, 2006. IEEE, 2006, p. 8 pp.: IEEE.

[13] H. Haeberlin and M. Real, "Arc detector for remote detection of dangerous arcs on the DC side of PV plants," in 22nd European Photovoltaic Solar Energy Conference, Milano, Italy, 2007, vol. 200.

[14] X. Yao, J. Wang, and D. L. Schweickart, "Review and recent developments in DC arc fault detection," in Power Modulator and High Voltage Conference (IPMHVC), 2016 IEEE International, 2016, pp. 467-472: IEEE.

[15] M. Baran and I. El-Markabi, "Adaptive over current protection for distribution feeders with distributed generators," in Power Systems Conference and Exposition, 2004. IEEE PES, pp. 715 – 719 vol.2, oct. 2004.

[16] D. Popovic and E. Boskov, "Advanced fault management as a part of smart grid solution," in SmartGrids for Distribution, 2008. IET-CIRED. CIRED Seminar, pp. 1 –4, June 2008.

[17] H. Shateri and S. Jamali, "Over-reaching factor for distance relay with mho characteristic," in Universities Power Engineering Conference, 2007. UPEC 2007. 42nd International, pp. 333 –337, sept. 2007.

[18] D. Yuan, N. Zhang, X. Dong, Z. Bo, and A. Klimek, "An adaptive noncommunication protection for distribution systems," in Universities Power Engineering Conference, 2007. UPEC 2007. 42nd International, pp. 257 –261, sept. 2007.

[19] S. Jang, J. Choi, J. Kim, and D. Choi, "An adaptive relaying for the protection of a wind farm interconnected with distribution networks," in Transmission and Distribution Conference and Exposition, 2003 IEEE PES, vol. 1, pp. 296 – 302 Vol.1, sept. 2003.

[20] G. Benmouyal, M. Meisinger, J. Burnworth, W. Elmore, K. Freirich, P. Kotos, P. Leblanc, P. Lerley, J. McConnell, J. Mizener, J. Pinto de Sa, R. Ramaswami, M. Sachdev, W. Strang, J.Waldron, S.Watansiriroch, and S. Zocholl, "IEEE standard inverse-time characteristic equations for overcurrent relays," Power Delivery, IEEE Transactions on, vol. 14, pp. 868 –872, jul 1999.

[21] T. Sidhu, L. Mital, and M. Sachdev, "A comprehensive analysis of an artificial neural-network-based fault direction discriminator," Power Delivery, IEEE Transactions on, vol. 19, pp. 1042 – 1048, july 2004.

[22] J. G. Priolkar and V. N. Sheth, "A Review on Protection Isssues in Microgrid," International Journal of Emerging Trends in Electrical and Electronics (IJETEE), vol. II, pp. 6-10, 2013.

[23] V. Ajjarapu, C. Christy, "The continuation power flow: a tool for steady state voltage stability analysis," IEEE Trans. Power Systems, vol.7, pp. 416-423, Feb. 1992.

[24] P. M. Anderson, B.K. LeReverend, "Industry experience with special protection schemes," IEEE Trans. Power Systems, vol. 11, iss.3, pp.1166-1179, 1996.

[25] B. Bozoki, et al., "The effects of GIC on protective relaying," IEEE Trans. Power Delivery, vol.11, iss.2, pp.725 -739, Apr. 1996.

[26] M. J. Damborg, M. Kim, J. Huang, S. S. Venkata, A. G. Phadke, "Adaptive protection as preventive and emergency control," Proceedings of IEEE Power Engineering Society 2000 Summer Meeting, vol. 2, pp. 1208 -1212, 2000.

[27] P. K. Dutta, P. B. Dutta Gupta, "Microprocessor-based UHS relaying for distance protection using advanced generation signal processing," IEEE Trans, on Power Delivery, vol. 7, no. 3, pp.1121-1128, 1992.

[28] D.S. Fitton, I P. Gardiner, "Advantages for power system operation using a neural network based adaptive single pole autoreclosure relay," IEE Colloquium on Artificial Intelligence Applications in Power Systems, pp. 4/1 -4/7, 1995.

[29] Q. Huang, Y. Li, B. Li, "A new adaptive autoreclosure scheme to distinguish transient faults from permanent faults," Proc. of PowerCon 2002, International Conference on Power System Technology, vol.2, pp. 671 -674, 2002.

[30] A.T. Johns, Y.H. Song, R.K. Aggarwal, "Study of turbine-generator torsional oscillations with particular reference to adaptive autoreclosure," Proc. of TENCON '93, IEEE Region 10 Conference on Computer, Communication, Control and Power Engineering, vol.5, pp. 133 - 136, 1993.

[31] G. Li, J. Yates, R. Doverspike, and W. Dongmei, "Experiments in Fast Restoration using GMPLS in Optical / Electronic Mesh Network," Optical Fiber Communication Conference and Exhibit, pp. PD34_1 -PD34_3,2001

[32] A.G. Phadke, S.H. Horowitz, and J.S. Thorp, "Anatomy of power system blackouts and preventive strategies by rational supervision and control of protection systems," ORNL Report, ORNL/Sub/89-SD630C/l, Jan. 1995

[33] R. Ramaswami, M.J. Damborg, and S.S. Venkata, "Coordination of directional overcurrent relays in transmission systems - a subsystem approach," IEEE Trans, on Power Delivery, vol. 5, no. 1, 1990.

[34] A. Sang-Pil, K. Chul-Hwan, R.K. Aggarwal, A.T. Johns, "An alternative approach to adaptive single pole auto-reclosing in high voltage transmission systems based on variable dead time control," IEEE Trans, on Power Delivery, vol. 16, no. 4, pp. 676-686, 2001.

[35] F. Wang, M.H.J. Bollen, "Quantifying the potential impacts of disturbances on power system protection," IEE Proc. of the Seventh International Conference on Developments in Power System Protection, pp. 262 -265,2001.

[36] Elkadeem, M. Alaam, and M. Azmy, “Reliability Improvement of Power Distribution Systems using Advanced Distribution Automation”, Renewable Energy and Sustainable Development, 3(1), pp.24-32, 2017

[37] C. Marnay, S. Chatzivasileiadis, C. Abbey, R. Iravani, G. Joos, P. Lombardi, P. Mancarella and J. von Appen. "Microgrid Evolution Roadmap", International Symposium on Smart Electric Distribution Systems and Technologies (EDST), 2015.

[38] N. Hatziargyriou, V. Kleftakis, V. Papaspiliotopoulos, G. Korres, " Adaptive Protection for Microgrids," presented at Power & Energy Society General Meeting, Boston, United States, July 17 -21, 2016.

[39] J. Weng, D. Liu, N. Luo, and X. Tang, “Distributed processing based fault location, isolation, and service restoration method for active distribution network,” Journal of Modern Power Systems and Clean Energy, vol. 3, no. 4, pp. 494–503, Jul. 2015.

[40] Mahat, P.; Zhe Chen; Bak-Jensen, B.; Bak, C.L., "A Simple Adaptive Overcurrent Protection of Distribution Systems with Distributed Generation," Smart Grid, IEEE Transactions on, vol.2, no.3, pp.428,437, Sept. 2011

[41] Uthitsunthorn, D.; Kulworawanichpong, T., "Adaptive OverCurrent Relay Coordination Based on Multi-Agent System”: A Case Study on Transmission Line Outage," Power and Energy Engineering Conference (APPEEC), 2012 Asia-Pacific, vol., no., pp.1,4, 27-29 March 2012.

[42] Luckett, R. G., Munday, P.J., and Murray, B.E., ‘Substation Based Computer for Control and Protection’, Developments in Power System Protection, IEE Conference Publication No. 125, London, March 1975.

[43] J. Codling, S. House, J. Joice, K. Labhart, J. Richards, J. Tenbusch, M. Tullis, T. Wilkerson, and N. Rostamkolai, “Adaptive relaying. A new direction in power system protection,” IEEE Potentials, vol. 15, no. 1, pp. 28–33, 1996.

[44] Horowitz, S H., Phadke, A.G., Throp, J.S., ‘Adaptive Transmission System Relaying’, IEEE Transaction on Power Delivery, Vo1.3, no.4, Oct.,1988, pp.1436-1445.

[45] Mathur A, Das B, Pant V. Fault analysis of unbalanced radial and meshed distribution system with inverter based distributed generation. Int J Electr Power Energy Syst 2017;8 5:164–77.

[46] Ma J, Wang X, Zhang Y, Yang Q, Phadke AG. A novel adaptive current protection scheme for distribution systems with distributed generation. Int J Electr Power Energy Syst 2012; 43:1460–6.

[47] Ozenir Dias, Maria Cristina Tavares. Comparison between traditional single-phase auto reclosing and adaptive technique based on harmonic content measurement. IET Gener. Transm. Distrib., 2017, Vol. 11, Iss. 4, pp. 905–914.

[48] H. H. Zeineldin, E. F. El-Saadany, and M. M. A. Salama, "Distributed Generation Micro-Grid Operation: Control and Protection," in Power Systems Conference: Advanced Metering, Protection, Control, Communication, and Distributed Resources, 2006. PS '06, 2006, pp. 105-111.

[49] P. Mahat, C. Zhe, B. Bak-Jensen, and C. L. Bak, "A Simple Adaptive Overcurrent Protection of Distribution Systems with Distributed Generation," Smart Grid, IEEE Transactions on, vol. 2, pp. 428-437, 2011.

[50] T. S. Ustun, C. Ozansoy, and A. Zayegh, "Modeling of a Centralized Microgrid Protection System and Distributed Energy Resources According to IEC 61850-7-420," Power Systems, IEEE Transactions on, vol. 27, pp. 1560-1567, 2012.

[51] M. A. Zamani, T. S. Sidhu, and A. Yazdani, "A communication-based strategy for protection of microgrids with looped configuration," Electric Power Systems Research, vol. 104, pp. 52-61, 2013.

[52] M. A. Haj-ahmed and M. S. Illindala, "The influence of inverter-based DGs and their controllers on distribution network protection," in Industry Applications Society Annual Meeting, 2013 IEEE, 2013, pp. 1-9.

[53] Maki K., Repo S., Jarventausta P., General Procedure of Protection Planning for Installation of Distributed Generation in Distribution Network. International Journal of Distributed Energy Resources, Vol. 2, No. 1, January-March 2006, pp. 1-23

[54] Seyed Amir Hosseini, Hossein Askarian Abyaneh, Seyed Hossein Hesamedin Sadeghi, Farzad Razavi, Adel Nasiri, “An overview of microgrid protection methods and the factors involved”, Renewable and Sustainable Energy Reviews 64 (2016) 174–186.

[55] W. Bower and M. Ropp, "Evaluation of islanding detection methods for photovoltaic utility interactive power systems," Sandia National Laboratories Photovoltaic Systems Research and Development2002.

[56] Kai-Hui Z, Ming-Chao X. Impacts of microgrid on protection of distribution networks and protection strategy of microgrid. In: Proceedings of international conference on advanced power system automation and protection (APAP); 2011. p. 356–359.

[57] S. H. Horowitz and A. G. Phadke, "Boosting Immunity To Blackouts," IEEE Power and Energy Magazine, vol. 1, no. 5, pp. 47- 53, Sept.-Oct. 2003.

[58] S. M. Brahma, “Use of wavelets for out of step blocking function of distance relays,” Proc. IEEE Power Engineering Society General Meeting, Montreal, QC, Canada, Jun. 2006.

[59] P. Nayak, J. Rao, P. Kundu, A. Pradhan, and P. Bajpai, "A Comparative Assessment Of Power Swing Detection Techniques," 2010 Joint International Conference Power Electronics, Drives and Energy Systems (PEDES) & 2010 Power India, pp. 1- 4, Dec. 2010.

[60] Mechraoui, and D. W. Thomas, “A New Principle For High Resistance Earth Fault Detection During Fast Power Swings For Distance Protection” IEEE Trans. Power Del., vol. 12, no. 4, pp. 1452-1457, Oct. 1997.

[61] IEEE Power System Relaying Committee (2002), Industry Experience with System Integrity Protection Schemes, Industrial survey on SIPS, System Protection

Subcommittee of IEEE PSRC of Power Eng. Soc. New York, 2002.

[62] Abdel-Majeed, A., Viereck, R., Oechsle, F., Braun, M., & Tenbohlen, S. (2011, September). Effects of distributed generators from renewable energy on the protection system in distribution networks. In Universities' Power Engineering Conference (UPEC), Proceedings of 2011 46th International (pp. 1-6). VDE.

[63] Yongfei, M., Chunlai, L., Yanjiao, H., Libin, Y., Shichang, Z., Xuan, W., ... & Jia, Y. (2016, November). Analysis of the Influence of Distributed Generation Access on the Operation and Management of Distribution Network. In Smart City and Systems Engineering (ICSCSE), International Conference on (pp. 194-196). IEEE.

[64] F. Z. Peng, Y. W. Li, and L. M. Tolbert, "Control and protection of power electronics interfaced distributed generation systems in a customer-driven microgrid," in Power & Energy Society General Meeting, 2009. PES'09. IEEE, 2009, pp. 1-8: IEEE.

[65] P. Basak, S. Chowdhury, S. H. nee Dey, and S. Chowdhury, "A literature review on integration of distributed energy resources in the perspective of control, protection and stability of microgrid," Renewable and Sustainable Energy Reviews, vol. 16, no. 8, pp. 5545-5556, 2012.

[66] G. Chen, D. Jiang, Z. Lu, and Z. Wu, "A new proposal for solid state fault current limiter and its control strategies," in Power Engineering Society General Meeting, 2004. IEEE, 2004, pp. 1468-1473: IEEE.

[67] S. Zocholl, J. Akamine, A. Hughes, M. Sachdev, L. Scharf, and H. Smith, "Computer representation of overcurrent relay characteristics: IEEE committee report," IEEE transactions on power Delivery, vol. 4, no. 3, pp. 1659-1667, 1989.

[68] G. Benmouyal et al., "IEEE standard inverse-time characteristic equations for overcurrent relays," IEEE Transactions on Power Delivery, vol. 14, no. 3, pp. 868-872, 1999.

[69] K. A. Wheeler, S. O. Faried, and M. Elsamahy, "Assessment of distributed generation influences on fuse-recloser protection systems in radial distribution networks," in Transmission and Distribution Conference and Exposition (T&D), 2016 IEEE/PES, 2016, pp. 1-5: IEEE.

[70] H. Yazdanpanahi, Y. W. Li, and W. Xu, "A new control strategy to mitigate the impact of inverter based DGs on protection system," IEEE Transactions on Smart grid, vol. 3, no. 3, pp. 1427-1436, 2012.

This page has been intentionally left blank.

Appendix A - Basics of power system communication leading to IEC 61850 Standard

A.1. Background

Digital communication is the basic component of IEC61850 based substation automation. Each data communication system requires a transmitter, medium and receiver. The data source such as a transmitter will convert the data into appropriate form that will travel via a communication link to a receiver that accepts and converts the signal to original form. In order, for the transmitter and receiver to be compatible, both should match in terms of signal type, logic definition, firmware, synchronization, rate of data exchange and error handling. These rules that specify the communication process are termed as protocols.

With use of an external clock, synchronous transmission can achieve high data exchange rate by transferring a dedicated clock signal or including the clock information in the communication to synchronize the transmitter and receiver clock. Greater block lengths can be transmitted due to this strategy. Whereas only low speed data transmittal and short block length is possible by asynchronous transmission.

A.2. System Topologies

A topology suggests the routing sequence that has a physical and a logical aspect. Bus and ring have both logical and physical connotations whereas star topology only has a physical meaning. Bus topology in its physical implementation has a single communication channel with each node having common message and logically a bus topology broadcasts the message. Some of the physical requirements of this topology include terminators and repeaters.

In a star topology, the system devices are connected to a central device that is called a hub. Ring topology physically is a closed loop of connected devices and logically data is transferred from the sender to the adjacent device that relays it to the next. The process is repeated until it reaches the destination that transfers the acknowledgement to the next device until it reached the sender, hence completing the loop. Each topology has its trade-offs, and the designer must select as per system requirements.

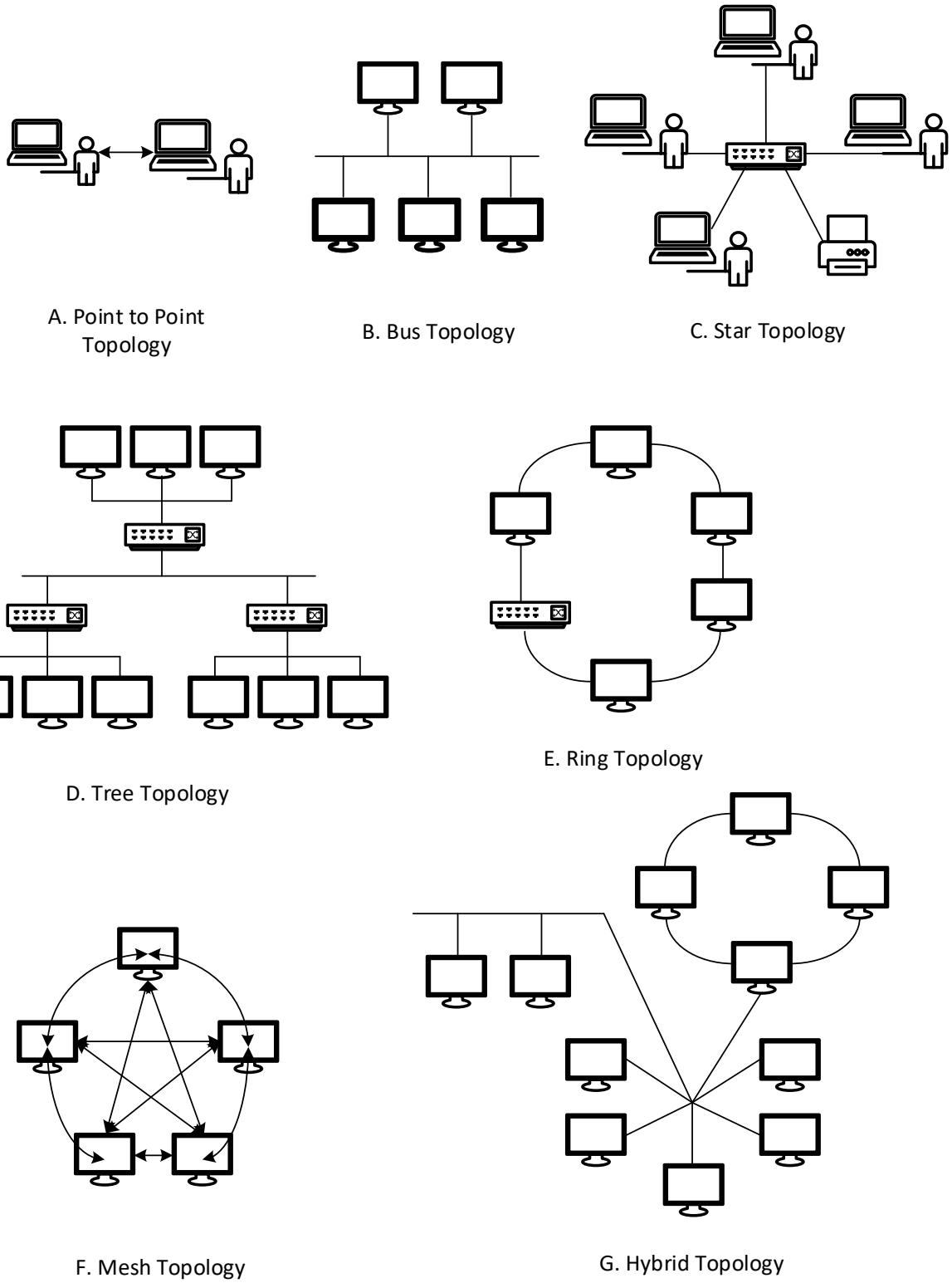


Figure A.1 - Physical and Virtual Network Topology

A.3. Communication methodology:

Building on the concept of topology, methodology is related to the communication permissions for individual devices, which is either Peer-to-Peer or Master Slave. In peer-to-

peer, method there is no central controller whereas in Master Slave method the central controller regulates all communication.

A.4. Access Rules:

Regulation of communication is critical for any communication to happen. In conventional or cyclic the master station initiates data transfer sequentially from slave stations and polling by exception is an additional technique used where data is transferred only if there is a change event. TDM (Time division multiplexing) allocates a time slot for each device to communicate whereas Token passing media access makes uses of a circulating token system giving opportunity to a device to transmit data when holding the token. In CSMA/CD (carrier sense multiple access with collision detection) a device only transmits data when the network is idle, and all the collision schemes are implemented on the device level.

This interrelated layered structure proposed by ISO provides broad and globally recognized structure for communication. The model consists of functionally exclusive layers, service dependent on adjacent layers and has awareness of only neighbouring layers. The model is presented in Table A.1 and stacking/de-stacking process is shown in Figure A.2.

Table A.1 - Summary of the OSI model

		Processes	Description
Layers	7	Application	Human interface services
	6	Presentation	Data validation and security services
	5	Session	Connection management services
	4	Transport	Data transmission services including protocol selection
	3	Network	Routing and data fragmentation/defragmentation services
	2	Data Link	Error handling and synchronization feature
	1	Physical	Provides mechanical and electrical parameters

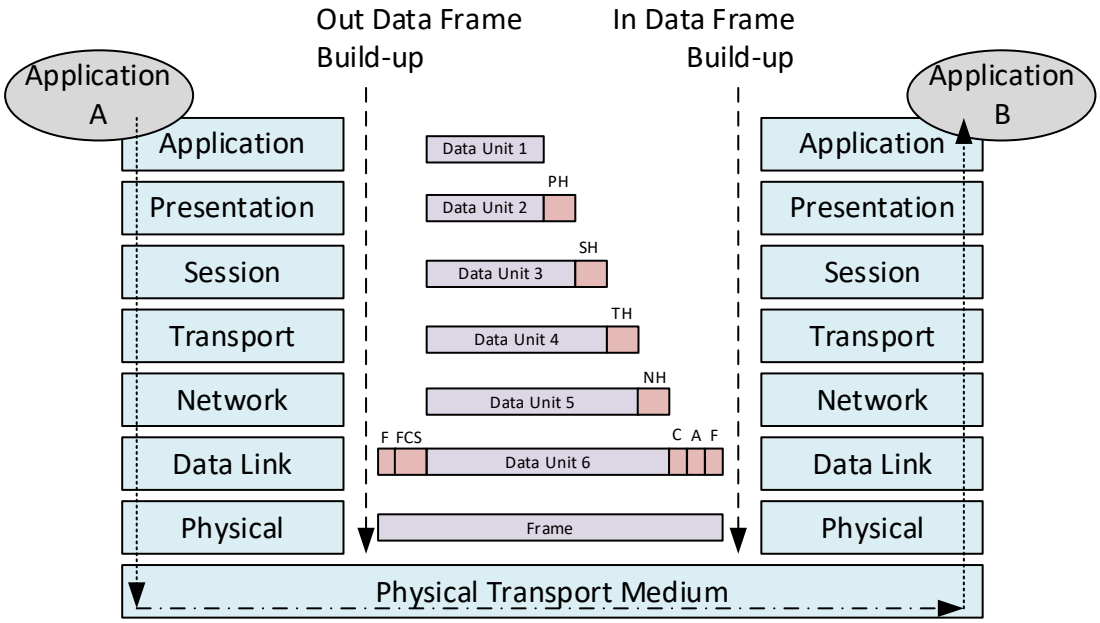


Figure A.2 - OSI stack related processes

The OSI stacking is a serial addition/modification process starting with data encoding at the presentation layer, session layer establishes the connection, transport layer regulates the transmission, network layer adds the routing information to the data, data link layer adds linking feature and physical layer ultimately performs the digital to analogy conversion. At the receiving end, the process in inversed and each layer strips/interprets the header or at physical layer performs analogue to digital conversion. The full model is only required for networks and for peer-to-peer communication only three layers are utilized. OSI model defines the structure, and the process is defined by different protocols of which some are widely implemented.

Table 4A.1 - Summary of existing protocols at electrical substations globally

S/No	Protocol	OSI stacks used	Speed	Access Control
First used by present day Schneider electric or its acquisition/merger				
1	FIP	1, 2, & 7	2.5 mbps	Time division multiplexing
2	Modbus	1, 2, & 7	19.2 kbps	Cyclic polling
3	Modbus Plus	1, 2, & 7	1 mbps	Token Passing
First used by present day Hitachi ABB or its acquisition				
4	SPA Bus	1, 2, & 7	19.2 kbps	Cyclic polling
5	MVB	1, 2, & 7 (Plus Pseudo Layer)	1.5 mbps	Time division multiplexing
6	LON	1 to 7	1.25 mbps	Pseudo carrier sense multiple access with collision detection

First used by present day GE or its acquisition/merger				
7	DNP 3.0	1, 2, & 7 (Plus Pseudo Layer)	19.2 kbps	Pseudo cyclic polling
8	UCA 2.0	1 to 7	10 mbps	Carrier sense multiple access with collision detection
First used by present day Siemens Energy or its acquisition/merger				
9	Profibus	1, 2, & 7	12 mbps	Token Passing
No specific early adaptors in the power sector vendors				
10	IEC Standard 60870 - 5	1, 2, & 7	19.2 kpbs	Cyclic polling
11	TCP / IP	1 to 7	10 mbps	Carrier sense multiple access with collision detection

A.5. Overview of DNP3 Protocol

DNP3 or Distributed Network Protocol version 3.0 is the most widely used protocol in the energy, water, and transport industry. This protocol uses three layers from OSI model and adds a fourth pseudo layer to provide complete functionality. The relationship between OSI stack and DNP3 stack is illustrated in the figure A.3.

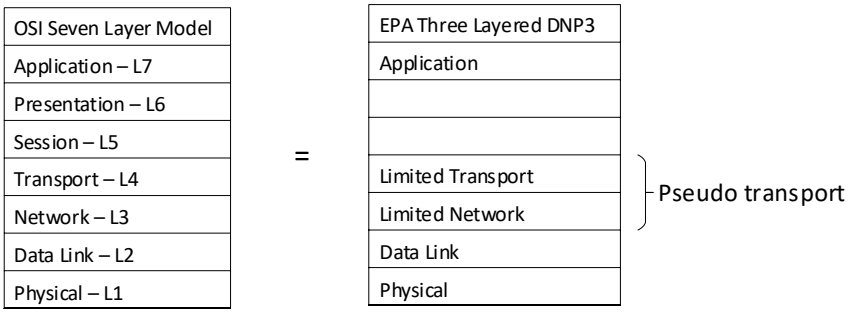


Figure A.3 - Comparison of OSI stack with DNP3

It is important to understand DNP3 as it is the most widely used protocol and is many cases needs conversion to the protocols used by IEC 61850. Background information is vital to understand the intent of various automation system concept. These systems have evolved from different applications and industries, but the future trend is towards uniformity or interoperability with the core aspect being remote control and analytics.

Data transmitted or received by DNP3 application layers originates from various applications and this data can be a status, event or up to a configuration file. Data is fragmented and converted to APDU (Application protocol data unit).

DNP3 message formation can summed in to following attributes starting from the application:

- Application functionality and commands are data independent
- Application layer groups the data in to an APDU with a size of 2048 bytes (max) which in turn is converted by a Pseudo Transport layer in TPDUs size of 250 (max).
- Followed by a conversion to LPDUs by Data link layer of size 292 bytes (max).

A.6. Networking and DNP3

DNP3 implementation in a generic network setting will consist of IP transport layer conversion of DNP3 datalink LPDUs instead of DNP3 physical layer with a recommendation to use Ethernet, switched of confirmations and use of TCP/UDP.

A.7. Applicable overview of IEC Standard 60870-5 and its protocols

The standard itself is produced by the same technical committee as 61850 and provides complete set of requirements for a SCADA system. The standard is applicable to wide area implementation. Associated standard section 103 provides information such as functionality and data type. Section 104 provides protocol mapping where section 103 and 104 are dependent on functional requirements section 101.

A.8. RTU (Remote Terminal Unit)

RTUs at its conception was intended as interface for field devices and SCADA providing data conversion. Local control provision was later available at the RTU level whereas previously a central mimic was used for control. These days all control functionalities can be implemented in a central RTU that increases substation wiring. Solutions become available with central and remote RTUs that transitioned in to remote RTUs communicating directly with SCADA. Remote or local RTUs are now labelled as bay controllers.

A.9. PLC (Programmable Logic Controllers)

As PLC is introduced for process control their main limitation is lack of communication capability with protection relays. PLC functionality is increasingly incorporated in protection relays.

Appendix B - Automation architecture for IEC 61850 standard deployment

B.1. Automation Architecture:

There are several automation architectures options with real world system implementation examples. The main difference between Substation Automation System (SAS) and Substation Control and Supervision Systems (SCS) is lack of intelligence at the bay level in the later. SCS usually include hardwired Input/Output's (I/O's) to a central RTU connected to SCADA.

A Substation/Power Automation System comprise of local intelligence and network connectivity to all elements that is applications/devices with a minimum one SCADA station. The limit of the automation system is up to the SCADA station and connected network (Intranet/Internet) is not part of the system.

The whole lifecycle objective of the substation is an important parameter to determine the architecture and plant considering that there is usually more development in the secondary equipment, with new devices introduced frequently. Moreover, secondary equipment has a shorter design life then primary equipment which can be 15/20 years as opposed to 40/50 years. Which means secondary devices and systems are maintained and replaced more frequently. There can a point after which system wide replacement is required because of cost and reliability concerns.

B.2. Requirement to automate brownfield sites

Change in market structure is creating new opportunities and to leverage on some of these opportunities a certain degree of automation is required which needs evaluation on case to case basis for brownfield sites and hence complete or partial upgrade maybe required. Automation requirement may also increase to comply with changing regulations in terms of quality or reliability. Information can give a competitive edge economically and it can be one of the reasons for substation automation. Another reason is to achieve a technical objective or solution to a technical problem is via automation. These solutions can be cover metering, communication, monitoring, protection, and control.

B.3. Basic structures involving substation automation

The basic structure and involved components for substation automation system are depicted in Figure B.1.

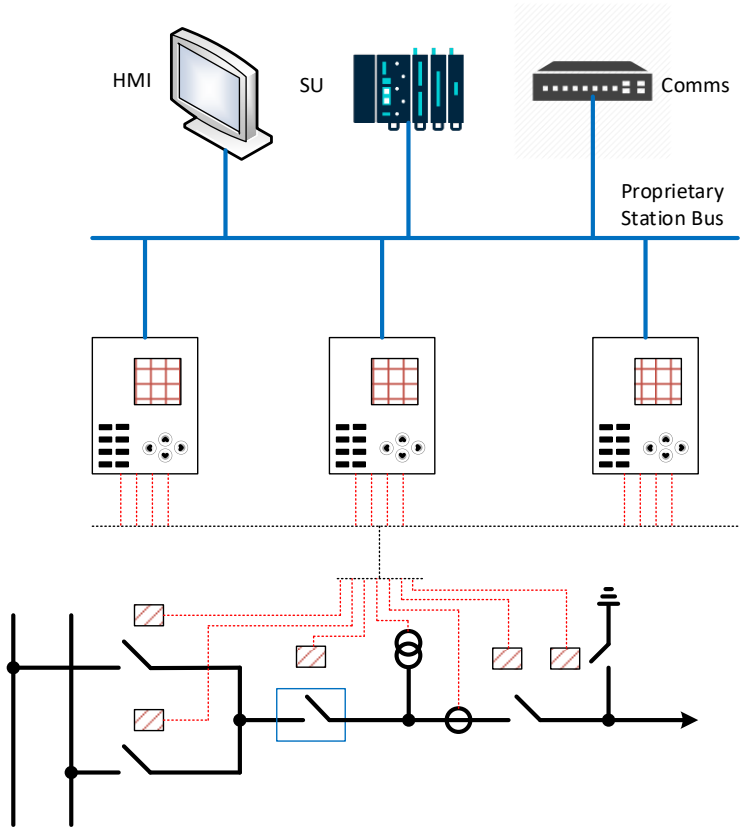


Figure B.1 - Substation automation specimen

Typical functions are grouped in table B.1. Similar station level functions exist which are usually in three categories of interlock, synchronization and data storage.

Table B.1 – Typical Functional Groups

Basic Control Functions	**Protection Functions**	**Higher Control Functions**
Circuit breaker Control	Busbar Protection	Sequenced Switching
Disconnector Control	Differential Protection	Automated Disconnection/isolation
Earthing Switch Control	Distance Protection	Autonomous bus change
Tap Changer Control	Overcurrent Protection	Smart reclosure
NCC Comms	Thermal Overload Protection	Load allocation – Line bays
Interlocks	Breaker Failure Protection	Smart load shedding
		Smart restoration

Some advanced equipment specific automation features can be implemented while adopting an improved architecture depicted in figure B.2. The features are listed in table B.2 and required use of IED and LAN connectivity across devices.

Table B.2 – Advanced Automaiton functionality

Equipment (Feeder Level)	**Equipment (Station Level)**
Feeder Protection Function	Remote Comm Function
Feeder Control Function	Feeder level Comm Function
Event Recorder Function	HMI for Station
Data Acquisition Function	Annunciation handling
	Status Monitoring
	Data analytics and storage
	Time Sync

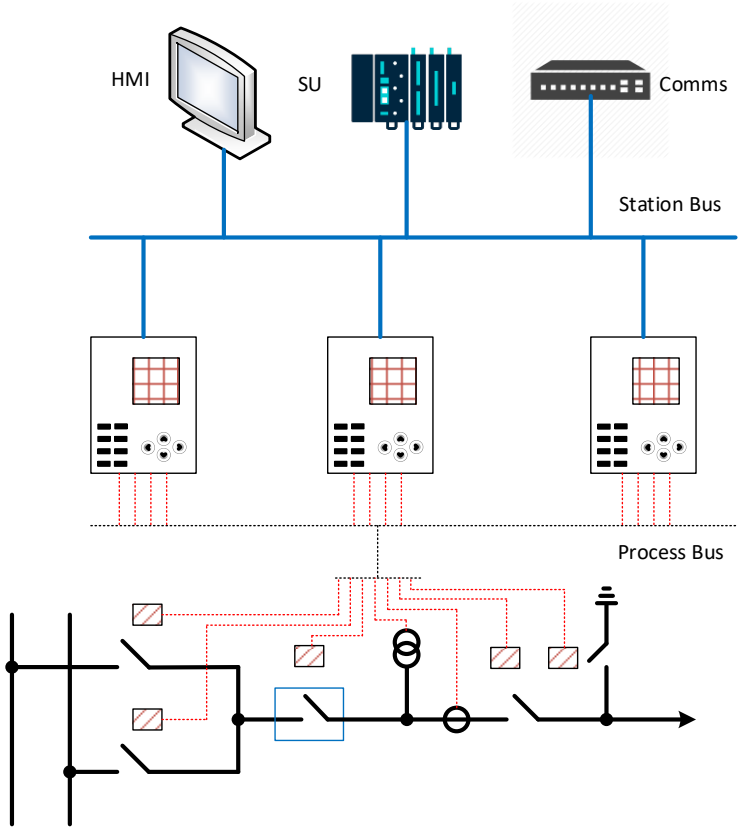


Figure B.2 - Substation Automation specimen (Advanced architecture)

Appendix C - Power system communication concepts leading to IEC61850

C.1. Basics of Communication Networks

Initially Ethernet was a radio link between universities campuses in Hawaii hence implied in the name. Later a consortium issued the version 1 and 2 of the Ethernet specification that was later standardized by IEE in the IEEE Standard 802-3. These days this standard is used in conjunction with other IEEE standards for performance optimization.

In power systems we still find various legacy systems having reminiscent of IEEE Standard 802 – 3 heritage connection technology enablers such as 10Base2/5/T/FL. Starting with IEEE Standard 802.3 – 10Base2 is a coaxial cable system. Another similar cabling system with a use of thicker fibre is 10base5 with similar speed but longer cabling span of 500meters where for thinner cable the span length was 185meter.

A 10BaseT utilizes a minimum of 24AWG CAT3 UTP Cable & RJ-45 Connectors for internode and hub connectivity via physical star topology, which logically is chained topology due to broadcasting. The transmit and receive pair has a length limitation of 100 meter. 10BaseT has been superseded by superior Gigabit Ethernet and Fast Ethernet. Another arrangement with three variations is a 10BaseFN-(FL/FP/FB) system employing wired hubs with an exemption that FL variant is point-to-point fibre connection up to ~2000meters.

Although obsolete yet present half-duplex ethernet has its unique design rules not relevant to new installations. It should be noted that determinism of an ethernet is dependent on both the system and the network. IEC Standard 61850-10 provides the breakdown of transmission time with only 20% allocation to latency.

The performance criteria are set on the transmission speed, bandwidth, signal to noise ratio, data throughput, error rate and response time. There is an additional relevant concept of virtual LAN which although may not be physically connected to different networks behave as if they are part of the same network.

Appendix D - Modelling an IEC 61850 Standard Environment

D.1. Modelling Concepts

Interoperability resides in the central benefits and expected outcome of IEC Standard 61850 adoption. The structure enables interoperability between all related functions that are implemented in or are part of different devices with various vendor-make options. This standard uses abstract models as opposed to concrete implementations with the possibility of virtualization that helps in analytics and communication with definitions limited to interoperability purposes. Functional decomposition of physical devices results logical nodes with the rational that data assignment is going to be on these nodes which are grouped for a device and called as logical device of virtual deposition. It is worthwhile to mention distributed functionality, which is a group of devices operating together towards a common functionality. The three virtual terminologies (Logical Device, Logical Node and Data Objects) discussed above are for actual data representation used for information exchange. This makes virtual information modelling independent of methodology and mechanism.

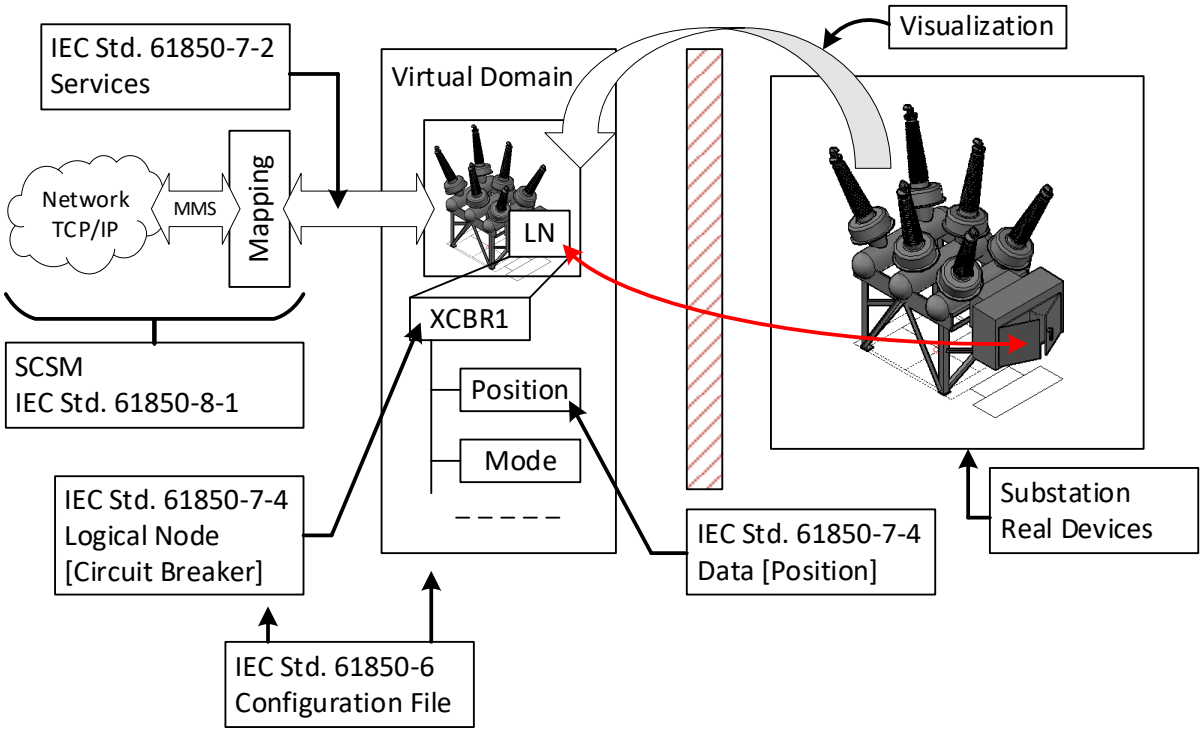


Figure D.1 - Mapping the virtual and actual environment

In the above figure D.1 a circuit breaker is modelled as a logical node from a bay that is a logical device and is represented as XCBR(N). Considering an IED (Intelligent Electronic Device) which as per the features contains a set of logical nodes, which in turn contains a data class, data set and data attributes. The underlying information is communicated a standard other than IEC Standard 61850.

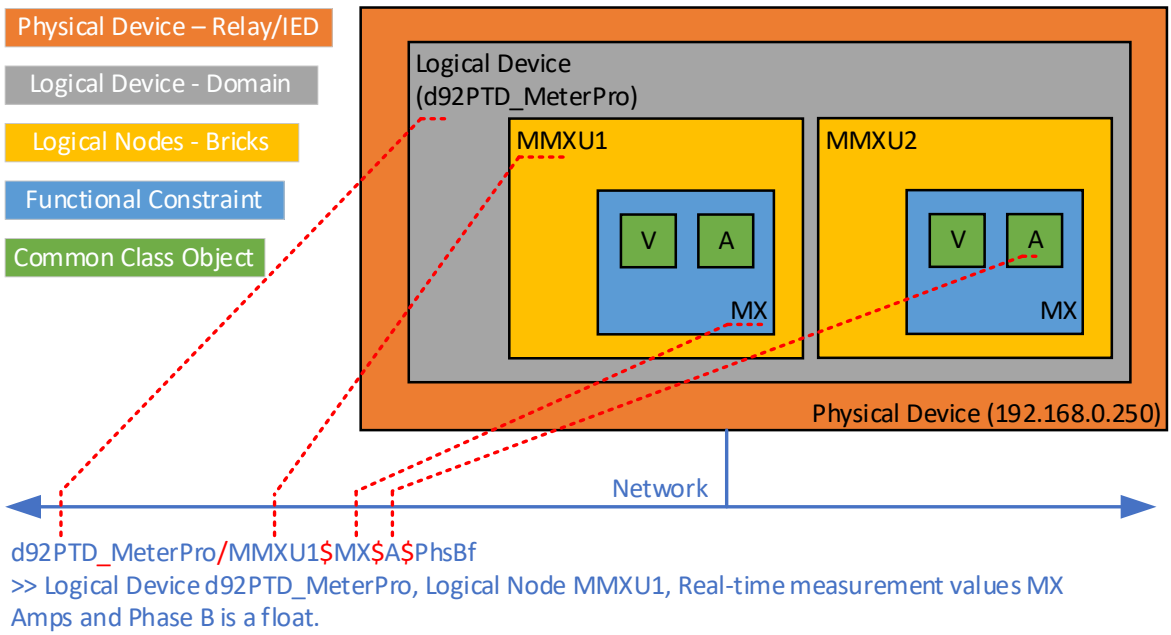


Figure D.2 - Physical and Virtual Containers.

The functionality centric approach in contrast with data standard centric method provisions interoperability due to flexible model. The access initiates with the network address leading to the aggregate virtual gateway elements such as logical device exploiting multiple functions called logical nodes. Each logical node may contain configuration information, analytics functions, control functions, and control group settings. Further decomposition leads to data nomenclature.

D.2. Information Exchange Model

The said model furnishes the details necessary to transfer data between client/server happening for control and monitoring. The model was developed keeping in mind the system physical topology giving allowance to visualize the physical object as an information object.

Appendix E - Tools and Testing norms for IEC 61850 based automation systems

E.1. Time synchronization for system operation

For the system elements to work in harmony while exchanging and interpreting information accurately, all local clocks should have minimum differences that can be in the order of less than a millisecond. This is achieved by time sync or synchronization.

Table E.1 - Application of classified time performance.

Time performance classification	Accuracy Tolerance	Application
T1	± 1 ms	Time stamping events like • Correlation of Lightning Strikes • Communication with IEDs • Disturbance/Event recorder data • SCADA Communication
T2	± 100 µs	Time tagged events like • Phasor • Travelling wave reflection location • POW switching
T3	± 25 µs	CT/VT Synchronization
T4	± 4 µs	CT/VT Synchronization
T5	± 1 µs	CT/VT Synchronization

E.2. Software application-based tools

Within IEC Standard 61850, PCM600 defines tools for IEDs which creates substation structures, communication services, functionality, LD & LN, IED Capabilities, user dataset definitions and control blocks. Resulting SCD file can be exported to CCT600 which as per IEC Standard 61850 defines system-based tools.

Appendix F - Implementing IEC 61850 Standard on Greenfield and Brownfield Installations

F.1. Migrating to current standards:

The main concern these days is the path to move from current system to a system based on IEC61850 Standard. Some Greenfield systems are already completely or partially adapting the IEC61850 Standard, but majority of assets can be labelled as legacy systems. Complete upgrade or rehabilitation projects thought to be straightforward can hold complexity of training and primary equipment with legacy standards. Most of the automation and communication system falls in three categories that is replacement, retrofit and extension.

Change here is usually called migration and migration strategy is depended on the substation control architecture that is either centralized or decentralized/ Decentralized PB. In a centralized control system, all control/monitoring is via central RTU hardwired to the processes whereas in decentralized control system, a station bus to connect HMI & Gateway. Decentralized PB has a process bus in addition to station bus hence least number of hardwiring requirements.

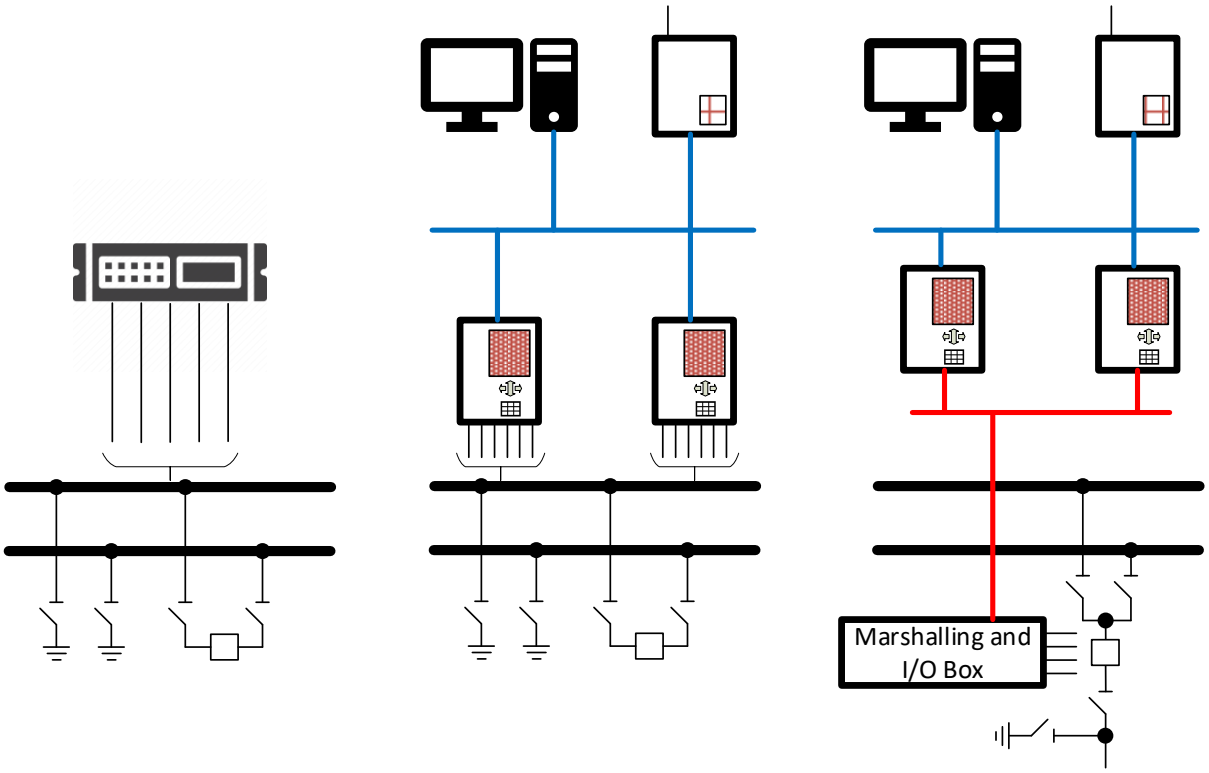


Figure F.1 - Three control system architecture examples

Funding can limit the extent of migration/change which is challenge as the product life cycle of secondary equipment and systems is shorter than primary equipment and systems. Obsolesce management can be a challenge during retrofitting. Typical protocol conversions scenarios for the three architecture types are listed in Table F.1.

Table F.1 - List of protocol conversion scenarios

	Decentralized Process bus		Decentralized		Centralized	
Station Level	Station Level IEC61850	Bay Level Proprietary	Station Level IEC61850	Bay Level Proprietary	N/A	
Bay Level	Bay Level IEC61850	Station Level Proprietary	Bay Level IEC61850	Station Level Proprietary	N/A	
	Bay Level IEC 81850	Process Level Hard Wired	Bay Level IEC 81850	Process Level Hard Wired		
Process Level	Process Level IEC61850	Bay Level Hard Wired	Process Level IEC61850	Bay Level Hard Wired	Process Level IEC61850	Bay Level Hard Wired

The migration process can start from or only effect bay, station, or process level. Failure or upgradation related replacement of bay level equipment such as IEC Standard 61850 compliant bay control unit would create data conversion requirement to both other levels. If we approach migration from a route starting from process level, then there is a possibility of retrofit or an extension case. A retrofit case will result in replacement of instrument transformers to smart sensors and associated process bus interface only. In extension only the new bays will get smart sensors while keeping all else like other bays, but the new bays will have 61850 process bus interfaces only and bay level will be same as legacy installation. Both cases will require configuration work for communication between process and bay level. The third approach to initiate migration from station level that involves reconnection/configuration or adding a series gateway.

While migrating the user needs to understand the benefits of IEC Standard 61850 in order to capitalize the investment. These benefits include simplifying spare stock and procurement by cost reduction (Installation, commissioning, instrumentation, wiring, change/migration, retrofit, extension, integration, and enhancement). Some motivations for modern IED adaption with IEC Standard 61850 capabilities is obsolescence, end of life cycle high running cost,

failure rate, new operational scenarios, early warning/self- check features in modern relays, multi-functionality as opposed to limited features, and better situational awareness. Modernizing the automation and protection system can happen in progressive steps or a complete overhaul but the predominant strategy in the industry is progressive upgrade. Progressive refurbishment can cause issues like increased complexity in terms of operations and maintenance due to the presence of a variety of components including obsolete elements. Modernization also changes the competence requirement for staff due to multifunction and communication centric devices that puts demand on personal to attain multidisciplinary skills while maintaining old skills for legacy systems/devices.

Any project involving power system automation scope has to deals with existing protection system. The protection philosophy will be dictated by existing system, present/future requirements presented in the proposal, and operators overall protection/control philosophy. Power automation system is inherently has integrated analytics, metering, control and protection functions. This calls for holistic strategy decisions and requirement engineering.

The Electromechanical, Static Electronic, Numerical and First Gen Digital Relays have no or limited communication capability that provides a strong case to replace these relays as part of a substation power systems automation project. Second Gen Digital Relays needs to be assessed on case-to-case basis but usually are replaced because of ongoing maintenance costs. Any implementation is usually staged as power system automation projects can be program of work rather than one of project. Single sourced suppliers are usually avoided although they provide reduced human resources and system integration costs. Multi-vendor approach provides a negotiation advantage, reduces organizational risk and augments the company's competencies that is possible due to different interoperability international standards that vendors are complying with, due to market demand.

There is a current trend in North America to present the system information on a secure web portal providing different functions-based security policy that can be monitoring the systems state, viewing event record, read data/meta data, and operate devices. The use of internet is restrictive cause of security, data integrity and time lag for which different enabling technologies are introduced each year.

There is no thumb rule for electrical power systems automation because it depends on user requirements including existing system setup. System design instead of focusing on the

technology limitations should use the functional/technical requirements as the basis that can hold future provisions.

F.2. Review of vendor Products

The main vendors for automation products and systems are SEL, GE, ABB (ABB Hitachi), Siemens (Siemens energy) and Alstom (GE Alstom).

F.3. Vendor 1 - GE (General Electric)

The system solution offered by this vendor is labelled as the Universal Family of devices where the vendor uses the term relay and IED interchangeably. This family of relays/IEDs offer seven product lines with varying protection features.

Each relay in this family of products incorporates a local and remote-control functionality and the devices are programmable via logical equations.

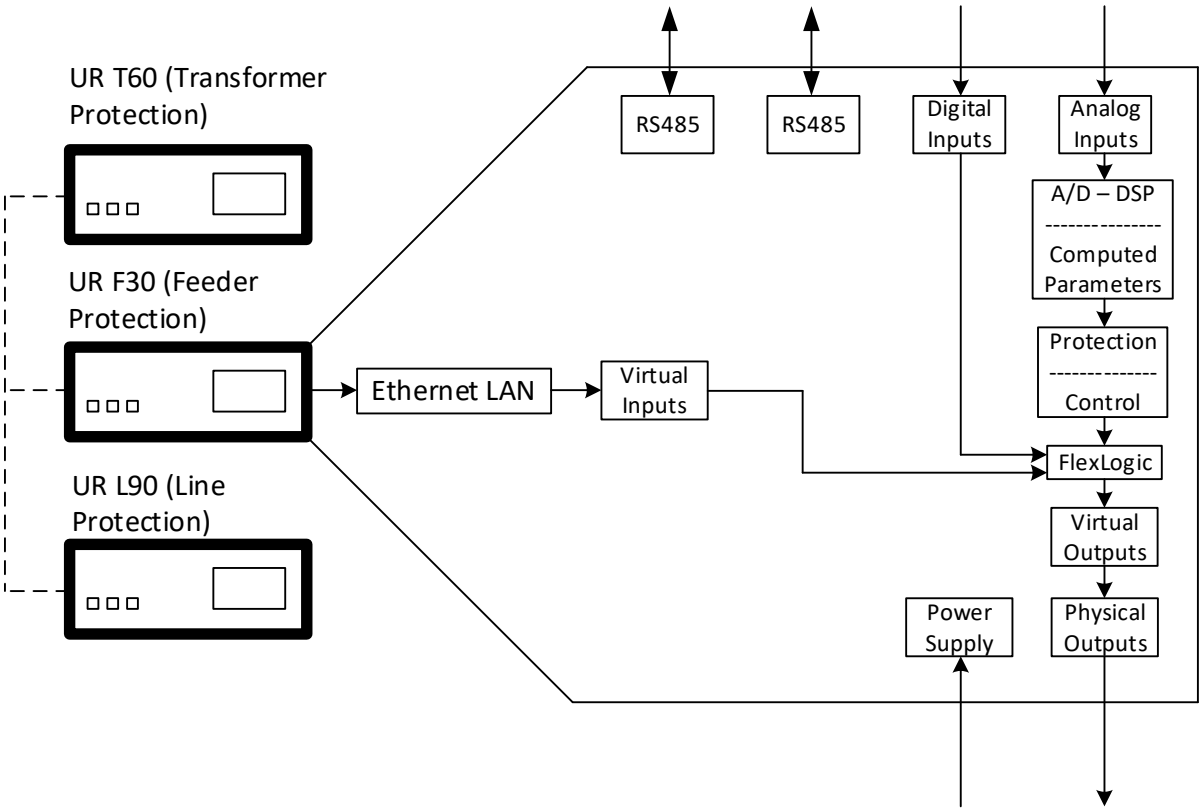


Figure F.2 – Typical configurational architectture offered by GE for UR family

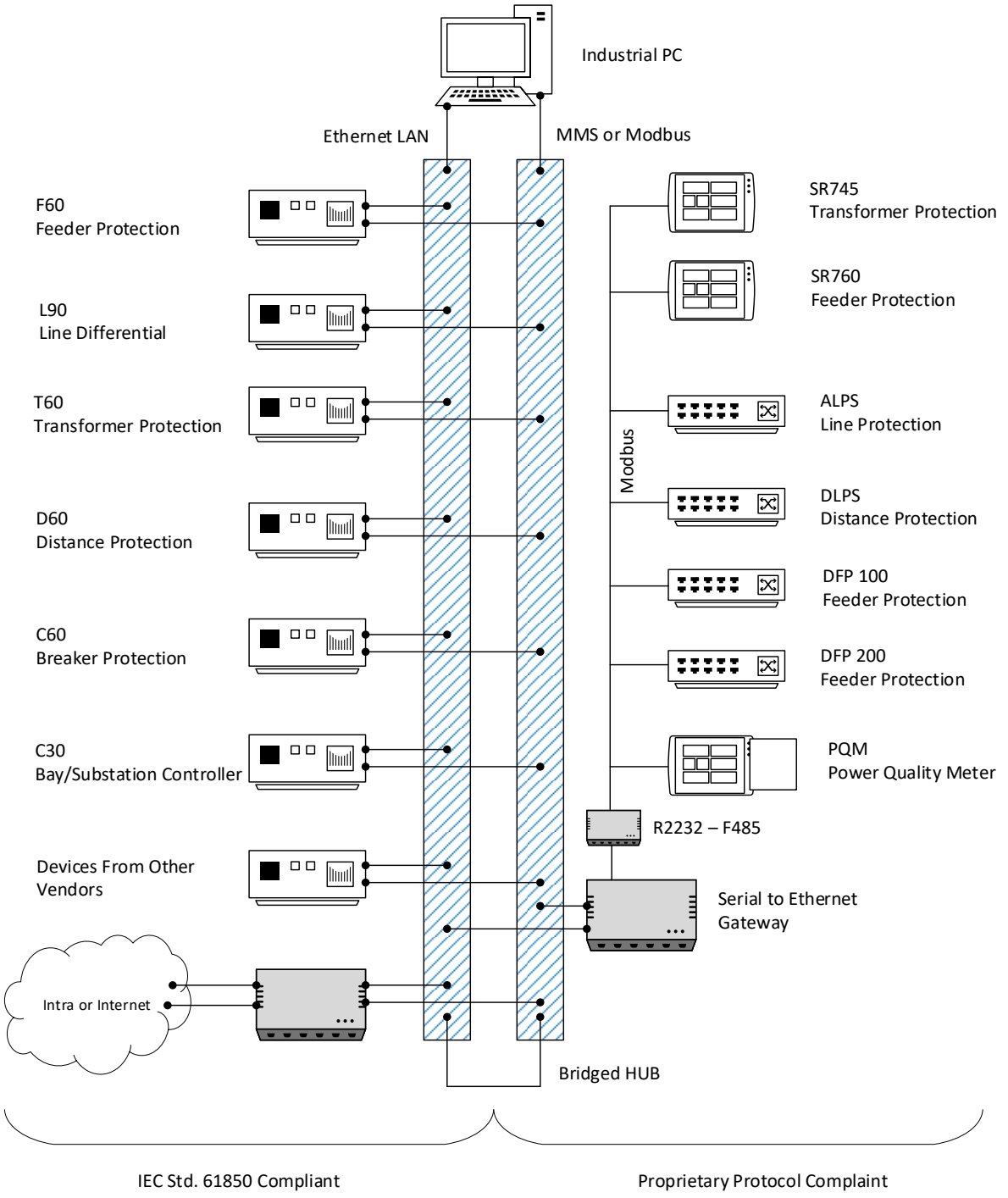


Figure F.3 – Typical Architechtural solution offering of GE

The vendor also has a hard-fibre system as per IEC Standard 61850 process bus with mapping allowance of measurements to IEDs with secure comms.

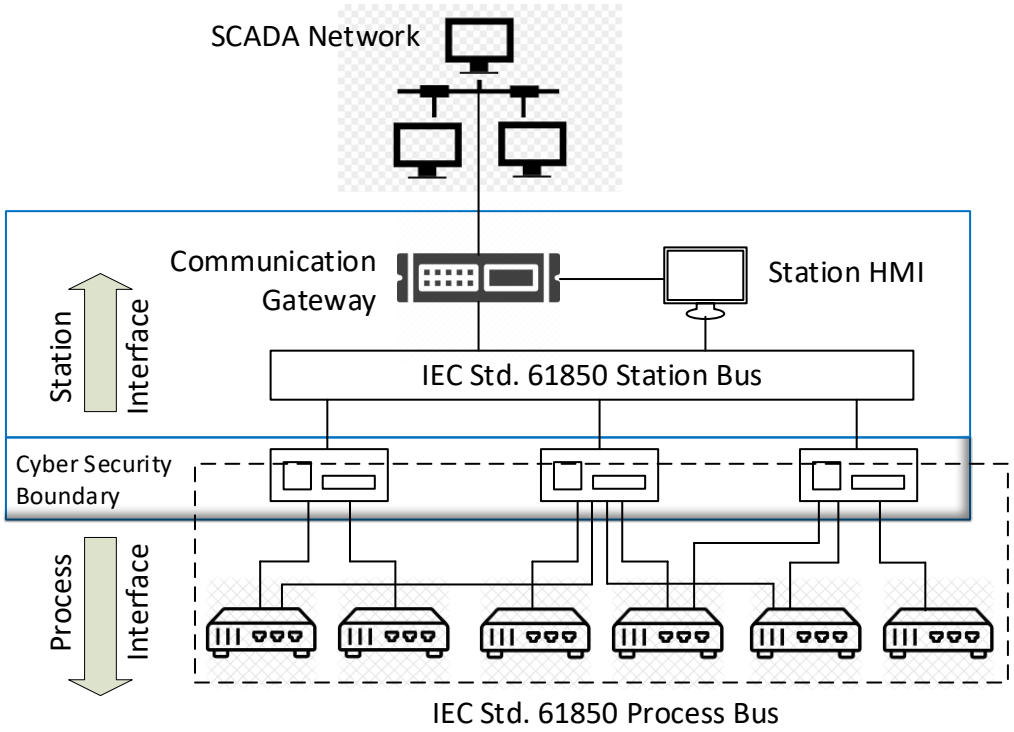


Figure F.4 – Hard fiber archtecture offered as part of Multilin series

F.4. Vendor 2 – Hitachi ABB

Previously ABB, now Hitachi Energy or Hitachi ABB offers substation automation products in two product lines that is type 1 and type 2. Type 1 system offering comes under the umbrella of well-known REF series of relays.

F.5. Vendor 3 – SEL

SEL is a vendor of choice for most utilities because of their type 3 offerings of IEDs with advanced communication capabilities. SEL IEDs comes with a card-based communication processor of 2030 or 2020 series.

SEL protection covers almost every application and feature for protection, control, metering, monitoring and associated data communication. SEL itself has no SCADA software application and makes use of offerings from other vendors. SEL has limitations in star network topology which may require a communication processor and additional nodes requires new point to point cabling.

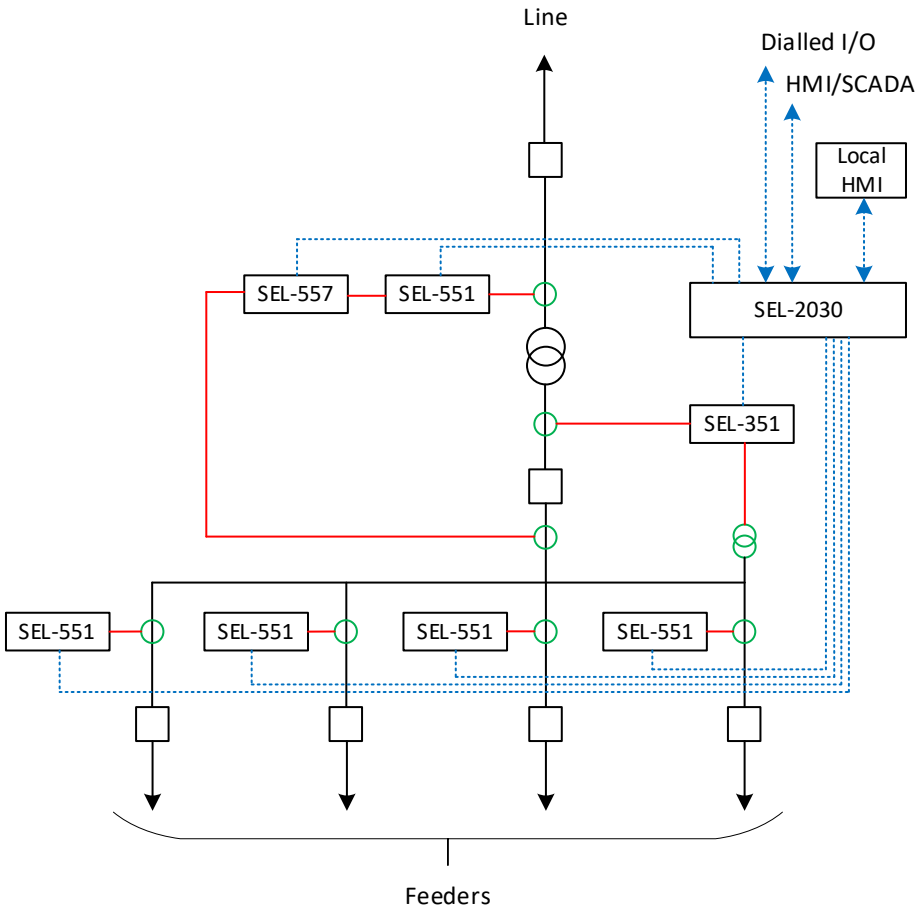


Figure F.5 – SEL implementation example

F.6. Vendor 3 – Siemens

Siemens or Siemens Energy has two series of which the legacy series is SINAUT-LSA and the contemporary product series is SICAM (PCC/SAS/RTU). The approach is very modular with protection functionality focus with limited integrated functionality.

The series 7 applies to high and medium voltage solutions which was previously labelled as numerical relays. These relay usually don't have a control, metering and monitoring functionality. The SINAUT falls under the category of substation protection and control systems rather than power automation systems.

The company also offers devices and systems for station control, remote terminal unit, I/O unit, bay control unit, and SCADA. The SICAM line fully compatible with IEC Standard 61850 for station and process bus.

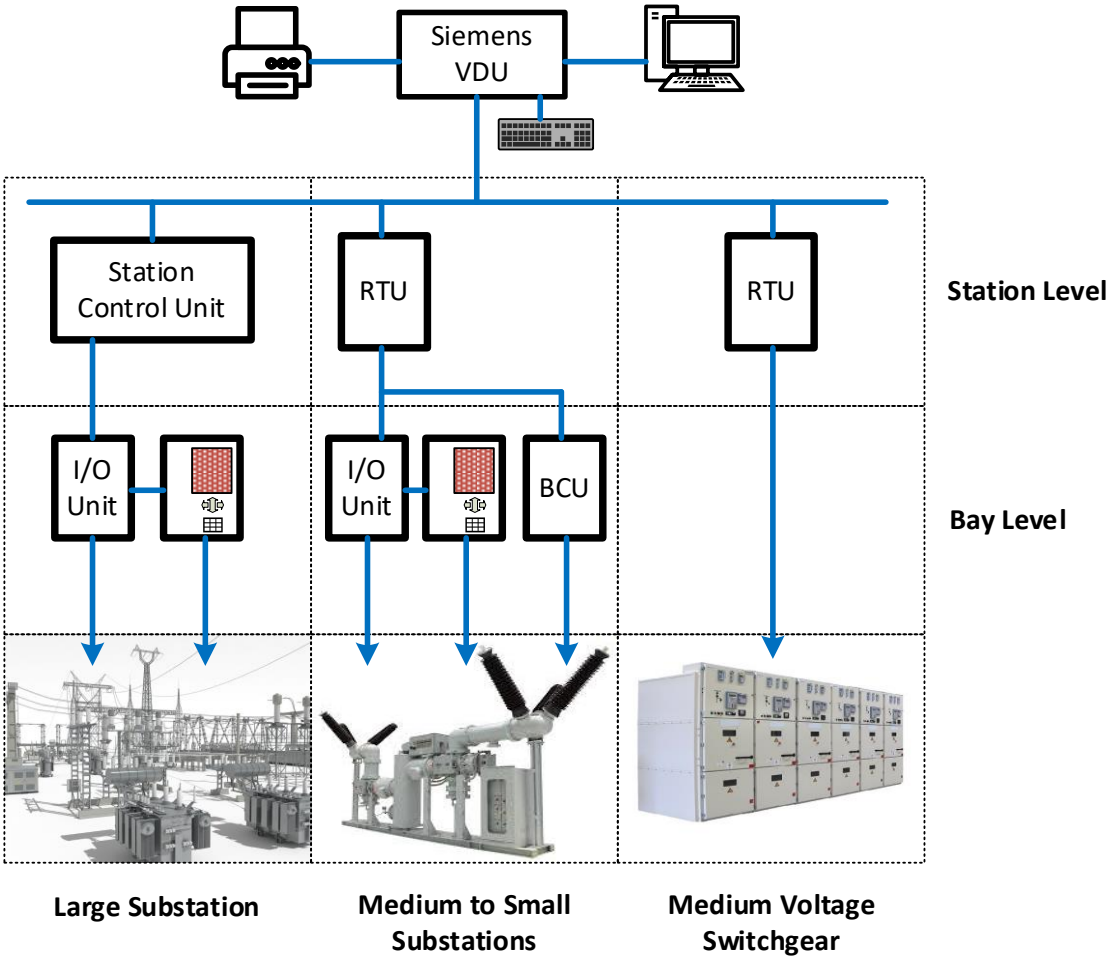


Figure F.6 – Typical architecture for Siemens SINAUT-LSA offering

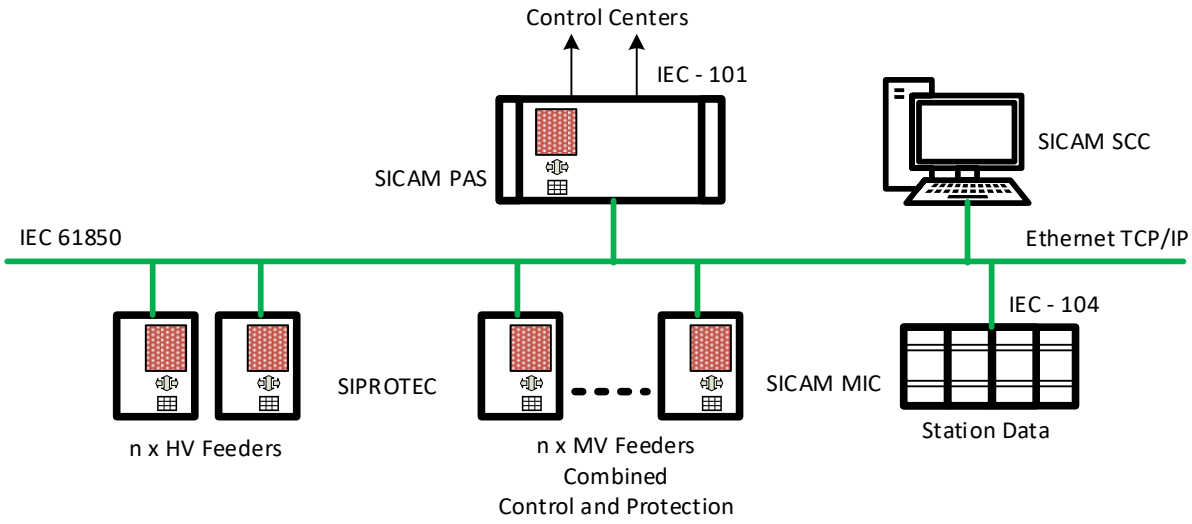


Figure F.7 - Typical architecture for Siemens SICAM offering

F.7. SAS (Substation Automation System)

Previously Alstom Grid and now GE Alstom offers AC/DC substation's digital control systems with the portfolio name of DS Agile. This product offering is IEC Standard 61850 compatible, capable of wide area implementation and conditional monitoring using PRP (Parallel Redundant Protocol) for smart grid functions.

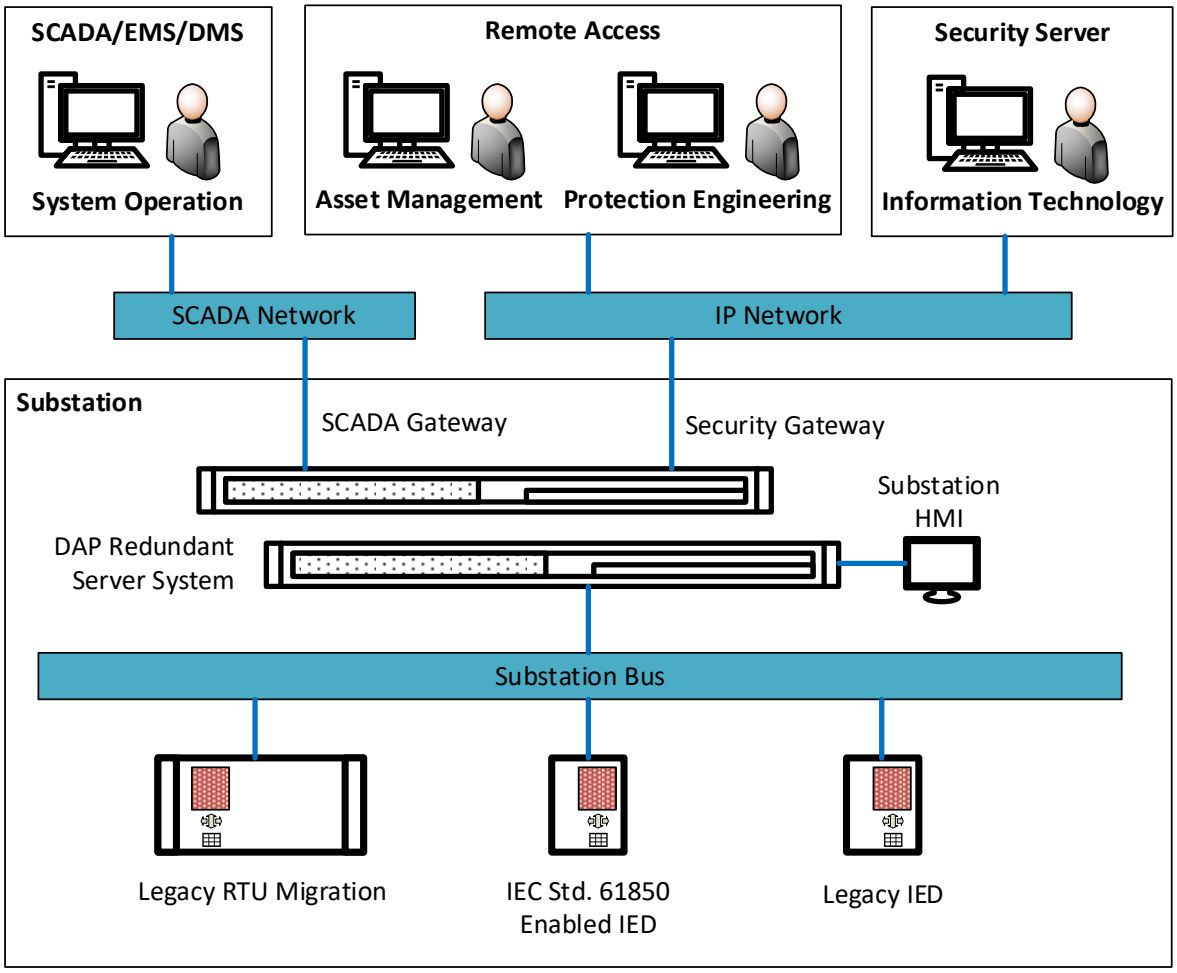


Figure F.8 – Typical architecture for GE-ALSTOM DAP Server System

F.8. DER (Wind Turbine) Object Model

The control and monitoring of wind turbine assets is covered by IEC Standard 61400-25 which includes communication within the wind turbine system, other actors and SCADA. This standard also provides abstract definitions, is independent of protocols/OS and provides interoperability. The standard itself is intended to be client/server based, specifies LN and provides communication hierarchy.

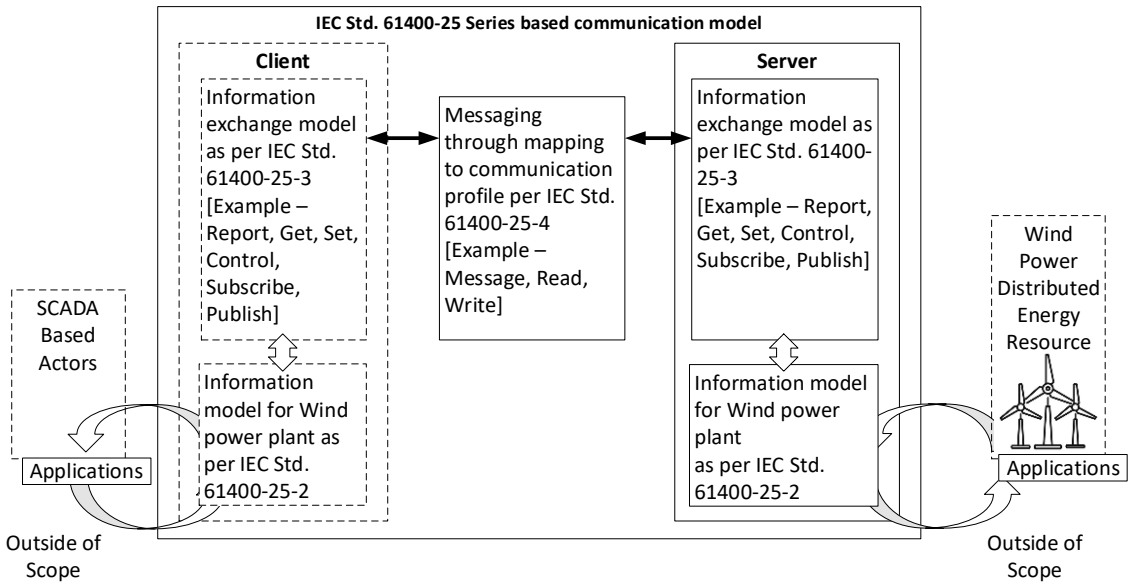


Figure F.9 – IEC Standard 61400 based communication conceptual model

F.9. Utilizing IEC Standard 61499

The backbone nominative standard 61499 provides generic functional blocks for industrial control/measurement architecture. Software units such as functional blocks entail behavioural encapsulation which can be either basic or composite or service interfaced.

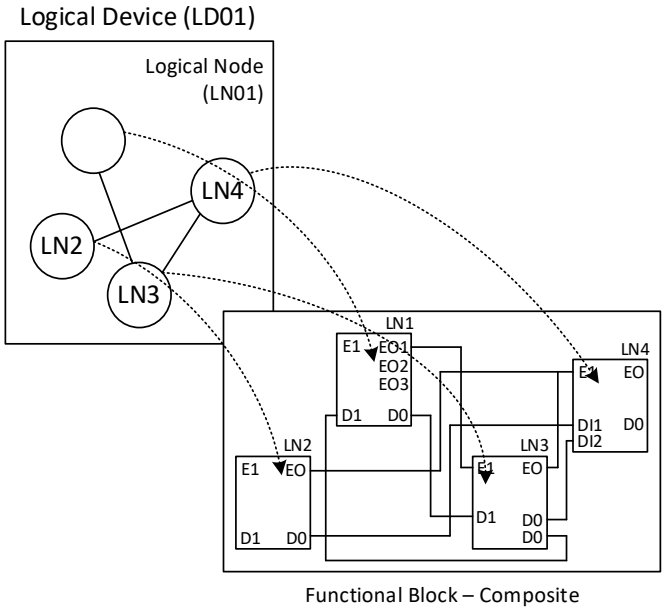


Figure F.10 – IEC Standard 61850 LNs/LDs based on IEC Standard 61499