School of Electrical Engineering, Computing and Mathematical Science

Automation, Protection and Control of Substation Based on IEC 61850

Shantanu Kumar

ORCID ID: 0000-0001-6789-7180

This Thesis is presented for the Degree of
Doctor of Philosophy
of

Curtin University

March 2023

DECLARATION

To the best of my knowledge and belief, this thesis contains no material previously published by any other person except where due acknowledgment has been made. This thesis contains no material which has been accepted for the award of any other degree or diploma in any university.

Electronic Signature

Signature: Shantanu Kumar

Date: 15th September 2023

ACKNOWLEDGEMENT OF COUNTRY

We acknowledge that Curtin University works across hundreds of traditional lands and custodial groups in Australia, and with First Nations people around the globe. We wish to pay our deepest respects to their ancestors and members of their communities, past, present, and to their emerging leaders. Our passion and commitment to work with all Australians and peoples from across the world, including our First Nations peoples are at the core of the work we do, reflective of our institution’s values and commitment to our role as leaders in the Reconciliation Space in Australia.

Acknowledgments

There are number of people and organisations that I wish to acknowledge in this journey towards a Higher Degree by Research (HDR).

First and foremost, I would like to profusely thank Professor Syed Islam, who was my main supervisor at the Curtin University, Perth, Australia, along with co-supervisor Dr Narottam Das at Curtin University, Perth, Australia when I commenced my PhD journey in 2014. After they left Curtin University for good, my new main supervisor was Professor Ahmed Abu-Siada, who guided me until the completion of this thesis. I express my deep gratitude to all three supervisors for their support, guidance and motivation. Their immense guidance, meticulous supervision and contribution of ideas at every juncture, including supervision of multiple laboratory experimentations and publications, are the highlights of my HDR journey. Without their supervision and guidance, I couldn’t have managed to complete this practical research at Curtin University, which is hugely beneficial to local mining and utilities industries authored by an industry supported student. I am also filled with profound gratitude to Professor Ahmed for his able guidance, in achieving publications in three reputed journals and for his thesis supervision. My sincere thanks to friend Mr Sejin Cheeran who supported me with experiment issues related to software, firmware and myriad challenges on interoperability issues. I am also indebted to Mr Rodney Hughes, Mr Chirag Mistry of GE, Mr Anisur Rahman of ABB, Mr David Gonzalez of SEL, Mr Filip Ivanovski & Leonardo Torelli of CSE Universe, Mr Ravi Desai & Maryam Khallaghi of Omicronenergy, and Mr Ian Young of Schneider for their technical support during multiple experiments on SAS at Curtin University.

This thesis couldn’t have been submitted on time without the huge effort by a professional editor Ian Mathieson, who pushed himself and diligently checked each and every sentence, by proofreading, editing, indexing and compiling this lengthy document over the weekend.

I thank Curtin University’s school technical coordinator Zibby Chelma, for his support in wiring connections whenever requested. Also, the digital substation project at Curtin University could only be achieved by virtue of substantial donations of equipment, peripherals and software tools related to Substation Automation System from ABB, CSE Uniserve, GE, ALSTOM, Schneider, and Siemens energy, SEL, Omicronenergy, Rodhughes Consulting, Westermo and Eaton. It was largely due to their kindness and donation to Curtin University’s digital laboratory that contributed towards to this practical research, exhibiting immense capabilities to carry out digital protection experiments applying multi-vendor equipment. It is envisaged that this research laboratory at Curtin University shall herald many future projects on digital SAS and cybersecurity that promises a new paradigm in digital Substation Automation Scheme as applicable to utilities and mining industries around Australia. I also express my sincere thanks and gratefulness to BHP and Westernpower for their support throughout my HDR journey. These utilities and mining giants provided me time-in-lieu and motivation to conduct this practical research based on the legacy issues related to condition monitoring, secondary systems, encountered by their operators at high and low voltage substations.

Last but not the least, I thank almighty and The Supreme Lord Krishna and my departed parents (Late Mr. Janaki Ballav Swain & Late Mrs. Kalayani Swain) for giving me resilience and tenacity to undertake this research. Additionally, I couldn’t have completed this challenging project, without the moral support of my family and friends particularly Natasha Swain (wife), Radhika Swain (daughter), Reeta Rout (sister), Mamta Khuntia (sister), Swagatika Swain (Sister), Anjali Patra (friend), Zubia Nizam (friend), Roopa Tharakkan (friend), Swagatika Swain Lenka (friend), Professor Sushama Wagh, Professor Prachi Mukherjee and Reeta Rath (friend) while working as a full time engineer and doubling up as a part time research scholar.

ABSTRACT

Automation, Protection and Control of Substation Based on IEC 61850

Reliability in power system protection systems has been an issue with the substation operation due to the use of multi-vendor equipment with proprietary features, environmental issues, and complex fault diagnosis. Failure to address these issues could have a significant effect on the performance of the entire electricity grid.

With the introduction of IEC 61850 standard, substation automation system (SAS) has significantly changed the scenario. With number of topologies and communication protocols used in a smart digital substation such as Generic Object-Oriented Substation Event (GOOSE) and Sampled Values (SV), Fibre optic cables (FO) could be a good substitute of messy copper cables and facilitate the use of Non-Conventional Instrument Transformers (NCIT). Thus, the substation operators will be able to address challenges related to legacy protocols while carrying out smooth network operation and perform with reliability of isolating a faulty incomer or feeder, fault diagnostics, achieve faster project completion and mitigate environmental problems associated with leaked oil or SF6 gas. However, IEC 61850 communication protocol comprises of few issues related to latencies, redundancies, and end-to-end (ETE) delays, time synchronization, and application of correct topologies.

In light of the above, the objective and motivation of this research is to undertake practical research at a laboratory environment to validate a reliable SAS network having multivendor intelligent electronic devices (IEDs), managed switches, Merging Units (MU) having proprietary features, and analysis of time synchronization issues associated with a digital protection scheme. Also, the significant advantages of using IEC 61850 protocol versus legacy conventional protocols such as MODBUS, PROFIBUS, PROFINET, DNP3 or TCP/IP have been highlighted in the following chapters.

STATEMENT OF CONTRIBUTION TO PUBLICATIONS

International Peer Review Journal Publications

This thesis includes technical materials and the results of experiments that have been published in international peer-review journals and conferences. These publications are:

1. S. Kumar, A. Abu-Siada, N. Das and S. Islam,"Review of the Legacy and Future of IEC 61850 Protocols Encompassing Substation Automation System,", *Electronics* 2023,12,3345, https://doi.org/10.3390/electronics 12153345
2. S. Kumar, A. Abu-Siada, N. Das and S. Islam, "Reverse Blocking Over Current Busbar Protection Scheme based on IEC 61850 Architecture," in *IEEE Transactions on Industry Applications*, 2022, doi: 10.1109/TIA.2022.3220727
3. S. Kumar, N. Das, S. Islam and A. Abu-Siada, "Toward a Substation Automation System Based on IEC," 2021. Electronics 2021, 10, 310. https://doi.org/10.3390/electronics 1003031

The main contribution of the candidate to these three journal papers are:

1. Conceptions and design, acquisition of data and Methods by setting up apparatus as applicable to digital substations. Data conditioning and manipulation of logic diagrams and program logics, analysis and statistical methods in modelling and generating of results, preparing graphical pictures and interpretation and discussion, manuscript preparation, final approval of manuscripts and incorporating valid comments and changes to reviewer's comments.
2. The main contribution of the co-authors to the journal paper 1, 2 & 3: Reviewing of results, verifying main author's contribution and novelty, discussion, assessing reviewer's comments, the quality of the experimental results and overall review of the manuscript.

Name	Author: Shantanu Kumar	Supervisor: Ahmed Abu-Siada
Signature	Electronic signature by SHANTANU KUMAR 15.09.2023	Ahmed Abu-Siada (Endorsed via electronic signature on 13.03.2023)

CONFERENCE PUBLICATIONS

1. S. Kumar, A. Abu-Siada, N. Das and S. Islam, "Comparison between Wired versus wireless Mode of Digital Protection Scheme Leveraging on PRP Topology," *IEEE Sustainable Power Conference (ISPEC),* Perth, Australia, 2022, pp. 1-6.
2. S. Kumar, N. Das, S. Islam and A. Abu-Siada, "A Fast and Reliable Blocked Bus Bar Protection Scheme Leveraging on Sampled Value and GOOSE Protection based on IEC 61850,"*2021 30th Australasian Universities Power Engineering Conference (AUPEC),* Perth, Australia 2021, pp. 1-6, 978-1-6654-3451-5/21/$31.00 © 2021 IEEE.
3. S. Kumar, N. Das, S. Islam and A. Abu-Siada, "Verification of Latency and Delays Related to a Digital Topology based on IEC 61850," *2019 29th Australasian Universities Power Engineering Conference (AUPEC),* Nandi, Fiji, 2019, pp. 1-6, doi: 10.1109/AUPEC48547.2019.211964.
4. S. Kumar, “Digital protection using NCIT in process bus environment”. APS-2018, Brisbane, Australia.
5. S. Kumar, N. Das and S. Islam, "Mitigation of Sympathetic Tripping Leveraging on IEC 61850 Protocol," *2018 Australasian Universities Power Engineering Conference (AUPEC),* Auckland, New Zealand, 2018, pp. 1-6, doi: 10.1109/AUPEC.2018.8758053.
6. S. Kumar, N. Das and S. Islam, "High Voltage Substation Automation and Protection System Based on IEC 61850," *2018 Australasian Universities Power Engineering Conference (AUPEC),* Auckland, New Zealand, 2018, pp. 1-6, doi: 10.1109/AUPEC.2018.8757995.
7. S. Kumar, N. Das and S. Islam, "Implementing PRP and HSR Schemes in a HV Substation based on IEC62439-3," 2018 Condition Monitoring and Diagnosis (CMD), Perth, WA, 2018, pp. 1-5, doi: 10.1109/CMD.2018.8535663
8. S. Kumar, N. Das and S. Islam, "Performance evaluation of two interconnected high voltage utility substations using PRP topology based on IEC 62439-3," *2017 Australasian Universities Power Engineering Conference (AUPEC),* Melbourne, VIC, 2017, pp. 1-5, doi: 10.1109/AUPEC.2017.8282401.
9. S. Kumar, N. Das and S. Islam, "Software implementation of two seamless redundant topologies in a digital protection system based on IEC 62439-3," *2016 Australasian Universities Power Engineering Conference (AUPEC),* Brisbane, QLD, 2016, pp. 1-5, doi: 10.1109/AUPEC.2016.7749323.
10. S. Kumar, N. Das and S. Islam, "Performance monitoring of a PMU in a microgrid environment based on IEC 61850-90-5," *2016 Australasian Universities Power*

Engineering Conference (AUPEC), Brisbane, QLD, 2016, pp. 1-5, doi: 10.1109/AUPEC.2016.7749356.

11. S. Kumar "Protection Redundancy in a Digital Network within a High Voltage Utility Substation based on IEC 62439-3", APS-2016, Melbourne, Australia.
12. S. Kumar, N. Das and S. Islam, "Performance evaluation of a process bus architecture in a zone substation based on IEC 61850-9-2," *2015 IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC)*, Brisbane, QLD, 2015, pp. 1-5, doi: 10.1109/APPEEC.2015.7381017.
13. S. Kumar, N. Das and S. Islam, "High performance communication redundancy in a digital substation based on IEC 62439-3 with a station bus configuration," *2015 Australasian Universities Power Engineering Conference (AUPEC)*, Wollongong, NSW, 2015, pp. 1-5, doi: 10.1109/AUPEC.2015.7324838.
14. S. Kumar, "Causes and Mitigation of Sympathetic Tripping Phenomenon Based on IEC61850", APS-2014, Sydney, Australia.
15. S. Kumar, N. Das and S. Islam, "Performance analysis of substation automation systems architecture based on IEC 61850," *2014 Australasian Universities Power Engineering Conference (AUPEC)*, Perth, WA, 2014, pp. 1-6, doi: 10.1109/AUPEC.2014.6966532.
16. S. Kumar, N. Das, J. Muigai and S. Islam, "Performance evaluation of data transmission in a single and double bus network within the utility substation based on IEC 61850," *2014 IEEE PES General Meeting | Conference & Exposition*, National Harbor, Washington, MD, USA, 2014, pp. 1-5, doi: 10.1109/PESGM.2014.6939273.

1. Book Publication of Chapter 9 titled :-

"Microgrid communications-protocols and standards" in the book "Variability, Scalability and Stability of Microgrids" by the IET Publication.

Name	Author: Shantanu Kumar	Supervisor: Ahmed Abu-Siada
Signature	Electronic signature by SHANTANU KUMAR 15.09.2023	Ahmed Abu-Siada (Endorsed via electronic signature on 13.03.2023)

CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

ADU – Application Data Unit

AIS – Air Insulated Substation

ARP – Address Resolution Protocol

CB – Circuit Breaker

CIT –Combined Instrument Transformer

CT – Current Transformer

DAN – Doubly Attached Node

DER – Distributed Energy Resources

DNP3 – Distributed Network Protocol

DOS – Denial of Service

ETE – End To End Delay

FIFO – First In First Out

GOOSE – Generic Object Oriented Substation Event

GUI – Graphical User Interface

HMI – Human Machine Interface

HSR – High-speed Seamless Redundancy

HV – High Voltage

IDMT – Inverse Definite Minimum Time

IEC – international Electrotechnical Commission

IED – Intelligent Electronic Device

IEEE – Institute of Electrical Electronics Engineers

IET – Internet of Things

IP– Internet Protocol

LAN – Local Area Network

LE – Light Edition

LRE – Link Redundancy Entity

MAC – Medium Access Control

MMS – Multimedia System

MTTF – Mean Time for Failure

MU – Merging Unit

NCIT- Non Conventional Instrument Transformer

FO – Fibre Optic

PDU – Protocol Data Unit

PROFIBUS – Process Field Bus

PROFINET – Process field network

PRP – Parallel Redundancy Protocol

PTP – Precision Time Protocol

RCT – Redundancy Control Trailer

RSTP – Rapid spanning tree protocol

RTU – remote Terminal Unit

SAN – Single Attached Nodes

SAS – Substation Automation System

SCADA – Supervisory Control Data Acquisition

SPP – Sample per second

STD – State Transmission Diagram

SV – Sampled Value

TC – Technical Committee

T&D – Transmission and Distribution

TCP/IP – Transmission Control Protocol

VLAN – Virtual Local Network

VT – Voltage Transformer

WAN – Wide Area Network

CHAPTER 1:

INTRODUCTION

1.1 INTRODUCTION

Reliability of protection equipment have been a burning issue for substation operators since the time electricity was invented. Failure to address these issues could have a significant effect on the operator’s performance in delivering power to customers, leading to blackouts. In addition to the protection challenges, there are issues related to failure of primary plant assets due to failure of protection and control. This could lead to huge financial impact on operators and service providers.

With the introduction of IEC 61850 as prepared by International Electro-technical Commission (IEC), communications between the primary plant assets and control rooms have reached a new paradigm in SAS. With numerous data exchanges in a smart digital substation utilising Generic Object-Oriented Substation Event (GOOSE) and replacing secondary copper cables by introducing fibre optic (FO) cables, there is overall improvement in protection and control. However, unless the system is tested and proven in relation to the acceptance of IEC 61850 communications protocol, it will not reach the desired acceptance, as shown in their experiment by Donovan et al. by conducting practical research on IEDs [1]. It is envisaged that in the next decade, a large number of IEC 61850 enabled substations shall rise up in the utilities and resource industry as the legacy protocols have issues in reliability, expandability, version upgrade, interoperability, obsolescence etc. The focus of this research is to test and recommend suitable automation, protection and control protocols that could adapt and upgrade conventional substations which can enable interoperability with multivendor equipment having proprietary features and analyze disturbances in the network to monitor the health of critical substation assets. Bharadwaj.et al have conducted research on various substation protocols such as PTP, IRIG-B, IEC60870, IEEE 37-238 and finally recommending IEC 61850 being the most beneficial [2].

1.2 OBJECTIVE OF THIS RESEARCH

The key objective of this research programme undertaken is to test and validate a reliable digital protection system in a high voltage (HV) substation with redundancy features that shall monitor critical substation key assets such as power transformers, circuit breakers, isolators etc. For any substation to operate smoothly, advanced information, communication, and automation play a vital role in enhancing an operator's knowledge of the asset health of the equipment. This not only prolongs the remanent life of the asset but also prepares the operator to protect its assets from electro-mechanical faults. IEC 61850 communication protocol supports qualitative and comprehensive idea of faster clearance of time of faults leveraging on novel technologies over the conventional peer-to-peer method, ease of disturbance diagnostic and optimum use of communication tools to automate the network from protection, control and measurement perspective.

IEC 61850 standard, that had been published by IEC in 2002, provides multiple data over Ethernet and FO wires encapsulating various components of substation automation. This standard gives clear direction on time critical information between various IEDs within the substation that shall protect and control substation equipment by transferring messages reliably and quickly. It provides a platform for interoperability of multivendor IEDs in an integrated automation system. This protocol adapts to conventional equipment carrying binary or analogue information which could be substituted with digital signals. It provides guidelines to communicate between intelligent electronic devices (IED's) and substation primary plant equipment in the switchyard, while focusing on an integrated control system from ease of operation perspective.

Globally, there have been a trend in IEC 61850 being applied to substation communications resulting in a healthy trend and stable operation of power system protection. However, there is a lack of confidence in the technology across utilities and industries due to lack of knowledge and understanding of its capabilities amongst operators. Compounding to this issue, many of the multi-vendor smart devices with proprietary features, does not communicate amongst themselves and cyber security threats undermine their confidence when operating on Internet of Things (IoT) which directly conflicts with the three fundamental elements of IEC 61850 as elaborated by Kumar and et al. using various topologies and traffic flow scenarios in a different environment are [3]:

- Interoperability
- Free configuration
- Long term stability

In the first case, Interoperability ensures that multi-vendor relays exchange data within the pre-defined time and use it for control and alarm. In order to achieve the fundamental regime of giving reliable protection and control using IEDs and other peripherals, different phases in the project were undertaken in the research program at Curtin University, with the researcher having a background being a full-time electrical engineering professional with over 33 years of industrial experience as outlined below:

1. Modelling of the real time performance of substation IEDs and exhibiting case studies related to the periodic, random, and burst data streams based on OPNET desk top simulation and verify latencies and End-to-End (ETE) delay.
2. Test and validate interoperability issues arising out of multi-vendor equipment.
3. Identification and comparison of different scheduling schemes; checking traffic flows in different topologies i.e., Tree, Bus, Mess etc. on a desktop model.
4. Testing and validating digital protection redundancies a substation network such as Parallel Redundancy Protocol (PRP) and High-Speed seamless Redundancy (HSR) in OPNET as well as practically.
5. Testing and commissioning interoperability of IEDs and peripherals in an IEC 61850 laboratory environment – assembling and testing a multivendor set-up consisting of Station bus and Process bus schemes in a virtual replica of a substation automation scheme.
6. Implementation of a reliable IEC 61850 protection scheme in an air insulated substation (AIS) using Non-Conventional Instrument Transformer (NCIT); this will reduce substation secondary cabling while performing comprehensive monitoring, data logging and ease of fault diagnostics without saturation effect. This equipment shall carry out the protection of the asset under accurate time synchronisation in Precision Time Protocol (PTP) mode.
7. Simulation Studies to verify and validate the operation of smart micro-grid, extensive off-line simulations performed using OPNET.

The ability for IED’s from one or several manufacturers to exchange information and use it for their own functions. For free configuration, the standard shall support different philosophies and allow a free allocation of functions e.g., it must work equally well for centralised (RTU like) or decentralised (SCS like) systems. In the case of Long-term stability – The standard shall be future proof, i.e., it must be able to follow the progress in communication technology as well as evolving system requirements.

1.2 Background

In the conventional method of protection, control and automation, the substation protection system usually interrogate and handles data using local devices based on its time curve setting. In a complex substation environment with digital data flowing, there are ever-increasing needs for fast-acting intelligent electronic devices (IEDs) which can perform data modelling and having a good communication performance. However, many non-critical messages queue up and delay the Generic Object-Oriented Substation Events (GOOSE) and Sampled Value (SV) message communication during heavy traffic, leading to traffic congestion [4]. This could have serious repercussion on the protection system, if the digital data is not exchanged reliably due to delayed messages packaging and parsing between the substation IEDs protecting substation HV, LV assets and the grid. Further, IEC 61850-5 requires these issues to be identified and mitigated in a dynamic network [5].

Fig. 1.1 shows a block diagram of IEDs which communicates based on IEC 61850 within a substation environment. Previous substation automation system has not taken full advantage of the new system environment and there is scope to develop it further. As well there are limitations in automation, protection and control devices using local data in a conventional substation due to hardwired point-to-point conventional IEC 61850 which uses efficient software methodologies to protect the primary plant assets with a smarter methodology based on digital and network-based systems [6]. This has given rise to complexity in digital automation related to protection, control and monitoring of the primary power plant assets in terms of redundancies, interlock, alarms and back up protections as guided in IEC 61850 and IEC62439-3 standards, which is a key motivation to conduct further research by the author. Previous conventional protection models within a substation environment have managed the protection coordination by using local data and time curves but with the advancement of technology, it is possible now to investigate a SAS based on Ethernet communication network [7].

Fig. 1.1 shows a simplified digital substation having IEDs and switches in the network. It uses first-in-first-out (FIFO) scheme for frame subscribed and broadcast by the smart devices, while using packet scheduling. This scheme have few limitations in data scheduling as the performance deteriorates during high scheduling time [8]. This thesis has researched and addressed GOOSE and SV message performance by using packeted scheduling schemes during peak traffic periods and highlighted the ETE at nodes and devices [9]. Additionally, Fig. 1.1

exhibits a digital substation switchyard wherein the field equipment transmits binary analogue inputs to Merging Units (MU) that transmit SV frames in Process bus mode to managed switches which broadcast to IEDs. The substation control room sends GOOSE commands to circuit breakers (CB) to open or close up and isolate power transformers for maintenance or diagnostic purposes. Control and monitoring via the managed switches are guided by using Virtual Local Network (VLAN) that have multiple channels to manage GOOSE and SV. Appropriate software tool monitors the GOOSE and SV frame traffic in the network [10].

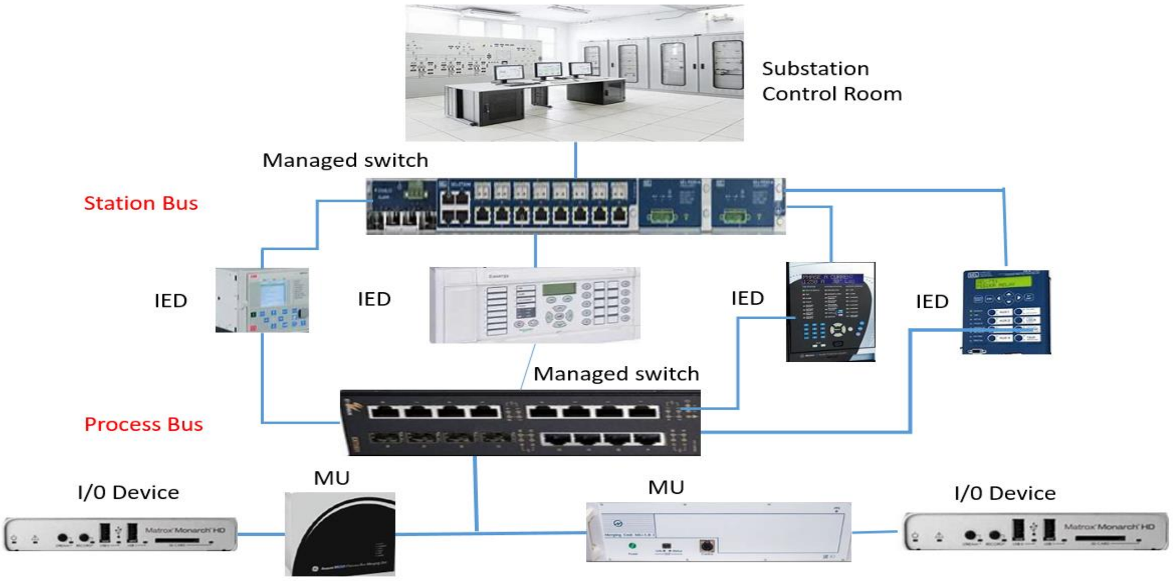


Fig. 1.1. SAS based on IEC 61850 systems.

The digital substation shown in Fig. 1.1 could reliably deliver power and also be able monitor the asset condition which will give better visibility to the operator particularly on an asset life health index and smooth power flow. Also, by virtue of the introduction of smart digital equipment, it could lead to a smaller footprint of digital substation devices and reduction in cable means. This will enable utilities to save financially and could still manage to operate with their aging infrastructure while managing optimum use of electricity generation, transmission, and distribution costs. Application of digital technology monitors using a diverse range of performance and condition information tools and this thesis highlights modern approach based on performance testing using practical equipment and software tools on digital devices of tomorrow.

1.3 RESEARCH SIGNIFICANCE

IEC 61850 researchers have so far focused on smarter operation of existing transmission and distribution (T&D) networks. However, there are multiple issues with respect to interoperability, cyber security, long development cycle, training costs, lack of knowledge base etc. To cope up with the future demand in power transmission and rising cost of electricity due to failure of assets, new research ideas in substation automation within its domain have been addressed applying IEC 61850 and advanced version IEC 62439, by testing in a laboratory using IEDs and switches, simulated on a virtual digital substation at Curtin University in Perth, Australia [11].

It is observed, multiple protocols in substations currently exist in substation automation domain which don't communicate well amongst each other due to proprietary features thereby compromising the reliability in a SAS network. The project undertaken and thesis highlights key issues of legacy protocols such as are posed in communication, latency, interoperability but not limited to:

- single protocol of a HV substation based on IEC 61850 protocol
- performance testing and validation of substation topologies
- Configure object modeling of data in the substation Interoperability within protection devices.

1.4 SAS IN A LABORATORY ENVIRONMENT

The author in this thesis has modelled and simulated a digital substation network based on OPNET software and compared the performances with a conventional substation. Further, data communication and traffic delays at nodes were determined in a lab set-up based on IEC 61850 encompassing the following topologies:

- Single bus
- Double bus
- Ring bus.

These topologies could be extended to an Air Insulated Substation (AIS) or Gas Insulated Substation (GIS) from SAS point of view including protection, control and monitoring from data flow perspectives. The experiments undertaken and the evaluation of digital SAS indicated the enhanced performance using redundancy technologies such as PRP and HSR topologies. It is highlighted that digital protection is able to perform better during the transmission of digital packets related to mission critical, time stringent tasks such as SV and GOOSE tripping over Ethernet LAN (Local Area Network) applications. A typical AIS generating substation in single line diagram (SLD) is shown Fig. 1.2, having multiple substations, at different voltage levels such as 11-kV and 132-kV which are usually the common HV voltages in a mining infrastructure for power dispatch.

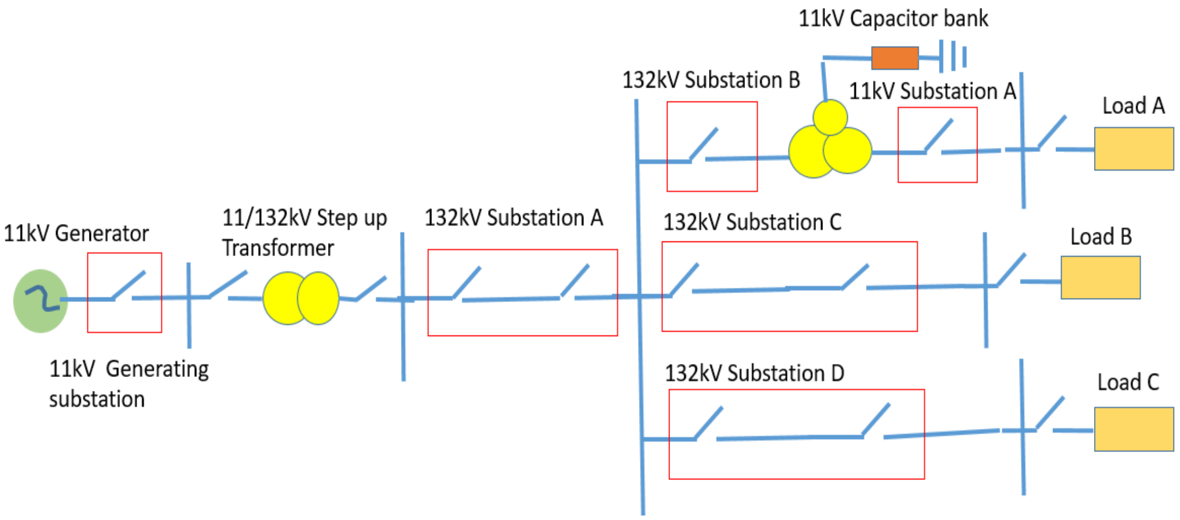


Fig. 1.2. Single Line Diagram of an AIS substation.

The methodologies applied to carry out substation automation, protection and control were to use digital frames over FO or Ethernet wiring to broadcast and subscribe them to IEDs while analysing the traffic flow. Traffic flow of digital frames usually slows down the frame speed compromising the protection. This thesis discusses the different topologies as applicable to substation integrated systems in Station and Process bus mode. Some of the prototype models were simulated and tested in OPNET, with results in the following chapters, relating to:

1. Real Time Simulation on station bus and process bus communication
2. study of a true interaction substation protection and power system model
3. analysis of maximum simulation efficiency (i.e., more contingencies can be investigated in less time)
4. study of the packet scheduling and traffic congestion scheme within the substation IEDs
5. reliability of GOOSE and SV trip time to address rapidness of fault clearance
6. impact of NCIT on smart protection.

Detailed investigation has been carried out in this thesis to assess the performances of traffic flow and data packet arrival within a predetrmined time. Delays in transmission in a digitally controlled substation occur due to message packaging and parsing which takes up most of the time. Simulation carried out to test data flow and results verified demonstrate the promises offered by using the IEC 61850 standard in future. Practical application using small size data structures and avoidance of large data populations is the key feature of this thesis as it has been found challenging to seggregate bigger size data that caused delays in data transmission [12].

1.5 RESEARCH METHODOLOGY

Stage 1, Literature review: This phase is narrated in the following section, wherein the main aim was to find out issues and problems related to existing substation communication, automation, and protection architecture. Also, gaps in the substation automation and protection need to be identified in order to improve the problems. It should be mentioned that the literature review is an ongoing process and many of the scopes are related to future work as it cannot be covered under this project.

Stage 2, Development of a digital substation in an IEC 61850 lab at the university: Laboratory was set up to IEC 61850 and enhanced to parallel redundancy protocol based on IEC 62439-3 [13]. Work was carried out on Station bus and Process bus configuration with various IEDs and switches using different vendors. Issues arising due to interoperability and proprietary software were be studied in this stage. At laboratory stage speedy data transfer and traffic issues at nodes were observed for time critical information such as status changes, blockings, releases, or trips between IEDs [14].

Stage 3, Testing of PRP and HSR protocols: In a digital substation of the future, it is critical to have redundancies in protection. Research in this direction focused on improving the protection redundancy using dual node IEDs and switches based on IEC 62439-3 making detailed recommendation and methodologies of installation, testing and commissioning of PRP and HSR.

Stage 4, Testing of NCIT: The research work was extended to test NCIT in a laboratory set-up for a Process bus scenario and determined its impact on other smart devices [15].

Stage 5, Testing of Reverse Blocking Over Current (RBOC): A test bench having IEDs, switches and peripherals was being used at present at Curtin university, using algorithms for validation. The results shall be published in international journals and conferences.

Stage 6, Recommendation for future works: A recommendation was made to use this protocol using PRP-HSR hybrid topology and condition monitoring of key assets.

1.6 LITERATURE REVIEW

This section presents a literature review on IEC 61850 communication protocol (Chapter 2), topologies applicable to IEC 61850 (Chapter 3). The other chapters such as Communication Redundancy in a Digital Substation using two seamless topologies (Chapter4), use of NCIT and Process bus (Chapter 5) and testing of protection using Reverse Block Over Current (Chapter 6) also have multiple references and critical analysis of other's research work which have been the scope of this thesis and as applicable to smart grid. Chapters 2, 3, 4, 5 and 6 provide and in-depth analysis through discussions, desktop modelling and practical laboratory testing. In each of these chapters, background actual testing and discussions have been carried out elaborately. A number of additional research projects have been suggested in chapter 7 which shall guide others to choose wide variety of projects as outlined in section 7.3.

Kanabar et al. have carried out the desktop simulation using an OPNET model on a distribution system and exhibited the effect of latencies on the digital protection system. The author has considered distributed automation system as applicable in a HV switchboard and linked it up with a Distributed Energy System (DER). The author proposed a communication requirement based upon IEC 61850, this the model has been tested at 10 Mb/s and 100 Mb/s which is prevalent speeds at the point of time of writing this paper [16]. Ingram et al. have compared different buses such as Process, Station, overall architecture and they have compared the mean time for failure (MTFF). The author has tested this MTFF in a laboratory condition and recommend further reliability tests [17]. Das et al have attempted to check the reliability, accuracy and speed for different topologies such as cascading, ring and tree topologies. They have carried out simulation using an OPNET platform on a star, ring and hybrid architecture. The author has validated it using bus bar protection (BBP) through multivendor equipment. Liuet al. have narrated the different protocols currently deployed by substations operators and the merits/demerits of having such protocols compared [18]. The author has recommended others to test out the MODBUS, PROFIBUS, PROFINET, DNP3, TCP/IP etc. Kumar et al. have highlighted the issues of not having redundancies and recommended new methodologies in their publication named as High performance communication redundancy in a digital substation based on IEC 62439-3 with a station bus configuration [19]. Das et al have evaluated a digital substation performance with a conventional substation and modelled it a digital OPNET. The authors have further validated it with newer OPNET models [20]. Nojova et al. have modelled a HV power network of a 400 kV substation in OPNET with number of IEDs connected in a SAS network in IEC 61850 and DNP3 communication protocol. They have highlighted the widespread use of DNP3 protocol and attempted to find the latencies related to End-To-End (ETE) communication delay. The author of this thesis have discussed the performance of DNP3 versus IEC 61850 in chapter 2. He has presented the results and discussions including latencies encountered due to ETE in a power transformer [20]. The author has validated using OPNET model for a similar HV substation. Ingram et al. have carried out a system-based testing wherein a power transformer in a Process bus network has been tested with a Merging Unit (MU) in the SAS circuit. In a similar comparison, the author has also introduced the concept of Precision Time Protocol (PTP) which deals with the time synchronisation in the digital network [21]. Heine et al. have experimented with two relays. He has used conventional versus digital IEDs. He has involved other being routed by MU to an IED and has experimented it with practical examples on NCIT's interoperability with IED. This thesis' author has carried out similar exercise using a 11- kV switchboard to test these NCITs in a HV mining substation network. The thesis' author provides a strong case for deployment of NCITs in the network [22]. Chatrefou et al have discussed Interoperability and have included Non-Conventional Instrument Transformers (NCIT) and Intelligent Electronic Devices (IED) in their discussion [23], Thesis' author has extensively used practical research on interoperability of SAS network in a HV substation to validate the interoperability which has been a challenge to substation operator using digital protection scheme. Zhang et al. have discussed the impact of loss of SV data packet that would have on a protection scheme during the mal-formation of digital frames. They further discuss the impact a loss of SV would have on the process topology due to traffic congestion and lack of time synchronisation. It is inferred from these papers that delay also could be attributed due to switching, fibre and rated delay in a process bus topology [24]. Further testing has been carried out by thesis author to prove the reliability of the digital protection system. Xu et al. have compared the performance of HSR with a PRP topology. These authors have also done a modelling of PRP and HSR networks and evaluated the performance under fault condition [24]. Thesis author has conducted an OPNET modelling of HSR and PRP topologies in chapter 4 and exhibited the method of achieving redundancies in a digital network. Liu et al. have calculated the performance of a Red Box embedded within the network under fault conditions, and delay measurement as it passed via various nodes. A prototype model has been designed on a software platform and its performance evaluates the Red Box [25]. This thesis' author has replicated the experiment using an OPNET and experimented using an OPNET platform for delay and latencies.

Liu et al have discussed different protocols such as RSTP, Process bus and Station bus for comparison for performance under dynamic conditions. These authors exhibit the number of trip delays as frames get clogged up or malformed and finally, they have recommended PRP and HSR for future deployment [26], Thesis author has done experiments using PRP and HSR and hybrid topologies in a OPNET platform as well as physical hardware at Curtin university lab. They have validated digital model on an experimental test bed as well as on an OPNET platform that included traffic queuing. Bernardino et al have compared the speed of data transfer for GOOSE and SV in the network and evaluated Process bus latency. The authors have highlighted the importance of time synchronisation in IEC 62439-3 with respect to PTP and IEEE 1588 and they have compared this with IEC 61850-5 standards requirement. The authors highlight that the reason for delay is attributed to typical PRP and HSR signatured frames which only specific peripherals can perform. The authors have compared the delays in circulating GOOSE and SV messages for PRP and HSR during normal stable condition as well as fault condition. The estimated value of the latency during normal and fault conditions exhibits appreciable difference [27]. Thesis author has carried out practical tests at the Curtin laboratory and has improved the protection results on a digital platform. Goraj et al. have exhibited a Rapid Spanning Tree Protocol (RSTP) and have compared it with a Multiple Spanning Tree Protocol (MSTP). The authors have cited IEEE 802.1D and discussed the restriction on RSTP protocol. It highlights the VLAN configuration to be carried out in order to allow GOOSE and SV to appropriately be routed via managed switch [28]. The Thesis author has practically conducted experiments and enabled a SEL switch with VLAN gate for GOOSE and SV packets.

1.7 FACILITIES AND RESOURCES AT CURTIN UNIVERSITY, PERTH, AUSTRALIA – OVERVIEW OF IEC 61850 SAS LABORATORY

A new laboratory at Curtin University at Bentley, Perth, Australia with four cubicles containing switches, MUs and IEDs is occupying building 214-110 is shown in Fig. 1.3. This room possesses all digital equipment plus a digital projector and workstation with high specifications to carry out desktop simulation on OPNET, MATLAB and OPAL RT tools. This thesis has a number of results obtained by execution of a small protection and automation project, connecting IEDs and switches obtained largely from donations from industry partners i.e., ABB, ALSTOM, SCHNEIDER, Siemens energy, GE, SEL, Omicronenergy and EATON. A desktop PC with adequate RAM and memory when connected to an operational technology infrastructure, analyses the traffic load and carries out the research project. The local area network on which this OT platform operates begins with 10.128.68.XX. Secondary injection tool i.e., Omicron Energy IED Scout software of Omicronenergy equipment i.e., CMC 356 which could simulate a single phase and three phase faults in unbalanced state. A number of software by original equipment manufacturer (OEM) have been used to make the communication with multi-vendor IEDs possible and to monitor their possible tripping and opening times such as PCM-600 by ABB, Easeargy by Schneider, DigSi by Siemens energy, Accelerator by SEL etc. The exact IEDs pick up and tripping time could be identified by the Test universe software along with other general software like DigSi, MATLAB/Simulink and Microsoft Office. These sniffs the GOOSE frames circulating in the network from modelling and simulation perspective. SV scout of Omicronenergy is used to check the characteristics of wave generated by digital traffic and sniff the technical key of MUs.

Fig. 1.3 shows the exact layout of the panels within the laboratory with Cubicle 1, 2, 3 housing mainly IEDs while switches and Red Box have been located in cubicle 4. The experimental results produced by virtue of undertaking this research have attracted many utilities and industries in Perth, to visit the state-of-the-art IEC 61850 laboratory and receive a better understanding on the SAS protocol laid down to IEC 61850 standard. In nutshell, it heralds a new paradigm in digital technology by actual simulation and validation of the protection schemes in a laboratory environment. The facilities available in the proposed Green Electric Energy Park of the Curtin University, Perth, Australia promise to be included in the future curriculum of electrical engineering while lending support to local utilities and resources industries. Further research work could be carried under different projects in Infrastructure for real-time communication in smart grid [29].

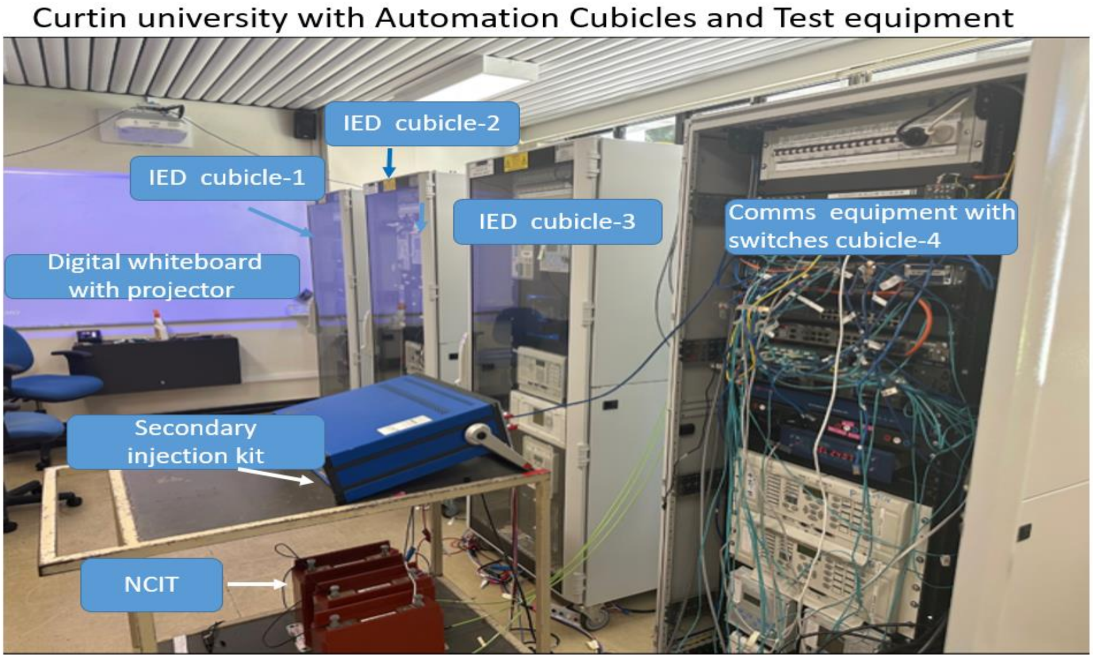

Curtin university with Automation Cubicles and Test equipment
IED cubicle-2
IED cubicle-1
IED cubicle-3
Comms equipment with switches cubicle-4
Digital whiteboard with projector
Secondary injection kit
NCIT

Fig. 1.3. Hardware overview of IEC 61850 Communication and SAS equipment lab set-up at Curtin University, Perth, Western Australia, Australia.

1.8 DATA STORAGE

All the data such as traffic congestion, data corruption, malfunction and load profile have been stored at a secured location in the lab and with the author of this thesis. All electronic and paper format data resulting from this research program have been kept in a safe and secure location in the School of Electrical Engineering, Computing and Mathematical Sciences at Curtin University, Perth, Australia.

1.9 REFERENCES

[1] M. O. Donovan, A. Heffernan, S. Keena and N. Barry, "An Evaluation of Extending an Existing Substation Automation System using IEC 61850," 2022 57th International Universities Power Engineering Conference (UPEC), Istanbul, Turkey, 2022, pp. 1-6, doi: 10.1109/UPEC55022.2022.9917631.

[2] S. Kumar, A. Abu-Siada, N. Das and S. Islam, "Review of the Legacy and Future of IEC 61850 Protocols Encompassing Substation Automation System,", *Electronics* 2023,12,3345, https://doi.org/10.3390/electronics12153345

[3] V. Bhardwaj, M. I. Singh, S. Pardeshi and R. Arora, "A review on various standards for digital substation," 2014 International Conference on Green Computing Communication and Electrical Engineering (ICGCCEE), Coimbatore, India, 2014, pp. 1-5, doi: 10.1109/ICGCCEE.2014.6922364.

[4] S. Kumar, N. Das and S. Islam, "High Voltage Substation Automation and Protection System Based on IEC 61850," *2018 Australasian Universities Power Engineering Conference (AUPEC)*, Auckland, New Zealand, 2018, pp. 1-6, doi: 10.1109/AUPEC.2018.8757995.

[5] I. H. Lim and T. S. Sidhu, "Design of a Backup IED for IEC 61850-Based Substation," in *IEEE Transactions on Power Delivery*, vol. 28, no. 4, pp. 2048-2055, Oct. 2013, doi: 10.1109/TPWRD.2013.2258686. C. Hoga, "New Ethernet Technologies for Substation Automation", Powertech 2007, Lusanne, AB, Canada.

[6] IEC61850-5: Communication requirements for functions and device models

[7] M. Goraj and R. Harada, "Migration paths for IEC 61850 substation communication networks towards superb redundancy based on hybrid PRP and HSR topologies", DPSP, 2012, IET Conference.

[8] T. S. Sidhu, S. Injeti, M. G. Kanabar, and P. P. Parikh, "Packet scheduling of GOOSE messages in IEC 61850 based substation intelligent electronic devices (IEDs)," in *Power and Energy Society General Meeting, 2010 IEEE*, 2010, pp. 1-8.

[9] L. Andersson, C. Brunner, and F. Engler, "Substation automation based on IEC 61850 with new process-close technologies," in *Power Tech Conference Proceedings, 2003 IEEE Bologna*, 2003, p. 6 pp. Vol.2.

[10] C. Brunner, "The Impact of IEC 61850 on Protection," in Developments in Power System Protection, 2008. DPSP 2008. IET 9th International Conference on, 2008, pp. 14-19.

[11] N. Das, M. Wu, and S. Islam, "Comparison study of various factors affecting end-to-end delay in IEC 61850 substation communications using OPNET," in Universities Power Engineering Conference (AUPEC), 2012 22nd Australasian, 2012, pp. 1-5

[12] Kumar, N. Das, J. Muigai and S. Islam, "Performance evaluation of data transmission in a single and double bus network within the utility substation based on IEC 61850," *2014 IEEE PES General Meeting Conference & Exposition*, National Harbor, Washington, MD, USA, 2014, pp. 1-5, doi: 10.1109/PESGM.2014.6939273.

[13] S. Kumar, N. Das, S. Islam and A. Abu-Siada, "Toward a Substation Automation System Based on IEC 61850," 2021. Electronics 2021, 10, 310. https://doi.org/10.3390/electronics 1003031

[14] S. Kumar, N. Das, J. Muigai and S. Islam, "Performance evaluation of data transmission in a single and double bus network within the utility substation based on IEC 61850," 2014 IEEE PES General Meeting | Conference & Exposition, National Harbor, Washington, MD, USA, 2014, pp. 1-5, doi: 10.1109/PESGM.2014.6939273.

[15] V. Leitloff *et al*.,"Testing of IEC 61850 based functional protection chain using non-conventional instrument transformers and SAMU," *13th International Conference on Development in Power System Protection 2016 (DPSP)*, Edinburgh, UK, 2016, pp. 1-6, doi: 10.1049/cp.2016.0037.

[16] P. M. Kanabar, M. G. Kanabar, W. El-Khattam, T. S. Sidhu and A. Shami, "Evaluation of communication technologies for IEC 61850 based distribution automation system with distributed energy resources," *2009 IEEE Power & Energy Society General Meeting*, Calgary, AB, Canada, 2009, pp. 1-8, doi: 10.1109/PES.2009.5275787.

[17] D. M. E. Ingram, F. Steinhauser, C. Marinescu, R. R. Taylor, P. Schaub and D. A. Campbell, "Direct Evaluation of IEC 61850-9-2 Process Bus Network Performance," in *IEEE Transactions on Smart Grid*, vol. 3, no. 4, pp. 1853-1854, Dec. 2012, doi: 10.1109/TSG.2012.2205637.

[18] S. Kumar, N. Das and S. Islam, "Performance analysis of substation automation systems architecture based on IEC 61850," *2014 Australasian Universities Power Engineering Conference (AUPEC)*, WA, 2014, pp. 1-6, doi: 10.1109/AUPEC.2014.6966532

[19] S. Kumar, N. Das and S. Islam, "High performance communication redundancy in a digital substation based on IEC 62439-3 with a station bus configuration," 2015 Australasian Universities Power Engineering Conference (AUPEC), NSW, 2015, pp.1-5, doi: 10.1109/AUPEC.2015.7324838

[20] S. Kumar, N. Das and S. Islam, "Performance evaluation of a process bus architecture in a zone substation based on IEC 61850-9-2," 2015 IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC), QLD, 2015, pp. 1-5, doi: 10.1109/APPEEC.2015.7381017

[21] N. Liu, M. Panteli and P. A. Crossley, "Reliability evaluation of a substation automation system communication network based on IEC 61850," 12th IET International Conference on Developments in Power System Protection (DPSP 2014), Copenhagen, Denmark, 2014, pp. 1-6, doi: 10.1049/cp.2014.0057.

[22] N. Das, H. Modi and S. Islam, "Investigation on architectures for power system communications between substations using IEC 61850," 2014 Australasian Universities Power Engineering Conference (AUPEC), Perth, WA, Australia, 2014, pp. 1-6, doi: 10.1109/AUPEC.2014.6966480.

[23] D. Nojova, K. Ogudo and P. Umenne, "Modelling the IEC 61850 and DNP3 Protocol Using OPNET in an Electrical Substation Communication Network," 2022 International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems (icABCD), Durban, South Africa, 2022, pp. 1-7, doi: 10.1109/icABCD54961.2022.9856151.

[24] D. M. E. Ingram, P. Schaub, R. R. Taylor and D. A. Campbell, "System-Level Tests of Transformer Differential Protection Using an IEC 61850 Process Bus," in *IEEE Transactions on Power Delivery*, vol. 29, no. 3, pp. 1382-1389, June 2014, doi: 10.1109/TPWRD.2013.2291789

[25] H. Heine, P. Guenther and F. Becker, "New non-conventional instrument transformer (NCIT) - a future technology in gas insulated switchgear," 2016 IEEE/PES Transmission and Distribution Conference and Exposition (T&D), Dallas, TX, USA, 2016, pp. 1-5, doi: 10.1109/TDC.2016.7519939.

[26] Chatrefou, Dupraz and Montillet, "Interoperability Between Non-Conventional Instrument Transformers (NCIT) and Intelligent Electronic Devices (IDE)," *2005/2006*

IEEE/PES Transmission and Distribution Conference and Exhibition, Dallas, TX, USA, 2006, pp. 1274-1279, doi: 10.1109/TDC.2006.1668694.

[27] Zhang, Z. Cai, X. Li and R. He, "Propagation delay measurement and compensation for sampled value synchronization in a smart substation," in CSEE Journal of Power and Energy Systems, vol. 3, no. 2, pp. 196-202, June 2017, doi: 10.17775/CSEEJPES.2017.0024.

[28] L. Xu, H. Li and P. Mohapatra, "Assessments and comparisons of IEDs functionality and performance for both HSR and PRP configurations under laboratory setup and tests," *15th International Conference on Developments in Power System Protection (DPSP 2020)*, Liverpool, UK, 2020, pp. 1-6, doi: 10.1049/cp.2020.0138.

[29] J. Liu, Y. Li, X. Li, H. Lyu, G. Yang and J. Wen, "Design and Implementation of Delay Measurement in PRP and HSR RedBox," *2019 IEEE 2nd International Conference on Electronics Technology (ICET)*, Chengdu, China, 2019, pp. 45-50, doi: 10.1109/ELTECH.2019.8839567.

[30] R. C. Bernardino, C. M. Martins, P. S. Pereira, G. E. Lourenço and P. S. P. Junior, "Link redundancy in the process bus according to IEC 61850 ED.2: experience with RSTP, PRP and HSR protocols,"*16th International Conference on Developments in Power System Protection (DPSP 2022)*, Hybrid Conference, Newcastle, UK, 2022, pp. 164-169, doi: 10.1049/icp.2022.0931.

[31] M. Goraj and R. Harada, "Migration paths for IEC 61850 substation communication networks towards superb redundancy based on hybrid PRP and HSR topologies," *11th IET International Conference on Developments in Power Systems Protection (DPSP 2012)*, Birmingham, UK, 2012, pp. 1-6, doi: 10.1049/cp.2012.0055

[32] V. Dehalwar, A. Kalam and A. Zayegh, "Infrastructure for real-time communication in smart grid," *2014 Saudi Arabia Smart Grid Conference (SASG)*, Jeddah, Saudi Arabia, 2014, pp. 1-4, doi: 10.1109/SASG.2014.7274281.

CHAPTER 2:

MOTIVATION TO ADOPT IEC 61850 IN SUBSTATION AUTOMATION SYSTEMS

2.1 INTRODUCTION

Reliable communication between the field devices and the local or remote-control station are the key feature in a modern substation automation system (SAS). Traditionally, utilities have deployed MODBUS, PROFIBUS, IEC 60870, DNP3, and TCP/IP protocols to exchange data between field equipment and control room. With the advance of digital technologies and application of Ethernet and fibre optics (FO) in the secondary system, the SAS has undergone a paradigm change in the communication protocol leveraging on IEC 61850 standard [1]. This chapter presents a comprehensive comparison of data communication using conventional and digital substation protocols. This comparison reveals the superiority of IEC 61850 protocol due to its multiple advantages, which facilitates its application in the future SAS. The feasibility of implementation IEC 61850 protocol is verified in a digital lab using IEDs, MU, managed switches, and NCIT. Latencies while transporting digital data packets over an Ethernet network to various nodes were simulated using an optimized network engineering tool (OPNET). Results attest that IEC 61850 protocol offers better features than the conventional ones.

2.2 CONVENTIONAL PROTOCOLS

Fault identification and isolation of power systems feeders have been the key features of a smart protection system. Whether it be conventional or digital, the ultimate objective of an SAS is to help the operator carry out control, measurement, availability and condition monitoring of the trip circuit, and record readings while providing real-time information of circuit parameters when interrogated by a human-machine interface (HMI) device. Conventional communication protocols suffer from inefficiency of communication, which could be attributed to many factors as enumerated below [2]:

- slow data exchange resulting from noncompliance with the old equipment due to firmware or software incompatibility with an advanced digital secondary system,
- huge effort to re-engineer and reset relays,
- high chance of errors and failures,

- shutdown constraints,
- complex diagnostics,
- technical constraints to upgrade to a newer version.

While a number of communication protocols have been introduced in the last two decades in utilities and industrial substations, all were developed such that they are fully compatible with other existing operational equipment in the system. An analysis has been made of a scenario of a fault in an 11-kV High Voltage (HV) circuit breaker (CB) manufactured by vendor-A triggering an inter-trip of upstream CB of vendor-B. The control and command of these protection equipment is either done from local control centre or remotely over a DNP3 or legacy protocol.

Fig. 2.1 shows a typical a schematic diagram of a conventional communication protocol set-up in DNP3 protocol mode. In this figure, the user at the control room sends an OPEN command to add high voltage (HV) incomer circuit breaker in substation-A. This trip command to OPEN the circuit breaker downstream is cascaded to an upstream substation B OPEN, over a long transmission line using DNP3 protocol. However, these traditional communication modes suffer from a few shortcomings. For example, the DNP3 method of communication based on IEEE 1379-2000 exhibits unreliable security and is prone to hacking. Moreover, this protocol is slow to carry data packets when compared with the digital communication protocols. One of the main shortcomings of DNP3 protocol is its lack of interoperability capabilities [3].

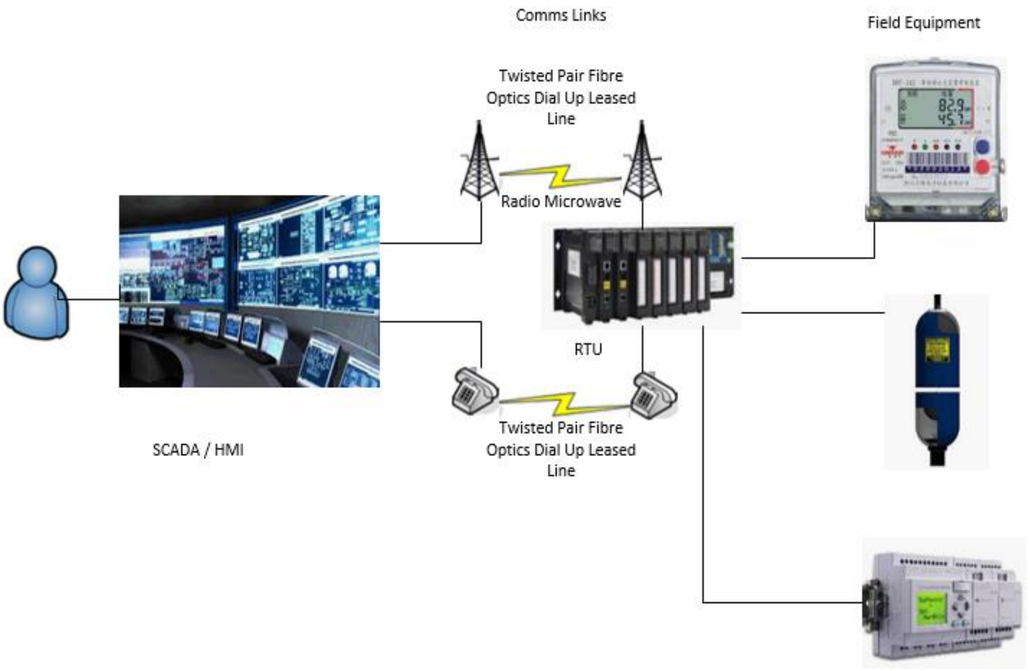

Comms Links
Field Equipment
Twisted Pair Fibre Optics Dial Up Leased Line
Radio Microwave
RTU
SCADA / HMI
Twisted Pair Fibre Optics Dial Up Leased Line

Fig. 2.1. Communication protocol – DNP3 [4].

2.2.1 Modbus

This protocol was established in 1979 for the use in Programmable Logic Controller (PLC) by Schneider Electric. This protocol is used mainly in industrial devices. It is user-friendly and has lesser restrictions when compared to other equivalent protocols. It leverages on serial, Ethernet or internet protocols of data exchange from one device to multiple devices in a master-slave architecture. The query and response message modes have been exhibited in Fig. 2.2 with device addresses, function codes, query data, response data and error check coming from the master device that is responded to promptly by the slave device [5].

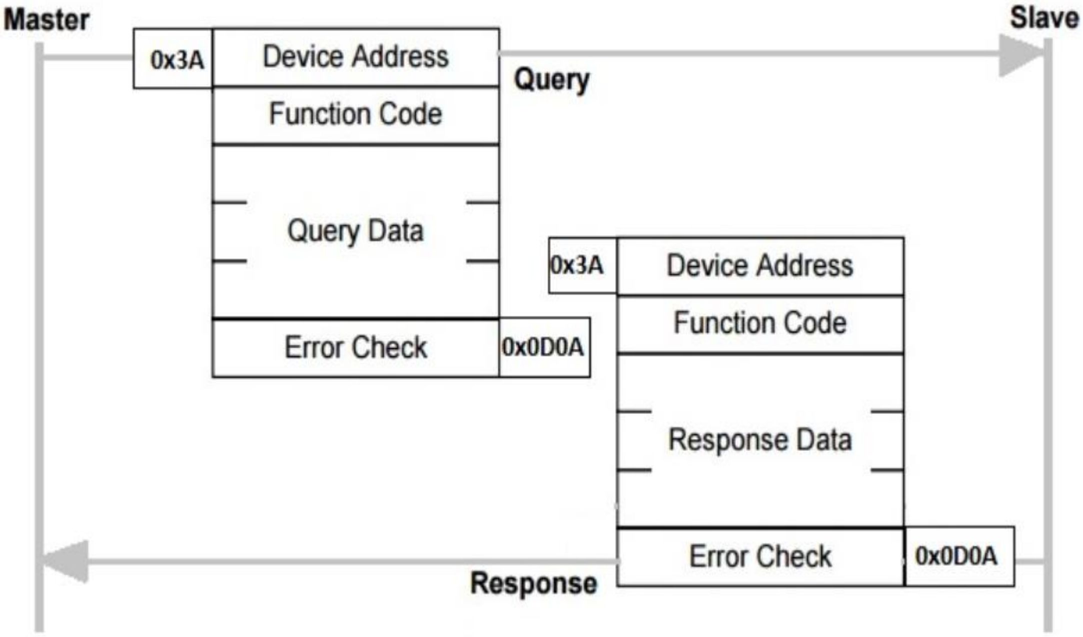


Fig. 2.2. Master-Slave architecture of communication of a MODBUS protocol [6].

Automation is achieved by riding on Remote Terminal Unit (RTUs) and SCADA system. Each device communicating on MODBUS protocol is given a unique address linked with RS-232 and RS-485. The frames flowing in the network with below-mentioned versions use one of the addresses embedded in an Application Data Unit (ADU) or Protocol Data Unit (PDU). This protocol interfaces easily with other protocols which is an advantage of this protocol.

Few of the different MODBUS versions currently in use in the industry are MODBUS RTU, MODBUS ASC II, MODBUS TCP/IP, and MODBUS UDP.

There are certain limitations of this protocol including:

- It doesn’t have a set standard to define a data object for example there is no standard to define temperature range between 30 to 175 ^{0}C.

- It is a client-server mode of communication in which data cannot be obtained from an event handler or client by the field device.
- There is a restriction to the number of devices connected in one data link (maximum 247).
- Security of the network could be poor and easy to compromise a data link or intercept data.
- High latency and timing issues with packets.
- Large data are not supported and consume large bandwidth.
- Issues of interoperability are encountered.

2.2.2 Profibus

Profibus, also known as process field bus, was first implemented in 1989 by BMBF, German Department of Education and then taken over by Siemens. PROFIBUS is a part of IED 61158 which was implemented to communicate with field devices using bit serial interface mode. It connects, controls, and provides automation to encoders, sensors, and actuators using a single bus cable. Many of the field devices manufacturers agreed to have a common mode of process automation and hence decided to have a common communication protocol. However, it was found that the designed common mode of process communication was too difficult to handle devices of different manufacturers. This gave rise to PROFIBUS DP where DP represents Decentralized Peripherals. Profibus DP is the most commonly used amongst the PROFIBUS versions, the other one being PROFIBUS PA where PA represents process automation. PROFIBUS DP is a faster communication protocol than PROFIBUS PA, which is mainly used in hazardous areas. It limits an explosive condition even if there is a malfunction in the process condition and its hardware confirms to IEC 61159-2. PROFIBUS PA could be networked with PROFIBUS DP using a linked equipment.

The main limitations of PROFIBUS are [7]:

- the data transmission rate is around 31.25 kbits/s only,
- if the process parameters change very rapidly the speed of data transfer may not be able to cope up and could lead to reading errors,
- lack of interest by the manufacturers to create devices that are compatible with this protocol,
- speed of communication of data packets is approx. 9-12 megabits/sec which is much slower in modern age of Ethernet and FO technology.

It is worth noting that PROFIBUS is different from PROFINET which is a different protocol.

2.2.3 Profinet

PROFINET or process field network is an industry field standard that uses Ethernet to communicate and deliver data under restricted time constraint. This mode of communication is supported by PROFIBUS having headquarters in Germany and deemed as a successor to PROFIBUS in the Hanover fair in 2008 [8].

PROFINET follows IEC 61784-2 standard that has been subdivided into Conformance class A, Conformance class B, Conformance class C, and Conformance class D.

PROFINET network is used with an IO Controller/Network/Device that works with PLCs. It is widely used in a process safety network which analyses safety, availability; security is of immense importance. It is a suitable device where redundancy in process automation is required. It also provides media redundancies with switching time less than 50ms. PROFIBUS sends two data packets in opposite directions as it would be in case of a High-Speed Seamless Redundancy (HSR) topology. PROFINET has a device driver called PROFIBUS drive that was developed in 1990s by PROFINET and PROFIBUS, which cover from the simplest to the most complex device drives. Using this protocol, a user could link up various devices in the process automation network and derive benefit by checking level, temperature, flow rate, valves, and actuators. Different versions of PROFINET are categorised as Class A, B, C, and D.

The limitations of PROFINET versions are:

- Data exchange is difficult using Ethernet wires based on 100base Tx or 100base Fx.
- Extension and buffer devices are required to establish data exchange amongst different version creating latency in data transfer.
- Declining acceptability of PROFINET Component Base Automation since 2014.
- This protocol uses special twisted cable CAT5 that is difficult to source.

2.2.4 DNP3

This is by far the most popular communication protocol currently used by utilities and industries as a standalone protocol or with other legacy protocol. Designed in 1993 by GE-Harris in Canada, it provides user friendly support such as [9]:

- bit mapping while dealing with other devices
- reliable communication to and from field devices
- overcoming distortion emanating of electromagnetic induction
- providing error checking, link control and prioritization

- providing time synchronization
- having better bandwidth over other protocols
- being more robust and reliable than MODBUS and PROFIBUS and PROFINET
- providing time stamped data,
- an ability to provide data in multiple formats such as 12bit, 16bit, 32bit with or without flag etc.
- compatibility with IEC 60870-5.

Fig. 2.3 exhibits master-outstation mode of data exchange with master layer on left hand side which initiates a data transfer using its Application Layer. The Outstation Layer on the right hand side with Data Link Layer receives octets from the physical layers and checks for errors. All error free octets are then passed on to Applicaion Layer within the Outstation Layer. Similarly, Outstation Layer transmits octet back to Master Layer.

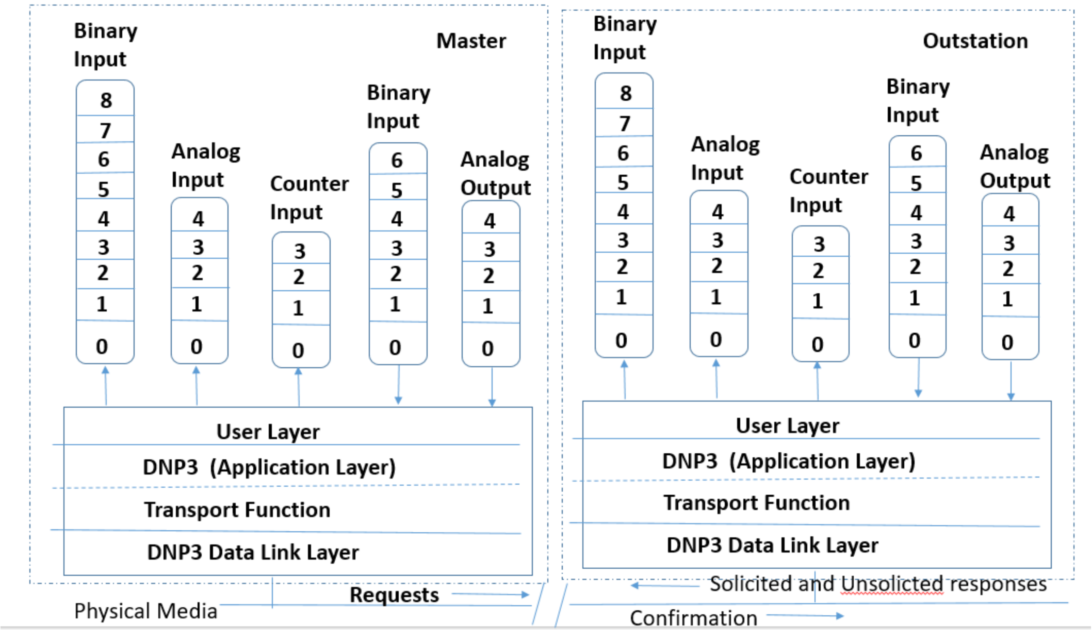


Fig 2.3. DNP 3 Outstation model [10].

On the flip side, DNP3 users have experienced a few disadvantages:

- complex diagnostics and fault finding in the network,
- interoperability is experiencing difficulty with new devices,
- field equipment encompassing complex secondary wirings makes troubleshooting difficult,
- it works mostly in low bandwidth,
- its wiring scheme is difficult to handle in the event of trouble shooting.

Meticulous planning and scheduling are required prior to commissioning. Wrong set-up could lead to delay in deciphering the fault and commissioning the system [11].

2.2.5 IEC 60870-5-103

This protocol is primarily used in utilities for power system monitoring and controlling of relays via Remote Terminal Units (RTUs) using fibre-optic cables, it was designed in 1997 and has its root in VDEW6 communication protocol of the 1980s. A VDEW6 device could work with IEC 60870-5-103 but not otherwise. It is a protocol used between devices in an electrical substation [12].

Some of the key features of this protocols are:

- no additional fee or hidden costs due to upgrade in version
- high performance and robust architecture while dealing at device level
- provides simple method to integrate to new devices
- it works with Linux system and uses it libraries
- multiple client-server simulation
- supports cyclic data transfer, redundancy, and file transfer
- this protocol supports “select before operate” file and “direct execute”.

Disadvantages of this protocol are:

- the speed rate of data transfer could slow down the large file upload as it has maximum speed 19200 baud.
- it is a slow transmission media due to maximum baud rate limit.
- it has limitations with certain specific manufacturers offering their devices for this protocol.
- it only works with its own series of standards i.e., with series on IEC 60870-5.
- interoperability is an issue with multivendor protection system.

2.2.6 TCP/IP

Invented in 1978, Transmission Control Protocol and Internet protocol (TCP/IP) bundle the information and transmit the data in an orderly manner. In short it is a language that computers speak and understand.

The information contained within the data packet determines its routing path. The IP section of packet focuses on logistics and guides the packet to its destination like a driver which operates and guides the vehicle to its destination from point A to point B. On the other hand, TCP checks for errors in the packet and if detected, it re-transmits the packet [13].

Some of the commonly addressed TCP/IP protocols that we encounter in our daily lives are HTTP, HTTPS, FTP, TCP/IP which consists of four layers namely, transport, internet, network access, application.

Advantages of TCP/IP are:

- it can be used in all types of computers using TCP/IP addresses such as static, dynamic & IP v6.
- it is industry standard model with good vendor support.
- devices can be interconnected in an heterogeneous network.
- all devices have IP address, and it is easy to detect them over a network.

A few issues with TCP/IP protocol are:

- it is not easy to remember the nomenclature and all abbreviated terms (example: Google uses 216.58.216.164 for our workplace computers and one doesn't have a clue of numbers that it uses).
- lower cost for installation and configuration and maintenance.
- cannot capture all dynamic or changing data packets in a computer system.
- TCP/IP are not in seen in one data packet. Multiple data packets are transmitted in the network. There is a possibility of nuisance tripping due to errors.
- vulnerability of data packets due to cyber threats and insecure mode of transportation.
- vulnerability of data packets due to cyber threats.

A summary of different legacy protocol with limitations and disadvantages of all conventional protocols is given in Table 2.1

Table 2.1 Limitations of conventional communication protocols.

Limitations	PROFIBUS	PROFINET	IEC 60870	DNP3	TCP/IP
Limitation in defining data object	Slow speed and low data transmission rate	Slow speed and many errors when Ethernet is used at 100base Tx	No encryption provided; easy to hack	Complexity in diagnostic and wiring of devices	Use of copper wires that makes communication slow
Restriction in number of client-server mode of communication	Cannot adjust to sudden change in process parameters	Errors due to latencies when the system is a little complicated	Incompatibility with multivendor devices	Works on low bandwidth	Point-to-point communication
High latency and timing issue	Limited communication due to more nodes	Declining acceptability of this protocol since 2014	Limited communication and no longer supported by vendors	High probability of hacking and disrupting at the nodes	Unable to carry digital packets
Incompatibility of multi-vendor equipment	Not many people have been trained on this protocol	On its phase-out stage and minimum vendor support available	Not many vendors manufacture devices to be compatible with this protocol	Device-to-device possible	Widely used protocol for point-to-point communication

2.2.7 IEC 61850 Protocol

With the advancement in technology and increasing shift towards digital automation in utility infrastructure due to issues with conventional protocols, IEC team assigned Technical Committee 57 in early 2001 to provide a guideline related to electrical power system [14]. This protocol features many advantages over legacy protocols such as:

- providing faster and reliable protection in less than 4ms
- minimising secondary copper wire and increasing FO wires in the network
- use of data frames related to MMS, GOOSE and SV
- faster communication, reliability in SAS and faster data transfer of events.

IEC 61850 have a series of standards which touch every aspect of a utility and industry electrical network. Fig. 2.4 shows a substation architecture having the three levels. The control and command originate at station bus level to control CB, identify CB status and its availability using IEDs present at bay level. At station bus the IED communicate horizontally while at process bus, field devices such as disconnectors, power transformers, current transformers (CT), voltage transformers (VT) etc. communicate with IEDs located in the control room through network peripherals such as switches, Red boxes, routers, and RTUs [15].

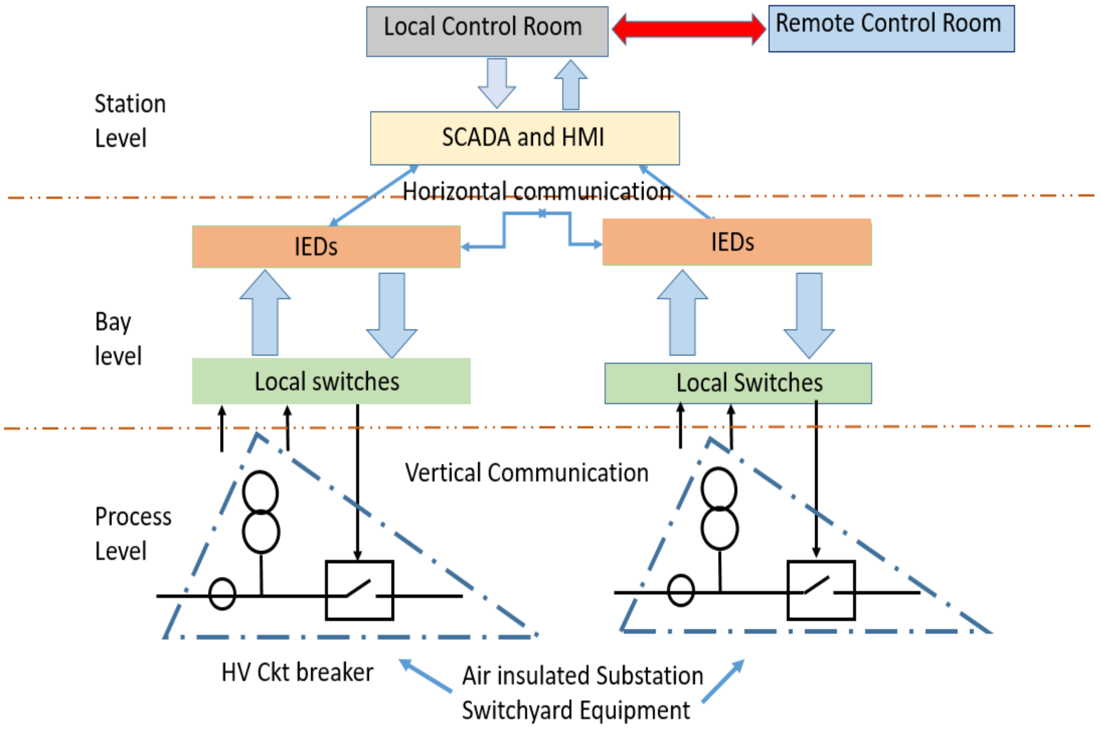


Fig. 2.4. Substation Automation Architecture for smart network [16].

IEC 61850 series of standards and their relevance can be summarized as shown in Fig. 2.5. There are about 10 main parts, and more standards are being set up on condition monitoring, asset management, and reliability extending the series [17].

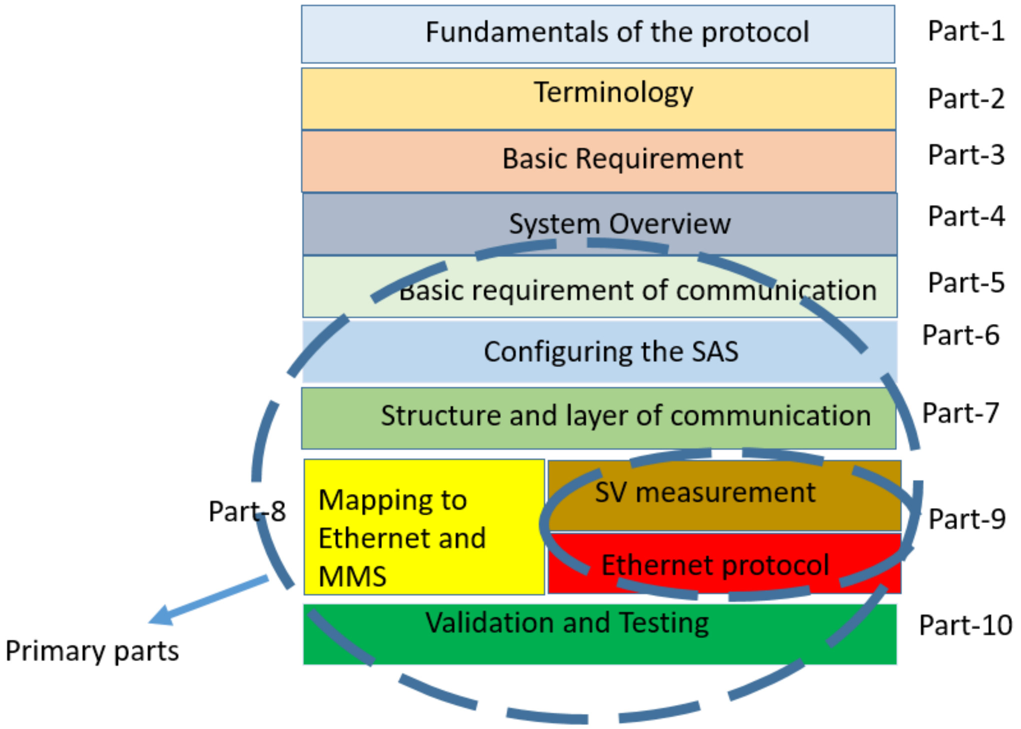
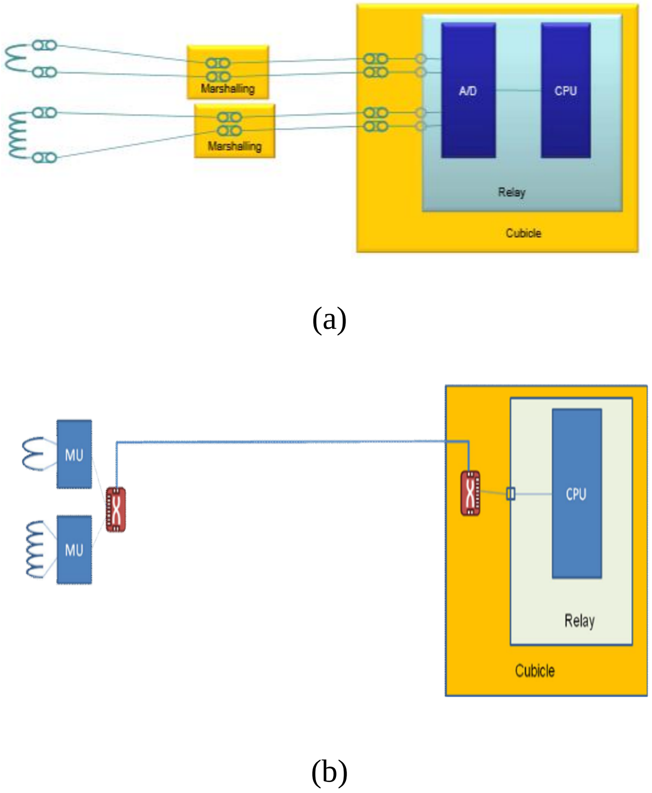


Fig. 2. 5. IEC 61850 series with special emphasis on specific topic [18].

Some utility operators in USA and Europe who have been running the IEC 61850 substations are of the opinion that it definitely saved them capital cost by 10 to 20% as opposed to similar conventional Air Insulated Substation (AIS) [19]. One of the Transgrid switching substations in New South Wales, Australia returned 18% savings to the utility operator encompassing smaller footprint of the switchboard, reduction in secondary cables to conduits, reliability in SAS [20].

Fig. 2.6 exhibits the complexity in cable wiring within a conventional topology as opposed to IEC 61850 topology. Comparison reveals that IEC 61850 offers [21]:

- ease of fault diagnostics
- reduction of arc flash and shock hazards due to the elimination of copper wires
- reducing the hazard of standing before medium voltage switchgear to interrogate IEDs
- lesser engineering and designing efforts, thereby reducing the man-hours to complete the project.



(a)

(b)

Figs. 2.6. (a) Multiple secondary wires from a set of field CT and VT (b) Reduction of copper wires to one fibre optic and Ethernet [22].

Another critical part of IEC 61850 topology has been communication with field equipment. The field devices such as CB and CITS feed the MU with analogue signals which are converted to SV frames and transmitted in digital packets to IEDs over an SAS network. Following the IEC 61850-5 guideline, the delay time of these frames arriving at the should be no more than 4 µs [23]. Fig. 2.7 depicts the functions of an MU which is basically an electronic box with analogue input and output cards. The digital output is fed to IEDs which provide huge benefit to operators by reducing secondary wiring from field devices and ease of diagnostics. The involvement of MU is an important part of the process bus architecture as IEC 61850-9-2 [24]. Some manufacturers keep the MU within the IED while few others prefer it to be stand-alone in the switchyard taking input from the secondary terminals of CITs. At Curtin University laboratory there are both types i.e., standalone (Alstom make) and inbuilt within the IED (ABB RET 615).

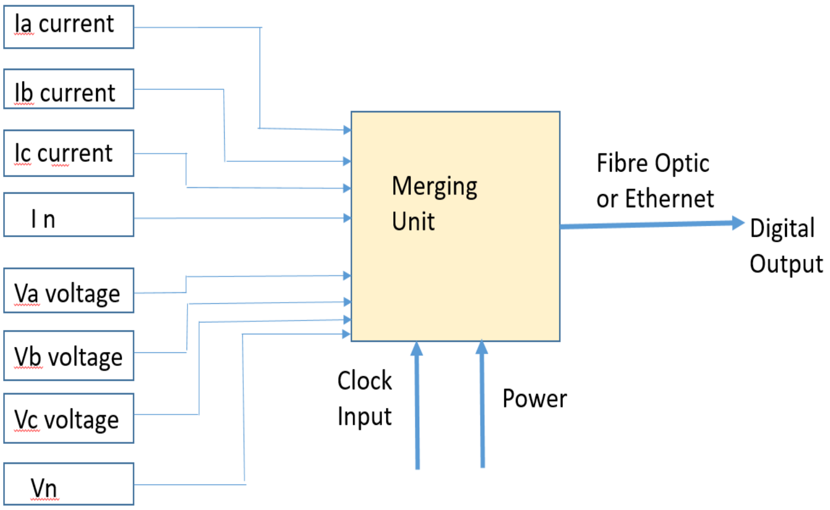


Fig. 2.7. Block diagram of an MU.

As mentioned previously, MU could work well with CITs but new sensor technology in the form of non-conventional instrument transformer (NCIT) could substitute for CITs. These sense high accuracy and data acquisition using SVs. The single-most advantage of NCIT is that they are immune to saturation due to lack of iron core and ferromagnetic material [26]. It is environmentally friendly and there is no requirement to fill NCIT with SF6 or insulating oil. Additionally, civil and structural design engineers have to deal with less footprint and weight of the primary plant. Introduction of NCIT has reduced errors as opposed to CITs which is vital in automation, protection and relaying from SAS environment perspective within a smart substation. It makes a fit case for retrofitment and making a huge impact on SAS protocol. However, in order to make it widely acceptable in the industry all scenarios need to be modelled and experimented in the laboratory [27]. Details of NCIT have been discussed in Chapter 5 with some experimental results.

Fig. 2.8 exhibits the wiring diagram of a real-life scenario with a lab based HV NCIT connection with an ABB make MU i.e., SMU 615. It is connected via a managed switch SEL to an IED i.e., Micom P545. Injection is carried out using Omicron kit CMC 356. HV NCIT converts to output voltage of 3mV to send it to SMU615. MU output is a digital frame of SV which is fed to a managed switch. A trip of the IED is initiated once the threshold of the IED is crossed, depending upon the byte size.

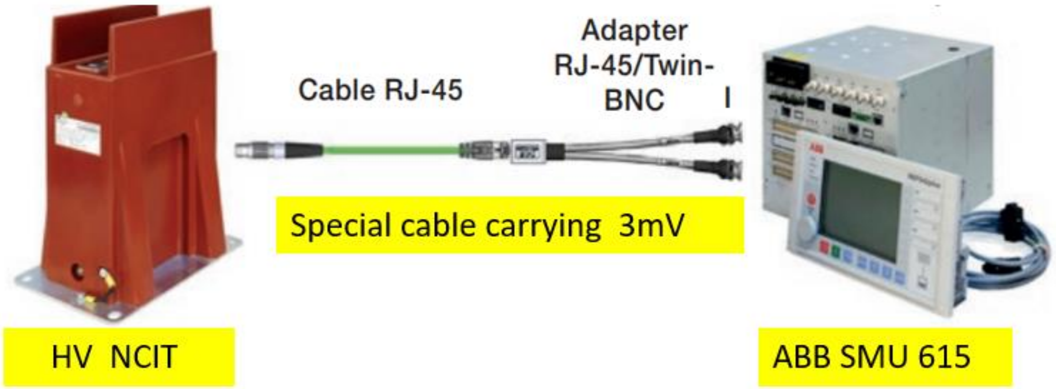
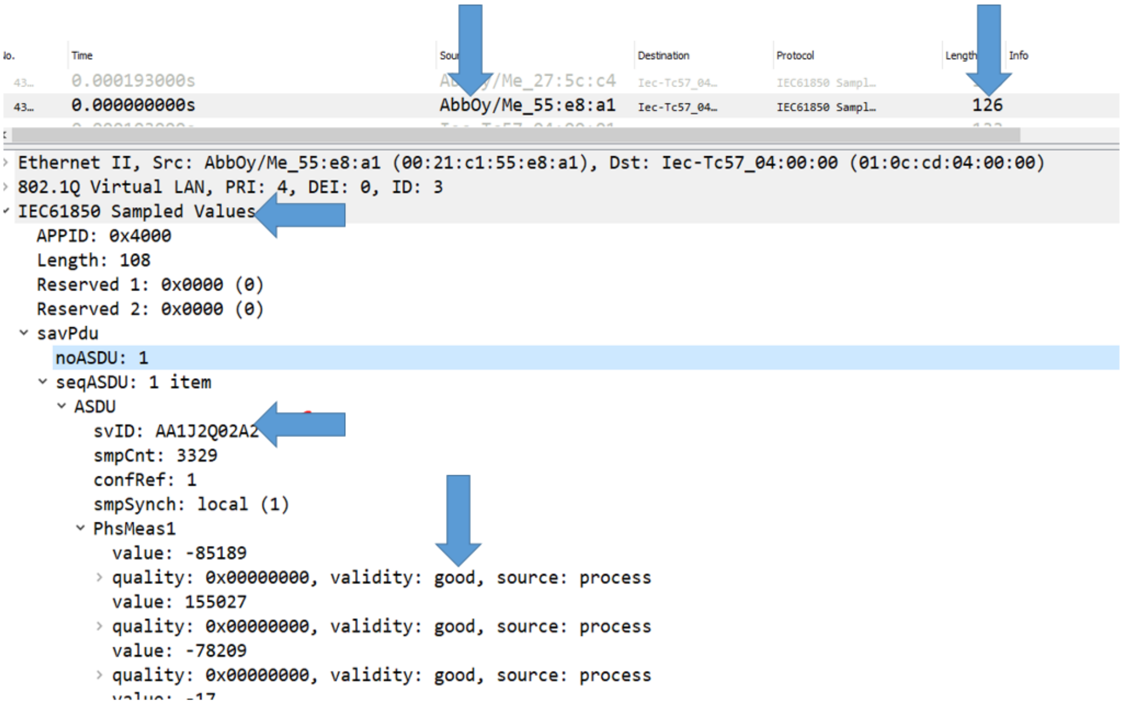


Fig. 2.8. Experimental connection of NCIT [29].

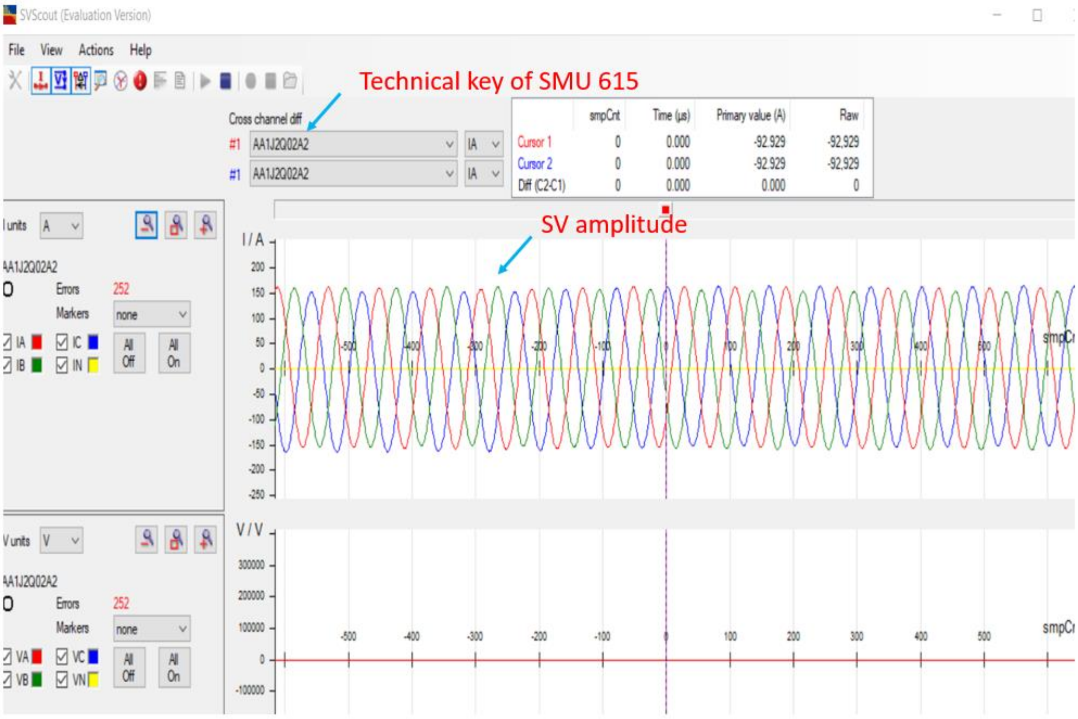
Fig. 2.9. is a screen shot captured from Wireshark which exhibits the signature of the SV packets representing SV packet serial 41 having a byte size of 126 ABB SMU 615 with a technical AA1JQO2A2 that is been subscribed by the IED MICOM P541. The SV frames are of good quality and there is no malformation of packets streaming in the network. The traffic of these packets follows IEEE 802.1Q standard and follows VLAN priority [30].



```
No.   Time           Sou...              Destination     Protocol          Length  Info
43…   0.000193000s   Ab…y/Me_27:5c:c4    Iec-Tc57_04…    IEC61850 Sampl…
43…   0.000000000s   AbbOy/Me_55:e8:a1   Iec-Tc57_04…    IEC61850 Sampl…   126

> Ethernet II, Src: AbbOy/Me_55:e8:a1 (00:21:c1:55:e8:a1), Dst: Iec-Tc57_04:00:00 (01:0c:cd:04:00:00)
> 802.1Q Virtual LAN, PRI: 4, DEI: 0, ID: 3
v IEC61850 Sampled Values
    APPID: 0x4000
    Length: 108
    Reserved 1: 0x0000 (0)
    Reserved 2: 0x0000 (0)
  v savPdu
      noASDU: 1
    v seqASDU: 1 item
      v ASDU
          svID: AA1J2Q02A2
          smpCnt: 3329
          confRef: 1
          smpSynch: local (1)
        v PhsMeas1
            value: -85189
          > quality: 0x00000000, validity: good, source: process
            value: 155027
          > quality: 0x00000000, validity: good, source: process
            value: -78209
          > quality: 0x00000000, validity: good, source: process
            value: -17
```

Fig. 2.9. Wireshark capture of SV out of an ABB MU.

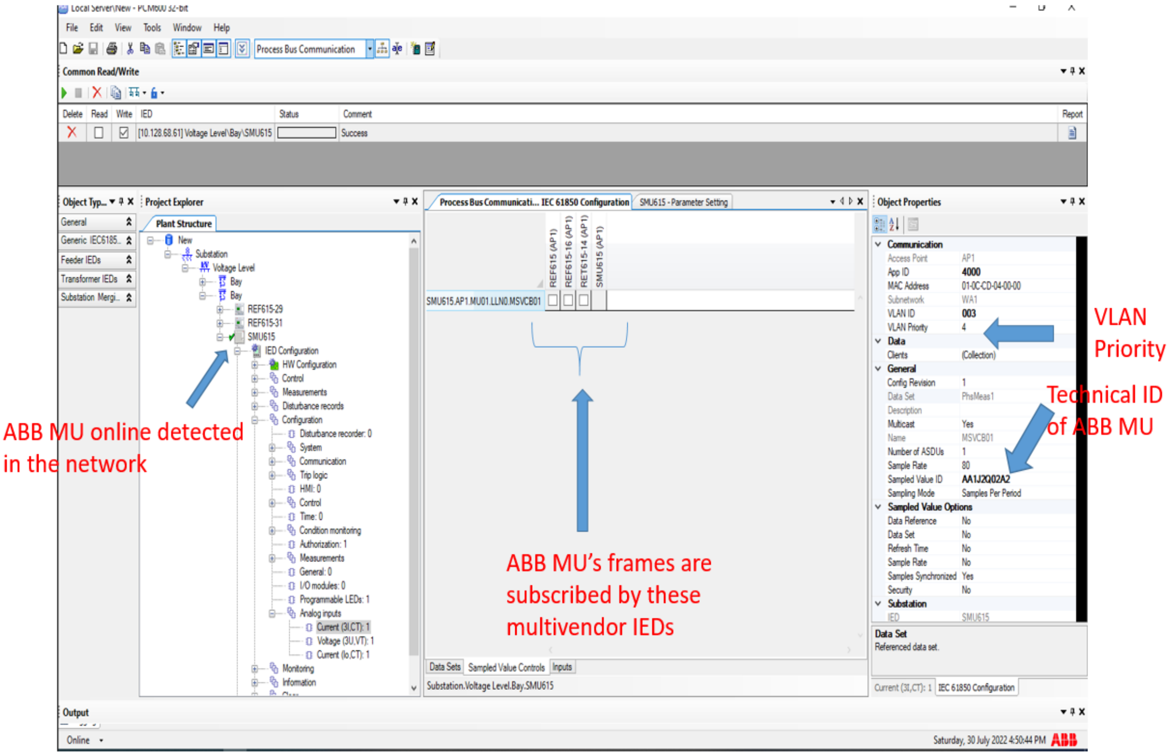
Fig. 2.10 exhibits a screenshot of SV amplitude detected using an Omicron SV Scout tool. This screenshot provides the MU technical key as detected by the omicron tool. All three phases of the input current are in balanced state and the SV stream is of good quality and doesn't represent short circuit.



	smpCnt	Time (µs)	Primary value (A)	Raw
Cursor 1	0	0.000	-92.929	-92,929
Cursor 2	0	0.000	-92.929	-92,929
Diff (C2-C1)	0	0.000	0.000	0

Fig. 2.10. Waveform of NCIT as seen through a managed SEL switch.

Fig. 2.11 is a screen dump PCM 600 tool that initiates changes in ABB SMU615. These settings are uploaded into Micom IED P545-M1 that subscribes this SV.


Local Server\New - PCM600 32-bit
File Edit View Tools Window Help
Process Bus Communication
Common Read/Write
Object Types
Project Explorer
Plant Structure
Process Bus Communicati... IEC 61850 Configuration
SMU615 - Parameter Setting
REF615 (AP1)
REF615-16 (AP1)
RET615-14 (AP1)
SMU615 (AP1)
SMU615.AP1.MU01.LLN0.MSVCB01
Object Properties
Data Sets Sampled Value Controls Inputs
Substation.Voltage Level.Bay.SMU615
Output
Online
Saturday, 30 July 2022 4:50:44 PM
ABB MU online detected in the network
ABB MU's frames are subscribed by these multivendor IEDs
VLAN Priority
Technical ID of ABB MU

Delete	Read	Write	IED	Status	Comment
☒	□	☑	[10.128.68.61] Voltage Level\Bay\SMU615		Success

Communication

Access Point	AP1
App ID	4000
MAC Address	01-0C-CD-04-00-00
Subnetwork	WA1
VLAN ID	003
VLAN Priority	4
Data	
Clients	(Collection)
General	
Config Revision	1
Data Set	PhsMeas1
Description	
Multicast	Yes
Name	MSVCB01
Number of ASDUs	1
Sample Rate	80
Sampled Value ID	AA1J2Q02A2
Sampling Mode	Samples Per Period
Sampled Value Options	
Data Reference	No
Data Set	No
Refresh Time	No
Sample Rate	No
Samples Synchronized	Yes
Security	No
Substation	
IED	SMU615

Data Set
Referenced data set.

Fig. 2.11 PCM600 (ABB Configurator) to configure SAMU.

2.3 TOOLS USED IN THE SUBSTATION AUTOMATION SYSTEM (SAS)

2.3.1 OPNET Modeller tool

Operational Network Technology (OPNET) is a simulation tool that has been extensively used in testing various network topologies as a desktop model. It provides flexibility and models complex network topologies used in digital Substation Automation System. This tool uses Graphical User Interface (GUI) to provide mathematical algorithms for computation. This simulation tool uses C++ language for writing codes and programming, and it has scalability and flexibility to model router/switches/server and IED [31].

Fig. 2.12 exhibits the OPNET model of 2 IEDs and 5 switches in a row. The parameter, process, node, and project editors set the profile of this linear topology to study the average Ethernet delay. The model assumed that the LAN speed was 100Mb/s at a burst of 1956 samples of SV frames.

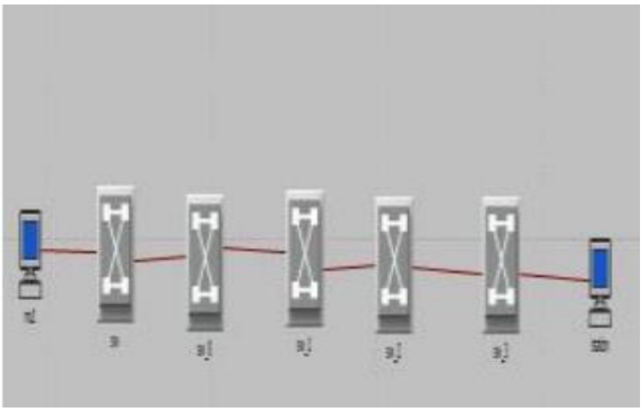


Fig. 2.12. OPNET model of switches and IED connected linearly.

Fig. 2.13 shows the performance of SV when LAN speed is 100 Mbps. This is simulated for data communication capability during a peak traffic of 400 kbps. The average Ethernet delay as the SV passes through different switches is of high importance as the transmission time is critical for SV data flow in a SAS network. As per IEC 61850-9-2, messages must be available during all operating conditions within the substation [32]. If the SV messages from field devices and NCIT to IEDs are delayed due to Ethernet traffic or errors in packets, it could seriously affect protection reliability. The blue colour characteristics in Fig. 2.13 show the Ethernet delay at the first switch and yellow characteristic is maximum Ethernet delay at the far end switch of SV packets. The last switch (yellow) experienced maximum delay as it passed via four other nodes.

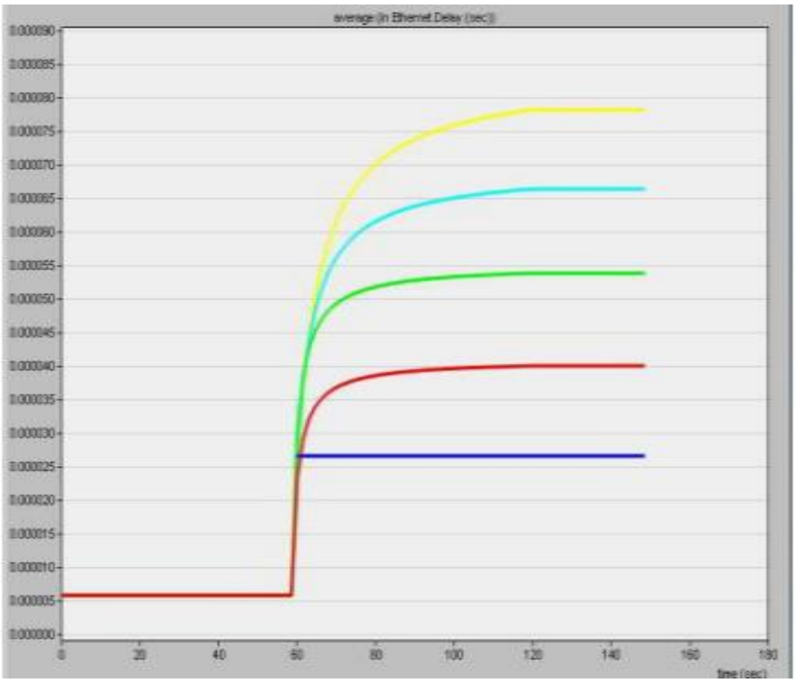


Fig. 2.13. Comparison of Ethernet delay of data packets for an SV burst through 5 switches.

It can be observed from Fig. 2.13 that the SV messages if subjected to propagation through more than one switch, performance degrades and the subscribing IED may mal-operate. The OPNET simulation is conducted using the parameters set in Table 2.2.

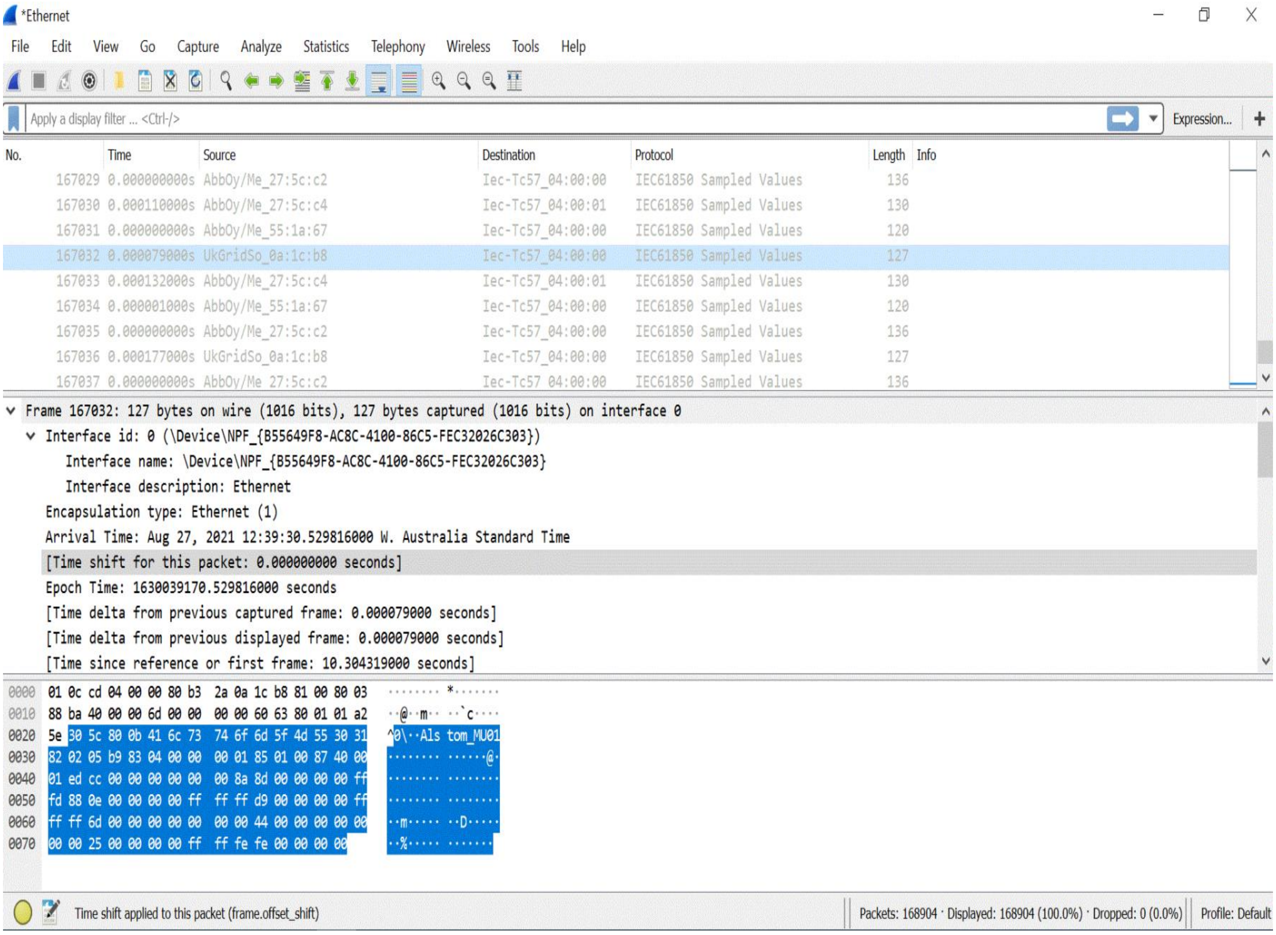
Table 2.2. Parameter setting for SV packets in an OPNET modeller.

Number of events	2,599,486
Average Speed (events/sec)	3,496950
Periodic repetition Time (ms)	1
Overall iteration (Hr)	1
Number of Discrete Event Simulation	5 entries
LAN speed (Mbps)	100
Speed (Kbps)	400
Ethernet delay at the last switch (Yellow) (µs)	653
Loss of SV (every second)	3
Rate of sampling (Hz)	4800

With the optimum speed as 100 Mbps with a rate of sampling at 4800-Hz, it can be safely assumed that the SV streams will reach the subscribing node without any loss provided the chain of nodes is less with no priority tagging. In summary, the above experiment indicates that the SV latencies in an Ethernet network is well within the acceptable limit of below 4 ms when tested with a LAN speed of 100 Mbps and sampling rate at 4800 sample/s.

2.3.2 Wireshark tool

Besides OPNET, another tool that has been used extensively across this thesis to monitor and analyse the network is Wireshark. This interactive network protocol analyser exhibits traffic movement, source, and origin of the packets. Wireshark tool supports all digital protocols such as IEC 61850 and IEC 62439-3 using .pCAP file extension to save and export data [33]. In order to capture the flow of traffic Wireshark needs to be connected to a network that enables it to capture all broadcast of unicast or multicast packets. One can apply filters and view the intended traffic such as Parallel Redundancy Protocol (PRP) or Sampled Values or GOOSE etc. as per the example in Fig. 2.14.



```
No.      Time         Source                 Destination         Protocol                 Length  Info
  167029 0.000000000s AbbOy/Me_27:5c:c2      Iec-Tc57_04:00:00   IEC61850 Sampled Values  136
  167030 0.000110000s AbbOy/Me_27:5c:c4      Iec-Tc57_04:00:01   IEC61850 Sampled Values  130
  167031 0.000000000s AbbOy/Me_55:1a:67      Iec-Tc57_04:00:00   IEC61850 Sampled Values  120
  167032 0.000079000s UkGridSo_0a:1c:b8      Iec-Tc57_04:00:00   IEC61850 Sampled Values  127
  167033 0.000132000s AbbOy/Me_27:5c:c4      Iec-Tc57_04:00:01   IEC61850 Sampled Values  130
  167034 0.000001000s AbbOy/Me_55:1a:67      Iec-Tc57_04:00:00   IEC61850 Sampled Values  120
  167035 0.000000000s AbbOy/Me_27:5c:c2      Iec-Tc57_04:00:00   IEC61850 Sampled Values  136
  167036 0.000177000s UkGridSo_0a:1c:b8      Iec-Tc57_04:00:00   IEC61850 Sampled Values  127
  167037 0.000000000s AbbOy/Me_27:5c:c2      Iec-Tc57_04:00:00   IEC61850 Sampled Values  136
```

```
v Frame 167032: 127 bytes on wire (1016 bits), 127 bytes captured (1016 bits) on interface 0
  v Interface id: 0 (\Device\NPF_{B55649F8-AC8C-4100-86C5-FEC32026C303})
      Interface name: \Device\NPF_{B55649F8-AC8C-4100-86C5-FEC32026C303}
      Interface description: Ethernet
    Encapsulation type: Ethernet (1)
    Arrival Time: Aug 27, 2021 12:39:30.529816000 W. Australia Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1630039170.529816000 seconds
    [Time delta from previous captured frame: 0.000079000 seconds]
    [Time delta from previous displayed frame: 0.000079000 seconds]
    [Time since reference or first frame: 10.304319000 seconds]
```

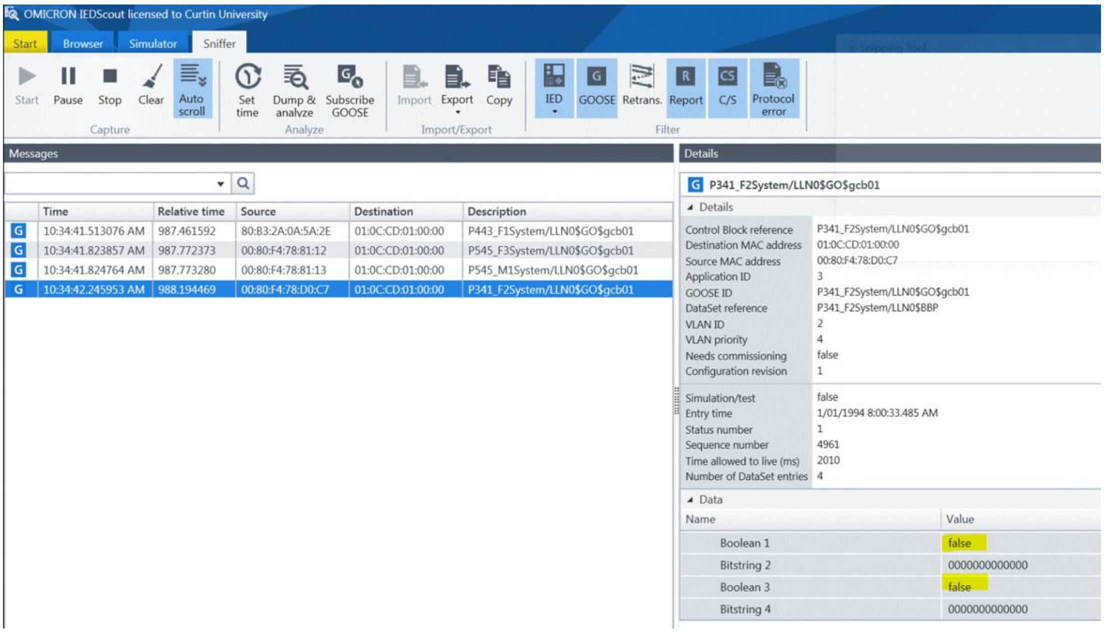
```
0000  01 0c cd 04 00 00 80 b3  2a 0a 1c b8 81 00 80 03   ········ *·······
0010  88 ba 40 00 00 6d 00 00  00 00 60 63 80 01 01 a2   ··@··m·· ··`c····
0020  5e 30 5c 80 0b 41 6c 73  74 6f 6d 5f 4d 55 30 31   ^0\··Als tom_MU01
0030  82 02 05 b9 83 04 00 00  00 01 85 01 00 87 40 00   ········ ······@·
0040  01 ed cc 00 00 00 00 00  00 8a 8d 00 00 00 00 ff   ········ ········
0050  fd 88 0e 00 00 00 00 ff  ff ff d9 00 00 00 00 ff   ········ ········
0060  ff ff 6d 00 00 00 00 00  00 00 44 00 00 00 00 00   ··m····· ··D·····
0070  00 00 25 00 00 00 00 ff  ff fe fe 00 00 00 00      ··%····· ·······
```

Time shift applied to this packet (frame.offset_shift) | Packets: 168904 · Displayed: 168904 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

Fig. 2.14. Wireshark capture of a network traffic flow.

2.3.3 IED Scout tool

IED Scout is a tool designed by Omicronenergy. This tool provides comprehensive details about the IEDs and senses them if they are located in the network, and it identifies data nodes and data logic embedded in GOOSE packets. It gives source and destination information to the network operator along with the byte size of the packet. It allows status change from FALSE to TRUE as indicated in Fig. 2. 15 and Fig. 2.16. The status before injection begins was FALSE while after the injection when the IED operated became TRUE. IED Scout further gives the status of managed switched ports whether the priority is for allowing GOOSE or SV along with date and time stamping.



	Time	Relative time	Source	Destination	Description
G	10:34:41.513076 AM	987.461592	80:B3:2A:0A:5A:2E	01:0C:CD:01:00:00	P443_F1System/LLN0$GO$gcb01
G	10:34:41.823857 AM	987.772373	00:80:F4:78:81:12	01:0C:CD:01:00:00	P545_F3System/LLN0$GO$gcb01
G	10:34:41.824764 AM	987.773280	00:80:F4:78:81:13	01:0C:CD:01:00:00	P545_M1System/LLN0$GO$gcb01
G	10:34:42.245953 AM	988.194469	00:80:F4:78:D0:C7	01:0C:CD:01:00:00	P341_F2System/LLN0$GO$gcb01

G P341_F2System/LLN0$GO$gcb01

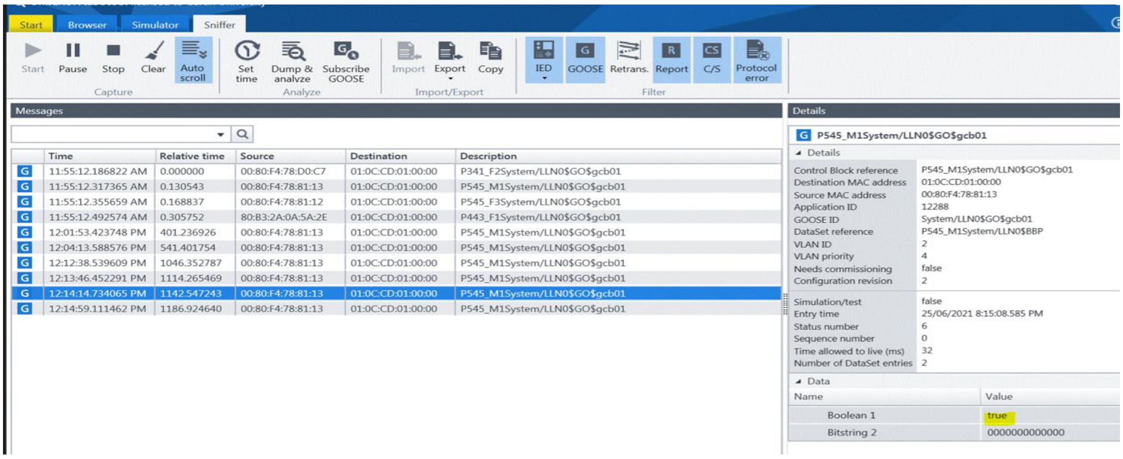
Details

Control Block reference	P341_F2System/LLN0$GO$gcb01
Destination MAC address	01:0C:CD:01:00:00
Source MAC address	00:80:F4:78:D0:C7
Application ID	3
GOOSE ID	P341_F2System/LLN0$GO$gcb01
DataSet reference	P341_F2System/LLN0$BBP
VLAN ID	2
VLAN priority	4
Needs commissioning	false
Configuration revision	1
Simulation/test	false
Entry time	1/01/1994 8:00:33.485 AM
Status number	1
Sequence number	4961
Time allowed to live (ms)	2010
Number of DataSet entries	4

Data

Name	Value
Boolean 1	false
Bitstring 2	0000000000000
Boolean 3	false
Bitstring 4	0000000000000

Fig. 2.15. IED Scout Tool used to capture IEDs in the network.



	Time	Relative time	Source	Destination	Description
G	11:55:12.186822 AM	0.000000	00:80:F4:78:D0:C7	01:0C:CD:01:00:00	P341_F2System/LLN0$GO$gcb01
G	11:55:12.317365 AM	0.130543	00:80:F4:78:81:13	01:0C:CD:01:00:00	P545_M1System/LLN0$GO$gcb01
G	11:55:12.355659 AM	0.168837	00:80:F4:78:81:12	01:0C:CD:01:00:00	P545_F3System/LLN0$GO$gcb01
G	11:55:12.492574 AM	0.305752	80:B3:2A:0A:5A:2E	01:0C:CD:01:00:00	P443_F1System/LLN0$GO$gcb01
G	12:01:53.423748 PM	401.236926	00:80:F4:78:81:13	01:0C:CD:01:00:00	P545_M1System/LLN0$GO$gcb01
G	12:04:13.588576 PM	541.401754	00:80:F4:78:81:13	01:0C:CD:01:00:00	P545_M1System/LLN0$GO$gcb01
G	12:12:38.539609 PM	1046.352787	00:80:F4:78:81:13	01:0C:CD:01:00:00	P545_M1System/LLN0$GO$gcb01
G	12:13:46.452291 PM	1114.265469	00:80:F4:78:81:13	01:0C:CD:01:00:00	P545_M1System/LLN0$GO$gcb01
G	12:14:14.734065 PM	1142.547243	00:80:F4:78:81:13	01:0C:CD:01:00:00	P545_M1System/LLN0$GO$gcb01
G	12:14:59.111462 PM	1186.924640	00:80:F4:78:81:13	01:0C:CD:01:00:00	P545_M1System/LLN0$GO$gcb01

G P545_M1System/LLN0$GO$gcb01

Details

Control Block reference	P545_M1System/LLN0$GO$gcb01
Destination MAC address	01:0C:CD:01:00:00
Source MAC address	00:80:F4:78:81:13
Application ID	12288
GOOSE ID	System/LLN0$GO$gcb01
DataSet reference	P545_M1System/LLN0$BBP
VLAN ID	2
VLAN priority	4
Needs commissioning	false
Configuration revision	2
Simulation/test	false
Entry time	25/06/2021 8:15:08.585 PM
Status number	6
Sequence number	0
Time allowed to live (ms)	32
Number of DataSet entries	2

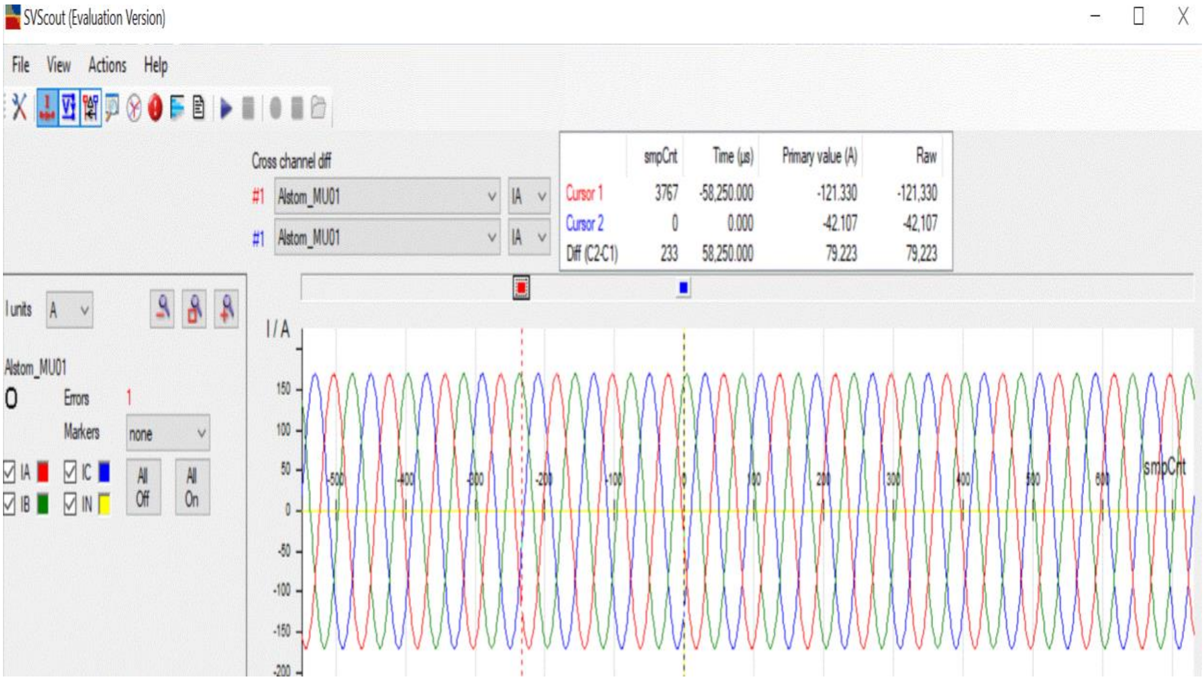
Data

Name	Value
Boolean 1	true
Bitstring 2	0000000000000

Fig. 2.16. IED Scout Tool used in highlighting the status change of the IED in the network.

2.3.4 SV Scout tool

SV Scout is another tool from Omicron Gmbh used in the experiments in this thesis to calculate the peak amplitude of current in the waveform and exhibit the MUs in the network. Once current is injected into the MU, a three-phase sinusoidal graph representing the injected current can be seen as in Fig. 2.17. SV scout enables the operator to understand the digital to analogue conversion.



	smpCnt	Time (µs)	Primary value (A)	Raw
Cursor 1	3767	-58,250.000	-121.330	-121,330
Cursor 2	0	0.000	-42.107	-42,107
Diff (C2-C1)	233	58,250.000	79.223	79,223

Fig. 2.17. SV Scout tool exhibiting the online IEDs.

2.4 CHAPTER SUMMARY

Traditional protocols such as MODBUS, PROFIBUS, PROFINET IEC 80870, DNP3 and TCP/IP suffer from client/server data exchange interoperability issues in addition to massive bundles of wires and termination points that complicate the secondary system wiring and diagnosis. On the contrary, advanced IEC 61850 protocol not only improves the topology architecture using Ethernet and FO wiring, that allows flow of digital data packets but also enhances reliability of the protection and automation within the HV substation.

IEC 61850 offers a comprehensive solution for SAS. It has the flexibility and versatility to amalgamate all aspects of substation events including protection, control, measurement, condition monitoring etc. In order to implement and install this communication protocol, all aspects of its features must be fully tested, and adaptability with legacy protocol needs to be proved.

This chapter highlights the advantage and disadvantages of various communication protocols. Furthermore, latency in the IEC 61850 model using an OPNET tool have been tested. Results indicate superior performance of IEC61850 over conventional protocols in terms of Average and Ethernet delays latencies when the nodes are too many and no priority has been assigned to frame circulation. Results attest the delay is minimum when the nodes are fewer and gradually increases when the SAS systems become complex with the number of switches increased. The following chapters have tested for different topologies and interoperability which have been a key issue in implementing IEC 61850 protocol in mass.

2.5 REFERENCES

[1] D. Nova, K. Ogudo and P. Umenne, "Modelling the IEC 61850 and DNP3 Protocol Using OPNET in an Electrical Substation Communication Network," in Proc. Of the *2022 International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems (icABCD), Durban, South Africa, 2022, pp. 1-7, doi: 10.1109/icABCD54961.2022.9856151.*

[2] T. S. Sidhu and Y. Yin, "Modelling and simulation performance evaluation of IEC 61850 based substation communication system", *IEEE Trans. On Power Del.,* vol. 22, no. 3, 2007.

[3] E. P. Vlasova, "Development and Research of a Model Using IEC Protocols for 110/6 kV Digital Substations," in Proc. Of the *2020 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon),* Vladivostok, Russia, 2020, pp. 1-4, doi: 10.1109/FarEastCon50210.2020.9271222.

[4] S. Mohagheghi, J. Stoupis and Z. Wang, "Communication protocols and networks for power systems-current status and future trends," in Proc. Of the *2009 IEEE/PES Power Systems Conference and Exposition*, Seattle, WA, USA, 2009, pp. 1-9, doi: 10.1109/PSCE.2009.4840174.

[5] J. Horalek, J. Matyska and V. Sobeslav, "Communication protocols in substation automation and IEC 61850 based proposal," in Proc. Of the *2013 IEEE 14th International Symposium on Computational Intelligence and Informatics (CINTI),* Budapest, Hungary, 2013, pp. 321-326, doi: 10.1109/CINTI.2013.6705214.

[6] A. Depari, P. Ferrari, A. Flammini, S. Rinaldi, E. Sisinni and A. Vezzoli, "On the use of PRIME PowerLine Communication in industrial applications: Modbus a first test case," in Proc. Of the *2013 IEEE International Instrumentation and Measurement Technology*

Conference (I2MTC), Minneapolis, MN, USA, 2013, pp. 587-592, doi: 10.1109/I2MTC.2013.6555484.

[7] Kyung-Chang Lee, Hyun-Hee Kim, Suk Lee and Hong-Hee Lee, "Communication delay properties in performance model of profibus token passing protocol," in Proc. Of the *7th Korea-Russia International Symposium on Science and Technology, Proceedings KORUS 2003. (IEEE Cat. No.03EX737),* Ulsan, Korea (South), 2003, pp. 433-439 vol. 2.

[8] UCA, "Implementation guideline for digital interface to instrument transformer using IEC 61850-9-2," UCA International User Group, Raleigh, NC, USA.

[9] M. Yang and G. Li, "Analysis of PROFINET IO Communication Protocol," in Proc. Of the *2014 Fourth International Conference on Instrumentation and Measurement, Computer, Communication and Control,* Harbin, China, 2014, pp. 945-949, doi: 10.1109/IMCCC.2014.199.

[10] K. Liu, X. Dong and Z. Bo, "Current Differential Protection Based On Non-Conventional Instrument Transformer and IEC 61850," in *proc. Of the 43rd Universities Power Engineering Conference 2008 (UPEC 2008),* 1~4 September 2008, Padova, Italy.

[11] DNP3:- "IEEE Standard for Electric Power Systems Communications-Distributed Network Protocol (DNP3)," in *IEEE Std 1815-2012 (Revision of IEEE Std 1815-2010)* , vol., no., pp.1-821, 10 Oct. 2012, doi: 10.1109/IEEESTD.2012.6327578.

[12] H. Yang, L. Cheng and M. C. Chuah, "Modelling DNP3 traffic characteristics of field devices in SCADA systems of the smart grid," in Proc. Of the *2017 Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES),* Pittsburgh, PA, USA, 2017, pp. 1-6, doi: 10.1109/MSCPES.2017.8064535

[13] B. Pham, C. Huff, P. E. Nick Vendittis, A. Smit, A. Stinskiy and S. Chanda, "Implementing Distributed Intelligence by Utilizing DNP3 Protocol for Distribution Automation Application," in Proc. Of the *2018 IEEE/PES Transmission and Distribution Conference and Exposition (T&D),* Denver, CO, USA, 2018, pp. 1-7, doi: 10.1109/TDC.2018.8440305.

[14] D. A. Poștovei, C. Bulac, I. Triștiu, B. Camachi, B. Kandamulla and V. Sanduleac, "Aspects of Data Models compatibility within Substation hybrid LANs," in Proc. Of the *2021 9th International Conference on Modern Power Systems (MPS),* Cluj-Napoca, Romania, 2021, pp. 1-6, doi: 10.1109/MPS52805.2021.9492585.

[15] R.K. Liao, Y.F. Ji and H. Li, "Optimized Design and Implementation of TCP/IP Software Architecture Based on Embedded System," in Proc. Of the *2006 International*

Conference on Machine Learning and Cybernetics, Dalian, China, 2006, pp. 590-594, doi: 10.1109/ICMLC.2006.258382.

[16] N. Das, W. Ma and S. Islam, “Comparison study of various factors affecting end to end delay in IEC 61850 substation communication using OPNET,” in proc. Of the Australasian Power Engineering Conferences 2012 (AUPEC 2012), Bali, Indonesia, 26-29 Sept. 2012.

[17] N. Paviya, A. Varghese, M. Boucherit, P. Newman and P. Diemer, “IEC 61850 Process bus application in Energinet Denmark,” in proc. Of the 12th IET International Conference Developments in Power System Protection (DPSP 2014), Copenhagen, Denmark, 2014.

[18] J. Schmid and M. Schumarcher, “IEC 61850 Merging Unit For The Universal Connection of Conventional and Non-Conventional Instrument Transformers,” Cigre, AS-306, 2008.

[19] M. Kanabar, “Investigation Performance and Reliability of Process Bus Networks for Digital Protective Relaying,” The University of Western Ontario, The School of Graduate and Postdoctoral Studies, PhD thesis, 2007.

[20] D. M. E. Ingram, P. Schaub, R. R. Taylor and D. A. Campbell, “Performance analysis of IEC 61850 Sampled Value process bus networks,” *IEEE Trans. On Industrial Informatics*, vol. 9, issue no. 3, 2013.

[21] R, Moore and M. Goraj, “New Paradigm of Smart Transmission Substation-Practical Experience With Ethernet Based Fibre Optic Switchyard at 500 Kilovolts,” ISGT Europe, 2011.

[22] S. Kumar, N. Das and S. Islam, “High Voltage Substation Automation and Protection System Based on IEC 61850,” *2018 Australasian Universities Power Engineering Conference (AUPEC)*, New Zealand, 2018, pp. 1-6, doi: 10.1109/AUPEC.2018.8757995.

[23] M. Mekkanen, E. Antila, R. Virrankpski and M. Elmusarati, “Using OPNET To Model and EVALUATE the MU Performance Based on IEC 61850-9-2LE,” AASRI International Conference on Industrial Electronics Applications (IEA), 2015.

[24] L. Yiqing, G. Houlei, X. Mingjiang, W. Xin, W. Peng and Z. Chunsheng, “Performance Testing Of Complete Digital Relays Based on ATP-EMTP and IEC61850-9-2,” DRPT, Pages 83-87, Shandong, 2011.

[25] G. Igarashi, J. C. Santos, S. N. Junior and E. L. Pellini, “Development Of A Digital Optical Instrument Transformer With Process Bus Interface According to IEC 6150-9-2 standard,” ISGT, Pages 893-897, Latin America, 2015.

[26] OPNET Modeller–OPNET Technologies, [Online]. Available in the weblink: *http://www.opnet.com*.

[27] A. Araujo, J. Lazaro, A. Astaloa, A. Zuloaga and N. Moeira, "Duplicate and Circulating Frames Discard Methods for PRP and HSR (IEC 62439-3)," in Proc. Of the 2013 Electricity Distribution, CIRED 2013, DOI 10.1049/cp.2013.0836, Stockholm, Sweden.

[28] L. J. Kovic, "Innovative Non-convention Current Transformer for Advanced Substation Design and Improved Substation Performance," Paper A3-208, 42nd Cigre session 2008, Paris, France.

[29] IEC 61850-9-2 2004, Communication Networks and Systems in Substations –Part 9-2: Specific Communication System mapping (SCSM) – Sampled Values Over ISO/IEC 802-3, First Edn., May 2005.

[30] IEC 61850-9-2 LE, Implementation Guideline for Digital Interface to Instrument Transformers Using IEC 61850-9-2, UCA International Users Group.

[31] V. Leitloff *et al*., "Testing of IEC 61850 based functional protection chain using non-conventional instrument transformers and SAMU," in Proc. Of the *13th International Conference on Development in Power System Protection 2016 (DPSP)*, Edinburgh, UK, 2016, pp. 1-6, doi: 10.1049/cp.2016.0037.

[32] IEEE 802.1Q: networking standard that supports virtual local area networking (VLANs) on an IEEE 802.3 Ethernet network.

[33] S. Kumar, N. Das and S. Islam, "Performance analysis of substation automation systems architecture based on IEC 61850," in Proc. Of the *2014 Australasian Universities Power Engineering Conference (AUPEC)*, Perth, WA, 2014, pp. 1-6, doi: 10.1109/AUPEC.2014.6966532.

CHAPTER 3:

TOPOLOGIES IN DIGITAL SUSTATION AUTOMATION SYSTEMS

3.1 INTRODUCTION

With the number of advantages seen in it, IEC 61850 protocol is steadily gaining popularity and acceptance amongst utilities and industries. With flexibility to expand, ease of diagnostics and reliability in protection, adaptability to communicate with legacy equipment with modification, this protocol is the future of substation world [1]. With faster data and frame transfer, the protection scheme is becoming more reliable and having fewer copper wires to deal with. However, due to proprietary issues, latencies and delays, and clogging at nodes, it is still a few years away from being fully acceptable to operators. Communication delays in transferring packets could complicate the secondary protection scheme and throw up interoperability challenges. To address these problems, end-users need to follow the IEC 61850-8 and IEC 61850-9 standards and test it rigorously with multi-vendor equipment [2]. With massive bursts of data and frames circulation in an Ethernet network, the right topology to adhere is very important [3]. Additionally, whether the SAS shall embrace GOOSE or SV for CB open-close or Isolator disconnection-close or operate on SV signals from CITs does have an impact on the IEC 61850 protocol. Byte size and speed at which frames travel determine the closing, tripping, latching etc. which in turn determines the success of the automation scheme, while non-critical bytes such as control, monitoring and measurements provide vital information to the end-user and decisions are taken accordingly. However, the challenge remains to allow priority messages to pass through in the network while placing non-critical messages in the bottom of the queue [4]. All these critical and non-critical frames could be rendered useless due to single point failure. Hence, testing and validation of network performance in different topologies with all nodes are of high importance particularly with multivendor equipment in play in different topologies.

3.1.1 Background of IEC 61850

Sometime in 2002 the International Technical Committee (IEC) with the support of Technical Committee TC57 produced a series of standards called IEC 61850. The idea of producing these standards was to provide a common platform of communication between field and control room smart devices with better engineering practices and less complexity in fault diagnostics. Data models of each intelligent devices such as instrument transformers, circuit breakers (CB) etc. were created and were mapped into different protocols based on manufacturing message specification (MMS), GOOSE and SV in a SAS network. These protocols can also work in tandem with legacy protocols such as Transmission Control Protocol (TCP) and Internet Protocol (IP). A suite of IEC 61850 standards published currently are located under the hyperlink which guides users to configure, install, test, and commission digital Substation Automation Scheme (SAS) "***https://en.wikipedia.org./wiki/IEC_61850*** " [5].

3.2 THREE FUNCTION LEVELS IN A DIGITAL SUBSTATION

A digital substation has three function levels as shown in Fig. 3.1. The bottommost level is process level, the middle one, bay level and the uppermost level is station level [6]. All field equipment sits at process level and communicates vertically with station level IED and control room. These smart devices communicate using SV frames over an Ethernet-based Local Area Network (LAN). SV manager devices scan the network continuously and look for mission-critical messages which follow IEEE 802.2Q priority in transmitting data packets [7]. At Bay level one can find smart devices such as IED and Switches; it can do horizontal and vertical communication amongst IEDs and peripherals. Supervisory control and data acquisition (SCADA) and Human Machine Interface (HMI) sit at the top level in the hierarchy in an IEC 61850 digital substation. At station level, the control room commands opening and closing of CBs as well as monitoring different protocol such as MMS, GOOSE and SV flow in the SAS network [8]. IEC 61850 digital substation provides improved configuration, object-oriented data, easy representation of power system schemes, improved visibility of the data due to condition monitoring packets at periodic interval [9].

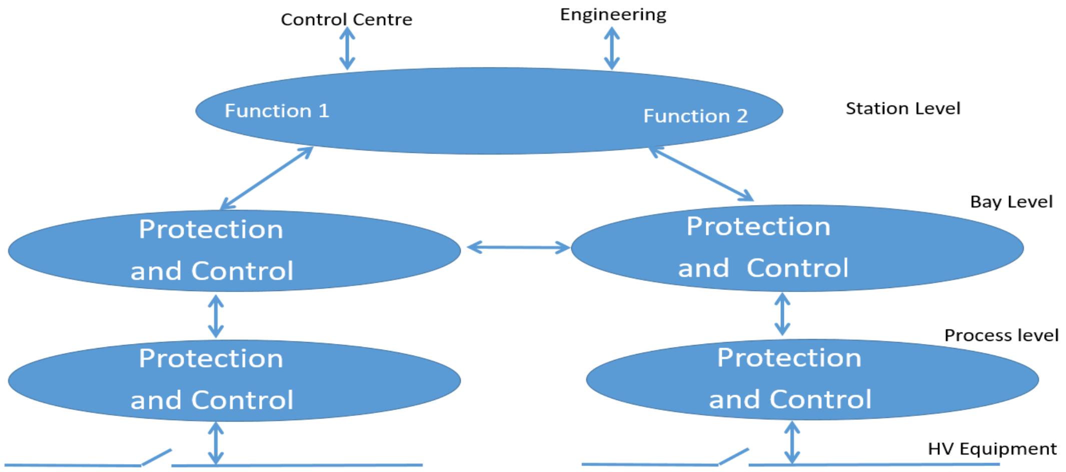


Fig. 3.1. Substation Automation System Interface Model [10].

The overall topology was modelled and tested for different topologies and at different LAN speed as shown in a later section.

3.3 ETHERNET ARCHITECTURES MODELLED IN OPNET

Desktop study of topologies allows the operator to understand the delay at the nodes and overall delay at the Ethernet network. At the Curtin University laboratory an OPNET simulation was carried out selecting a particular topology of a typical HV substation. Priority is allocated to a frame depending upon the byte size as stipulated in Table 3.1, extracted out of IEC61850-5. Highest priority is given to least byte size i.e. Type 1 [8].

Table 3.1. Criticality of messages.

Type of message	Event category	Priority	Byte size
Type 1	For Tripping the CB	5	50
Type 2	Interlock of CB	3	100
Type 3	Status of CB	2	150
Type 4	With SV and GOOSE	4	75
Type 5	Transmitting file settings	1	500 >

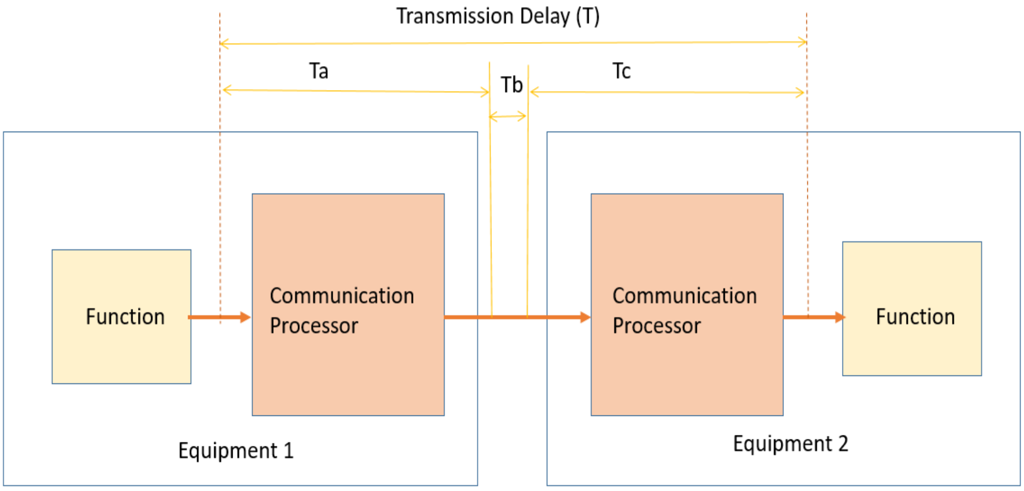
With the advent of digital substation and leveraging on communication protocol for substation automation, it is important to understand the shortcomings of having malformation or error in data packets consisting of GOOSE, SV, and MMS when frames are circulated and passed via

IEDs, switches, routers in an Ethernet and FO network with the aim to provide a superior, reliable, and stable network compared with the conventional protection. Digital protection provides better fault diagnostic in the fastest possible time with least effort in diagnostic. Hence the way in which a network is connected with Ethernet or FO plays an important role. However, several questions arise when a digital substation topology is considered, such as “How to design?” “How to maintain?” “How to perform condition monitor?” “How to ensure smooth flow of data packets without error and malformation?” and “What’s its vulnerability?” etc.

Topology selection in a digital infrastructure is of huge importance as it segregates Multi Media Systems (MMS), GOOSE and SV circulating in the same network without causing data clogging and data queuing. The design of the structure is such that it allows reliability of the information of data flow from publisher to subscriber without overloading the network. Where redundancy is required in digital protection scheme Parallel Redundancy Protocol (PRP) and High-speed Seamless Redundancy (HSR) is deployed. The other protocol, which is not so complicated but provides redundancy, High-Speed Seamless Redundancy (HSSR), is described in the following chapter. All the topologies could be designed as Station or Process bus. Process bus is preferred when the substation level is 66 kV or above in outdoor switchyard equipment using Virtual Local Area Network (VLAN). VLANs act like a gatekeeper separating SV, GOOSE and MMS passing via managed switches. The choice of Process bus or Station bus depends upon bus bar configuration i.e., double bus, single bus bar, breaker and half bus bar arrangement. Without compromising the protection scheme, it is recommended to have two main protections each having input/output for Process bus, protection IEDs and for communication network. As 11-kV, 22-kV and 33-kV level have IEDs mounted above the switchgear, it is wiser to have it as Station bus with GOOSE-controlled circuit breaker. Due to network performance and stricter regulatory requirement, PRP or double LAN is the preferred topology in utilities [10].

Most of the frame traffic that is circulating within a network has been channelized within a managed switch, to enhance the reliability in protection, ease of fault diagnosis and better visibility of the network. However, it is easier said than done and a good understanding of VLAN and filtering is required. VLANs are applicable to Station as well as Process bus. Station bus at the substation control room level stays with logical level while switchyard equipment should be kept at Process Bay level physical separation. At logical level, there are managed switches which have VLANS to manage the gates while at the physical level, the operator deals with unmanned switches which doesn’t require much technical skill or configuration. Frame speed at the switches, devices and peripherals using VLANs, could cause clogging, traffic jam, malformation of frame etc. At present due to infrastructure and device constraints the data speed has not reached 1 GB. When bulk digital packets consisting of SV and GOOSE pass through high speed it needs infrastructure that supports data packet transmission. The repercussion of not having faster data size infrastructure i.e. 1 GB/s is best understood when one device, i.e. IED or managed switch, is unable to handle more than 6-8 SV streams at 100 MB/s. This makes the digital protection a bit slow which is unable to apply more complex decision-making tools.

In a digital protection scheme, delay in transmission depends on the integration of topologies and the devices used. Fig. 3.2 exhibits the time taken by GOOSE and SV in transmission and distribution of data using a digital substation automation infrastructure.



Ta = Message Sending delay ; Tb = Message Transmitting delay : Tc = Message Receiving delay

Fig. 3.2. Delay in total transmission of a GOOSE and SV Packet.

By analysing and understanding network topologies that support the digital infrastructure, one could address the optimum solution desired to achieve SAS in substation. Delay in SV and GOOSE packet transmission is attributed to multiple factors, as the number of interconnecting nodes such as switches, MU, IEDs could impede the transmission and subscription. In general the following are the reasons for the delay:

- Store and Forward delay of switches (T_{sf}).
- Switch exchange delays (T_{sw}).
- Optical Fibre transmission delay (T_{wl}).
- Switch Frame Queuing Time (T_q).

Other forms of delays relate to processing time delay, Propagation time delay, Transmission delay, Queuing delay that result in Total Network Delay (TND). THD is a combination of all delays and mathematically represented as:

$$T_d = \sum^{H}{}_{h=1} T_{pch} + T_{qh} + T_{th} + T_{pph} \tag{1}$$

Where, T_d = Transmission delay

T_{pch} = Processing time delay at IED

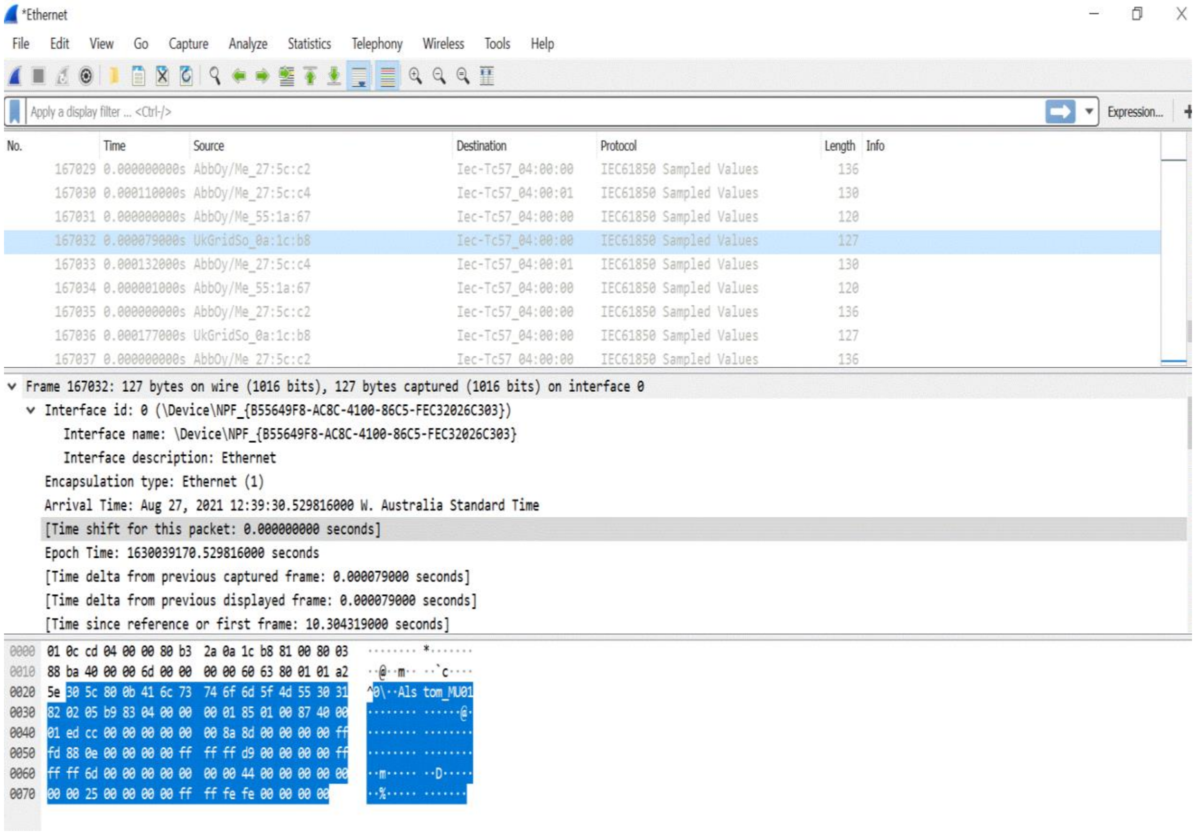
$T_{th} =$ Inter equipment delay

T_{qh} = Queuing delay

T_{pph} = Processing time delay at the switch

h = Hops

Fig. 3.3 is a typical screenshot that exhibits SV streams in healthy form having typical bit size 132-140 bytes, captured via Wireshark tool. In the event of a fault, these data packets undergo deformation in its bit size and their periodic repetition as SV packet changes causing IED to operate.



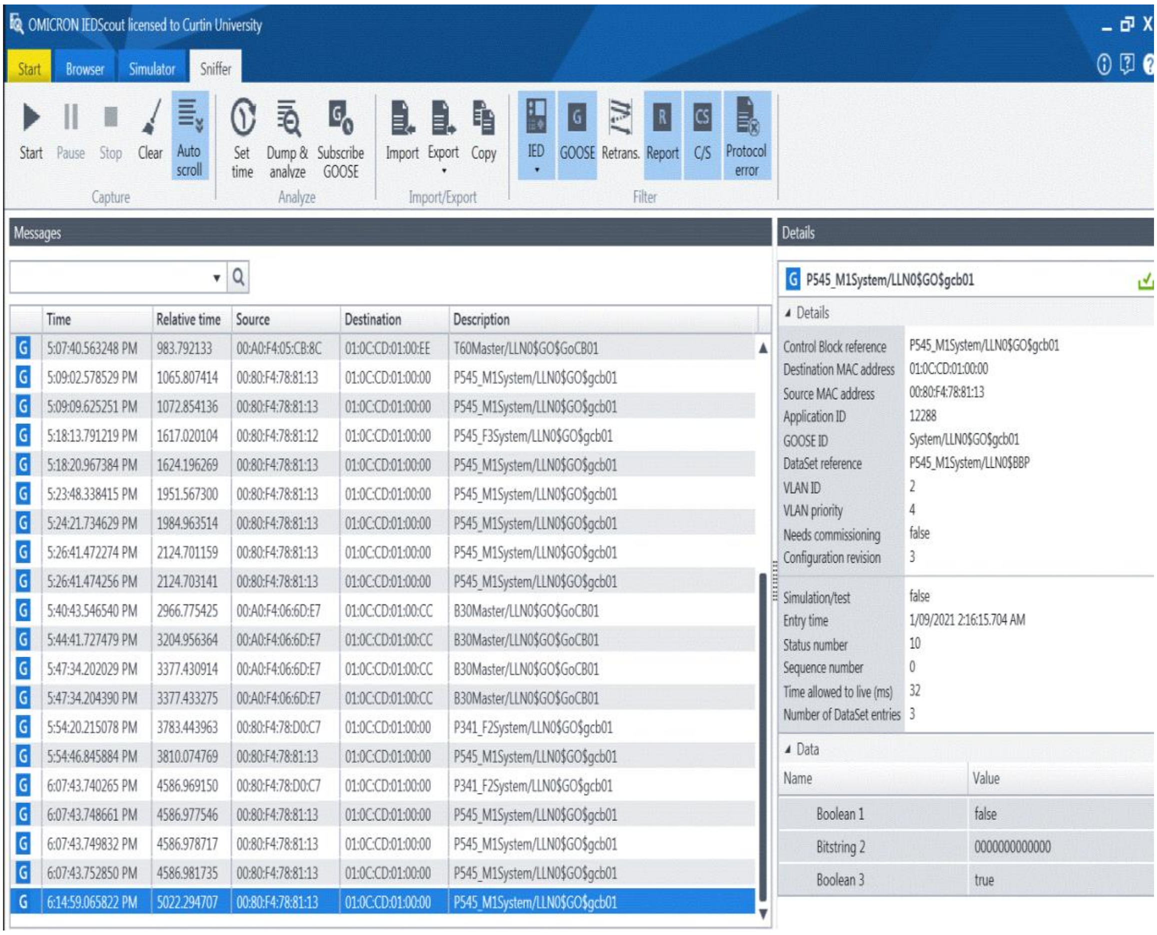
```
No.     Time         Source               Destination          Protocol                Length  Info
167029 0.000000000s AbbOy/Me_27:5c:c2    Iec-Tc57_04:00:00    IEC61850 Sampled Values  136
167030 0.000110000s AbbOy/Me_27:5c:c4    Iec-Tc57_04:00:01    IEC61850 Sampled Values  130
167031 0.000000000s AbbOy/Me_55:1a:67    Iec-Tc57_04:00:00    IEC61850 Sampled Values  120
167032 0.000079000s UkGridSo_0a:1c:b8    Iec-Tc57_04:00:00    IEC61850 Sampled Values  127
167033 0.000132000s AbbOy/Me_27:5c:c4    Iec-Tc57_04:00:01    IEC61850 Sampled Values  130
167034 0.000001000s AbbOy/Me_55:1a:67    Iec-Tc57_04:00:00    IEC61850 Sampled Values  120
167035 0.000000000s AbbOy/Me_27:5c:c2    Iec-Tc57_04:00:00    IEC61850 Sampled Values  136
167036 0.000177000s UkGridSo_0a:1c:b8    Iec-Tc57_04:00:00    IEC61850 Sampled Values  127
167037 0.000000000s AbbOy/Me_27:5c:c2    Iec-Tc57_04:00:00    IEC61850 Sampled Values  136
```

```
v Frame 167032: 127 bytes on wire (1016 bits), 127 bytes captured (1016 bits) on interface 0
  v Interface id: 0 (\Device\NPF_{B55649F8-AC8C-4100-86C5-FEC32026C303})
      Interface name: \Device\NPF_{B55649F8-AC8C-4100-86C5-FEC32026C303}
      Interface description: Ethernet
    Encapsulation type: Ethernet (1)
    Arrival Time: Aug 27, 2021 12:39:30.529816000 W. Australia Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1630039170.529816000 seconds
    [Time delta from previous captured frame: 0.000079000 seconds]
    [Time delta from previous displayed frame: 0.000079000 seconds]
    [Time since reference or first frame: 10.304319000 seconds]
```

```
0000  01 0c cd 04 00 00 80 b3  2a 0a 1c b8 81 00 80 03   ········ *·······
0010  88 ba 40 00 00 6d 00 00  00 00 60 63 80 01 01 a2   ··@··m·· ··`c····
0020  5e 30 5c 80 0b 41 6c 73  74 6f 6d 5f 4d 55 30 31   ^0\··Als tom_MU01
0030  82 02 05 b9 83 04 00 00  00 01 85 01 00 87 40 00   ········ ······@·
0040  01 ed cc 00 00 00 00 00  00 8a 8d 00 00 00 00 ff   ········ ········
0050  fd 88 0e 00 00 00 00 ff  ff ff d9 00 00 00 00 ff   ········ ········
0060  ff ff 6d 00 00 00 00 00  00 00 44 00 00 00 00 00   ··m····· ··D·····
0070  00 00 25 00 00 00 00 ff  ff fe fe 00 00 00 00      ··%····· ·······
```

Fig. 3.3. SV stream captured via Wireshark.

Fig. 3.4 exhibits the GOOSE packets captured in Omicron's IED Scout tool. The screen dump exhibits the configuration that needs carried out in VLAN id, VLAN priority, and Application ID. This figure also shows the status of IED before the inception of fault marked in the screenshot as "False" and provides VLAN id to be 2 for GOOSE and 4 for SV. VLAN acts as a security gate and gives priority to GOOSE and SV depending upon the type of file used.



	Time	Relative time	Source	Destination	Description
G	5:07:40.563248 PM	983.792133	00:A0:F4:05:CB:8C	01:0C:CD:01:00:EE	T60Master/LLN0$GO$GoCB01
G	5:09:02.578529 PM	1065.807414	00:80:F4:78:81:13	01:0C:CD:01:00:00	P545_M1System/LLN0$GO$gcb01
G	5:09:09.625251 PM	1072.854136	00:80:F4:78:81:13	01:0C:CD:01:00:00	P545_M1System/LLN0$GO$gcb01
G	5:18:13.791219 PM	1617.020104	00:80:F4:78:81:12	01:0C:CD:01:00:00	P545_F3System/LLN0$GO$gcb01
G	5:18:20.967384 PM	1624.196269	00:80:F4:78:81:13	01:0C:CD:01:00:00	P545_M1System/LLN0$GO$gcb01
G	5:23:48.338415 PM	1951.567300	00:80:F4:78:81:13	01:0C:CD:01:00:00	P545_M1System/LLN0$GO$gcb01
G	5:24:21.734629 PM	1984.963514	00:80:F4:78:81:13	01:0C:CD:01:00:00	P545_M1System/LLN0$GO$gcb01
G	5:26:41.472274 PM	2124.701159	00:80:F4:78:81:13	01:0C:CD:01:00:00	P545_M1System/LLN0$GO$gcb01
G	5:26:41.474256 PM	2124.703141	00:80:F4:78:81:13	01:0C:CD:01:00:00	P545_M1System/LLN0$GO$gcb01
G	5:40:43.546540 PM	2966.775425	00:A0:F4:06:6D:E7	01:0C:CD:01:00:CC	B30Master/LLN0$GO$GoCB01
G	5:44:41.727479 PM	3204.956364	00:A0:F4:06:6D:E7	01:0C:CD:01:00:CC	B30Master/LLN0$GO$GoCB01
G	5:47:34.202029 PM	3377.430914	00:A0:F4:06:6D:E7	01:0C:CD:01:00:CC	B30Master/LLN0$GO$GoCB01
G	5:47:34.204390 PM	3377.433275	00:A0:F4:06:6D:E7	01:0C:CD:01:00:CC	B30Master/LLN0$GO$GoCB01
G	5:54:20.215078 PM	3783.443963	00:80:F4:78:D0:C7	01:0C:CD:01:00:00	P341_F2System/LLN0$GO$gcb01
G	5:54:46.845884 PM	3810.074769	00:80:F4:78:81:13	01:0C:CD:01:00:00	P545_M1System/LLN0$GO$gcb01
G	6:07:43.740265 PM	4586.969150	00:80:F4:78:D0:C7	01:0C:CD:01:00:00	P341_F2System/LLN0$GO$gcb01
G	6:07:43.748661 PM	4586.977546	00:80:F4:78:81:13	01:0C:CD:01:00:00	P545_M1System/LLN0$GO$gcb01
G	6:07:43.749832 PM	4586.978717	00:80:F4:78:81:13	01:0C:CD:01:00:00	P545_M1System/LLN0$GO$gcb01
G	6:07:43.752850 PM	4586.981735	00:80:F4:78:81:13	01:0C:CD:01:00:00	P545_M1System/LLN0$GO$gcb01
G	6:14:59.065822 PM	5022.294707	00:80:F4:78:81:13	01:0C:CD:01:00:00	P545_M1System/LLN0$GO$gcb01

G P545_M1System/LLN0$GO$gcb01

Details

Control Block reference	P545_M1System/LLN0$GO$gcb01
Destination MAC address	01:0C:CD:01:00:00
Source MAC address	00:80:F4:78:81:13
Application ID	12288
GOOSE ID	System/LLN0$GO$gcb01
DataSet reference	P545_M1System/LLN0$BBP
VLAN ID	2
VLAN priority	4
Needs commissioning	false
Configuration revision	3
Simulation/test	false
Entry time	1/09/2021 2:16:15.704 AM
Status number	10
Sequence number	0
Time allowed to live (ms)	32
Number of DataSet entries	3

Data

Name	Value
Boolean 1	false
Bitstring 2	0000000000000
Boolean 3	true

Fig. 3.4. Status of GOOSE messages in the network before the fault.

GOOSE and SV streaming determines the success of SAS in a digital substation architecture, but it could be affected by network topology. Hence it is important to discuss some of the commonly used topologies and the traffic load they carry in an SAS network in the following section.

3.4 NETWORK TRAFFIC LOAD

Traffic flow of data packets is of high importance in a digital set-up as heavy traffic could cause malfunction of the SAS system. Gao, et al. [11] investigated and determined that in a healthy set-up without a fault there arise no issues but when a fault occurs there is a burst of frames belonging to SV and GOOSE. This burst of frames in a short span could get the network traffic very busy and the SAS network struggles to maintain its high performance. Periodic heartbeat monitored by a network manager provides information about these bursts and appropriate installation of network topology could avoid such congestion. In a digital network and at the time of fault and emergency condition, the system becomes highly unstable, and the digital network is stretched to accommodate these bursts, leading to congestion and delays. The method suggested by researchers indicates that multiple links or channels could address the issue [12]. For example, one channel could address heartbeat and periodic bursts, while the next channel could address emergency messages and control the primary substation assets. However, crowding the network with multiple links is not what the IEC 61850 standard is designed for as one of the fundamental bases of this standard is to reduce the wiring and make the network simple. Another method of reducing the high volume of traffic in a digital network is increasing the bandwidth that could improve control and features of the infrastructure [13]. A digital system promises faster reaction time to fault and is essential to achieve protection trip <4ms timing requirement as specified in the IEC 61850 standard [14]. Optimum performance of a digital network depends upon the network topology and the criticality of the network. In utilities, a double ring with two LANs is preferred while in a mining electrical substation where redundancy in a particular processing plant is not significant one can run the infrastructure with tree topology or combination of topologies [15].

Some of the most commonly used basic topologies are:

- Tree
- Bus
- Ring
- Mesh.

All these topologies could be modelled in desktop with suitable assumptions and speed selection. Desktop modelling and good understanding of the network behaviour without investing heavily on equipment, peripherals, and other hardware, gives the operator a good understanding of data corruption, link, and node failure. It considers various scenarios when queuing delay is more than one second.

Fig. 3.5 exhibits a switching scenario in which two switches are connected to a number of IEDs such as node 6, 7, 8 and 9. Traffic flow is routed via switches i.e., node 4 and node 5. These have been detailed in the End-to-End (ETE) and Average delay reports. In Fig. 5.5, node 2 and node 3 are the servers through which digital data packets are routed. Packets which are delayed for more than 1 second have been discarded. All traffic parameters assumed in this case study are inserted using Discrete Event Simulation (DES). A gui is kept in the model that allows a mathematical algorithm to perform few iterations.

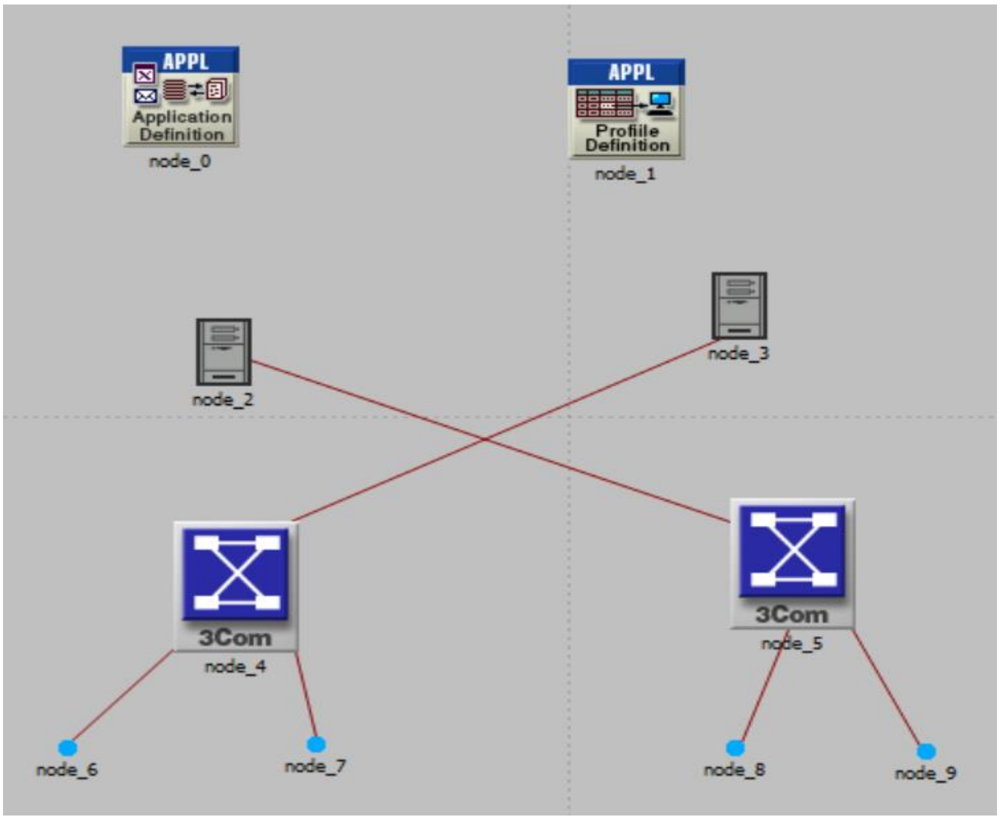


Fig. 3.5. Typical OPNET model of a simple digital network.

3.5 SUBSTATION TOPOLOGIES

The four basic topologies considered in this chapter are tree, bus, ring, and mesh topologies in a physical communication layer which needs to be rigorously tested and redundancy built. This must be proven at desktop and physical infrastructure setup. Once proven by modelling and physical testing it shall be deemed fit for installation. Besides the basic infrastructure on substation topology, choosing a particular topology could be done as a combination of topologies. It must be emphasised that it is challenging to integrate all IEDs, switches and peripherals of different vendors. For example, a Star-Ring topology in a particular utility substation becomes more effective when the switches are connected in ring while the number of IEDs can be connected via Ethernet or FO. In a general mixed approach, having different topologies embedded in the network produces ideal operational requirements in a digital automation substation project while lowering the overall budget and enhancing the protection reliability in a complex substation automation project. Some of the topologies are described below. Installation of managed switches in the digital infrastructure not only reduces wiring cost but also decreases congestion and the traffic load while enhancing the network performance. High-ended managed switches provide Quality of Service (QoS) which allows priority of message data packets to pass through, as exhibited by Sidhu and Yin et al. [14]. Their research and experimental work reveal that designing and engineering the configuration of a managed switch could significantly reduce the transit time. However, this methodology of allowing the digital packets via different gates in managed switches may not meet the condition at higher LAN speed, say 1 Gb/s network, and could have time synchronisation issues. Some of the most commonly used topologies are described in the following sections to gain a better understanding of the optimum solution.

3.5.1 Tree Topology

This topology is a hybrid topology and combination of star and bus networks, which is used for expanding a network arising due to addition of feeder or incomer. It offers flexibility in expansion to the network by linking each node in bus and star topology. The branches expand in a star formation with backbone linked in bus formation.

Fig. 3.6 exhibits expansion of a primary node in which there are three distinct levels, wherein all expanded nodes look like the branches of a tree. All linked secondary nodes can have multiple links. In this infrastructure expansion there is a single central node and remaining secondary nodes are linked to it in a hierarchy manner with each neighbouring node remaining at a lower level with a connection from point to point. Installation of star or bus topologies alone has issues with accuracy, cost and reliability causing performance issues. Hence a combination of star and bus is always beneficial and effective.

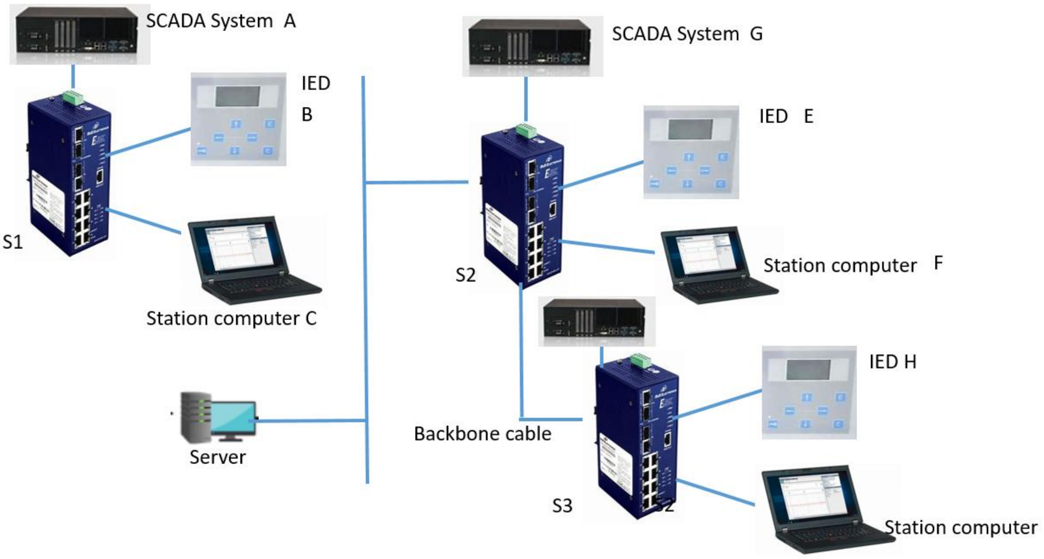


Fig. 3.6. Tree structure in IEC 61850.

The big disadvantage in this structure is that, if the primary node is damaged, the entire infrastructure shall be crippled which could seriously compromise the Substation Automation Scheme. All secondary nodes heavily depend on the primary node and a device failing at the primary node could compromise the entire infrastructure. In a nutshell, it is heavily dependent on the primary device performance. Also, with expansion, fault diagnostic becomes cumbersome and intricate due to the number of links and Ethernet/FO wires. The data packet transmission in this infrastructure needs to follow the 5-4-3 rule, with each SV or GOOSE needed to reach within specific time. Performance of this topology is also dependent on the Ethernet and FO cable used. It also raises a few concerns with security issues.

On the other hand, tree topology has multiple advantages. This topology is very useful in a small industrial substation where redundancy is not of critical importance. Tree topology is fault-tolerant and flexible in adding more nodes for future growth. If a few secondary sections in the network fail or get damaged, the network still performs, when infrastructure is great for small sized hub. Tree topologies have scalability and flexibility in adding a device to the network. Network performance is better than only star or only bus topology.

The tree topology infrastructure can be further expanded to:

- Cluster tree topology
- Bus tree topology
- Rapid spanning tree topology

3.5.2 Bus Topology

Bus topology, sometimes called line topology, links two nodes or devices using a single bus. Each device checks the circulating data packet in the network and scans for its byte size prior to acceptance. Data packets keep circulating until they home into the targeted receiver IED. In this type of connection one line connects two distinctive end points. When designing a simple bus topology, caution must be exercised to prevent weak and vulnerable spots.

Fig. 3.7 exhibits a simple bus topology with IEDs connected to bus in Station bus architecture where Rapid Spanning Tree Protocol (RSTP) ensures the frames do not circulate indefinitely and reach their targeted IED without delay. In this Station bus scheme redundancy is provided at the switch level.

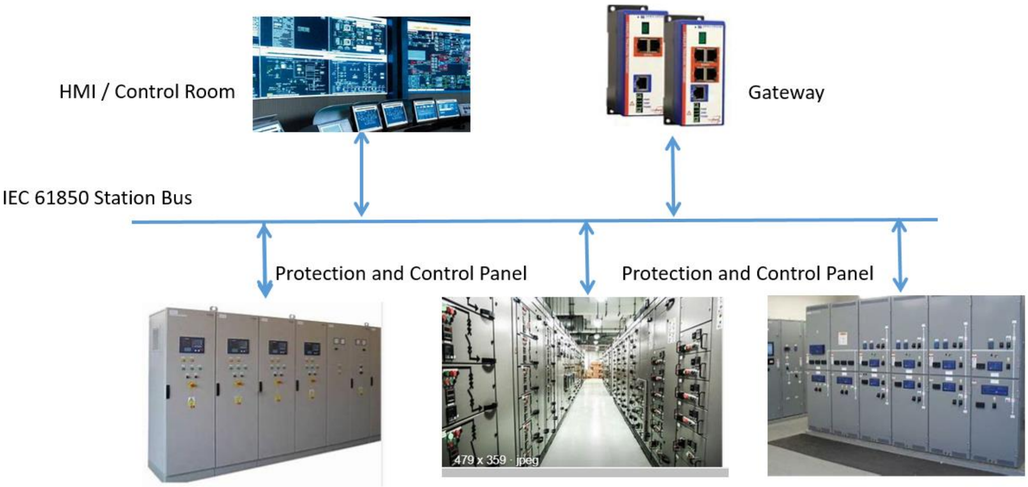


Fig. 3.7. Station Bus Architecture based on IEC 61850.

Fig. 3.8 exhibits an SAS architecture having station, bay, and process levels. Combination of station, bay and process level gives the optimum result in a digital substation. Field devices communicate to the local HMI and operational centre using SV frames in Process bus level while GOOSE frames reach the CBs at Bay level, moving horizontally. Control, command, and monitoring is maintained at the control room at Station level [16].

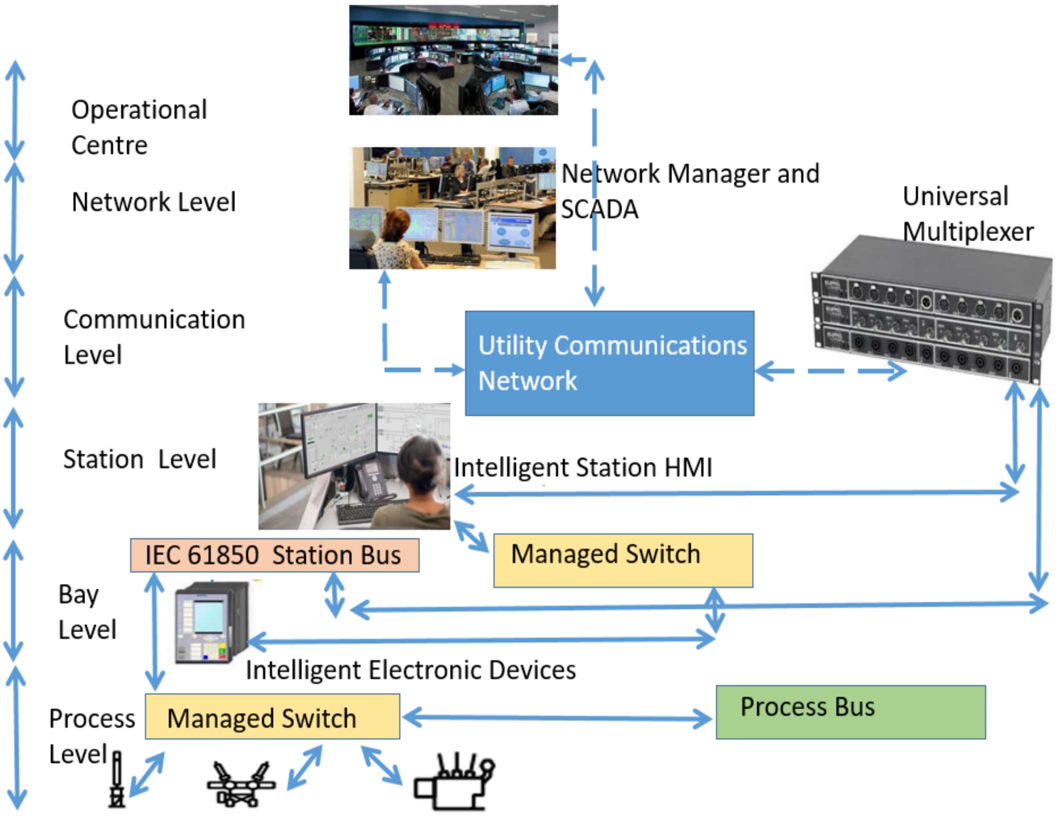


Fig. 3.8. A typical Process bus and Station bus level architecture of a digital SAS.

There are a few disadvantages associated with bus topologies such as the determination of the fault could be challenging in the interconnected bus links where blockages can’t be identified. It is akin to finding a faulty LED circuit on a Christmas tree as the electrician struggles to find the faulty wiring and checks each and every strand. The other disadvantage it offers is that the addition of each node slows down the traffic as the devices are connected via one cable. A burst of SV or GOOSE during a fault could jam and place all the data packets in the queue. Also, if the primary node goes down, it could significantly affect the performance of the network with error-prone communication. There is a risk of data collision and traffic jamming as the network becomes bigger in size. Administration of each node with a password could create issues related to security of the network as there is an opportunity to infiltrate weak spots.

Additional costs related to infrastructure and security may be incurred by the operator in installing a robust security network. Researchers have discovered more issues related to information such as data quality which could suffer and some IEDs may get the command messages due to poor data quality. For a long bus there may not be adequate or proper communication as the data packet is routed via a number of switches, network, IEDs etc. Design consultants should try and engineer an optimum solution with a baud rate normally capable to get acceptance from devices. Some data connected outside the network could be leaked, posing cybersecurity challenges. The infrastructure backbone and nodes need to support multiple transmission. Bus topology with a T-junction is a weak spot in the network which could throw up security challenges by entering via a weak node [17].

Notwithstanding the disadvantages described above, there are few advantages such as being cheap to install. Failure of one device in the network doesn’t completely impact the overall network. There is a significant advantage when a device in the network other than the primary node has no impact on the overall network performance and each new node can be added without a shutdown of the workstations. Additional devices i.e., IEDs could be added without many issues. In this topology there is no requirement to have hubs, switches and routers which reduces the project cost and engineering design time. This topology could stitch many IEDs together for the lowest possible cost. With each workstation connected in the bus, there is no requirement of power supply, and the devices communicate with each other effortlessly. In a bus topology a well-defined network could support a number of devices and peripherals [18].

3.5.3 Ring Topology

Fig. 3.9 Ring topology entails a circular loop around connected devices which saves wiring and number of switches. The frames travel in a bidirectional way. High Speed Seamless redundancy (HSR) is a classic example of frames circulating in a ring topology, described in detail in Chapter 4. By HSR it is meant there is no change over time in the event there is a faulty link. It is widely used in industry in compatible IEDs, and switches configured to accept and transmit HSR frames [19].

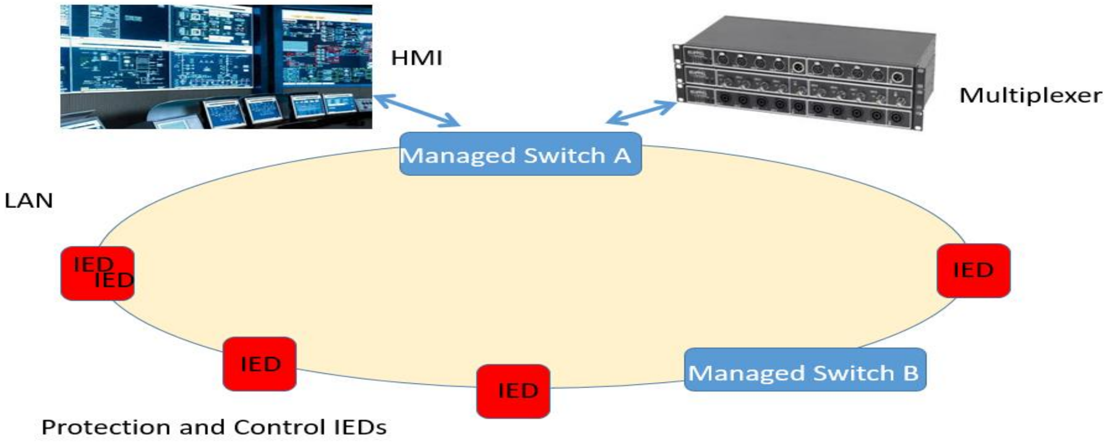


Fig. 3.9. Ring topology in HSR topology.

All switches and IEDs are connected in a ring. This topology provides self-healing ability to the circuit during a fault, and quickly orients to healthy state in the event of a fault. In this topology the frames circulate in two directions and during a link or IED failure the other frame manages to reach the IED, leveraging on a healthy network. In ring topology a number of repeaters are used [18].

This topology is not without challenges and has a few disadvantages. Due to being unidirectional in nature, a frame needs to pass through all nodes. When one node experiences a fault or goes down, it has slower performance as compared to bus topology. Addition or deletion of a physical device requires planning as connecting a new device could slow down the network performance. Total dependency is on two cables on the ring; hence planning is required for backup options.

There are significant advantages in this topology. Frames avoid collision by moving in different directions; hence there is low possibility of collision thus avoiding impact on network performance. This topology is cheap and easy to install. Frames circulation is fast in this topology and frames circulate in an orderly manner making transmission and subscription of data packets easy.

3.5.4 Mesh Topology

Mesh topology is a structure in which all devices are interconnected. Here redundancy is of importance and hence the total number of ports is N-1. In Fig. 3.10 five devices are interconnected. The total number of ports required is 4 i.e., N * (N-1). Here every device is linked to every other channel. Mesh topology can be fully interconnected amongst each device or partially connected. Here peripheral devices such as switches and RED Boxes are not interconnected while IEDs are interconnected [19].

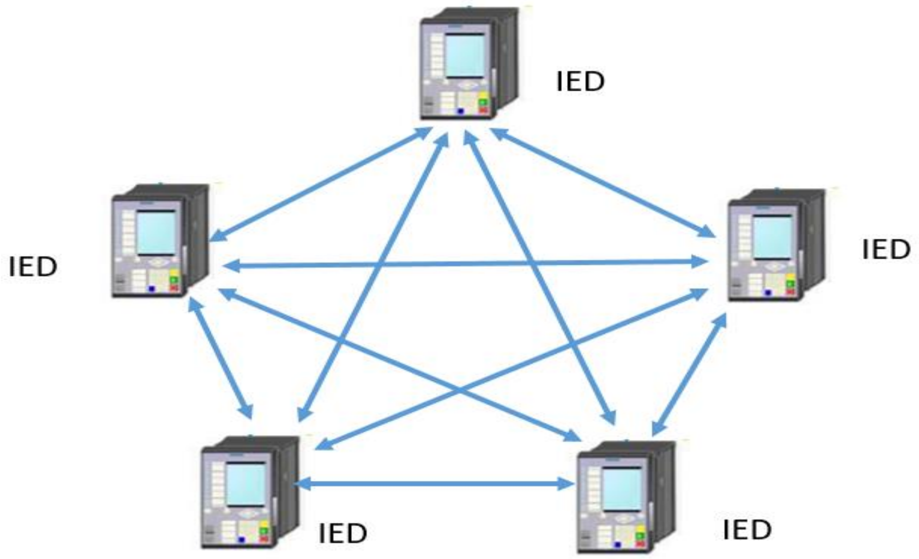


Fig. 3.10. Mesh topology with all devices linked to one another on a particular channel.

Major disadvantages of this topology are that it has complex wiring making engineering, testing, and commissioning lengthy; cost of cabling is high with maintenance is challenging; power connection to interconnected devices adds more cost; cyberattacks are more likely because of redundant connections.

The advantages this topology offers relate to robustness while achieving redundancy. Fault diagnostic is easily identifiable. Data transmission error and frame collision are minimal due to dedicated channels. Redundancy ensures that the network shall not be crippled by the failure of one of the interconnected devices. This provides privacy and security to the network. Data flow and frame circulation remain consistent due to the interconnected network and failure doesn’t disrupt the process. In this topology, expansion by adding a device is easy and no particular device has centralized authority.

3.5.5 Summary of Basic Topologies

All the four topologies commonly used in a digital SAS network are summarized in Table 3.2 These topologies can be applied to a standalone manner or in combination with different topologies in hybrid mode depending upon the network requirement and ability to provide redundancy.

Table 3.2. Summary of common topologies used in digital SAS [20].

Tree	Bus	Ring	Mesh
Nodes are organised in the form of a tree	Each node is connected point-to-point	Nodes are interconnected over a loop with two connections	Nodes are interconnected
This topology provides high security	Low security and vulnerable to cyberattack	Low security and vulnerable to cyberattack	High security, reliable and robust. Tolerant to cyberattack
This topology is complex	Easy in structure as the devices are connected linearly	Simple in structure and frames travel in bi-direction	Complex wiring due to interconnection
It is more complex in wiring, with more wires	It has one cable between two devices	Simplest amongst all topologies	Complex wiring due to interconnection
Tree topology is used for Wide Area Network (WAN)	Tree topology is used for LAN	Possible to connect in WAN and Metropolitan Area Network (MAN)	Suited to be connected to WAN
Fast compared to other three topologies and widely used for expansion	Bus topology is slow compared to tree as transmission is via one node at a time	It is fast due to fewer nodes	Slow in communication as frames have to pass through many nodes
Easy fault identification	Difficult to identify fault	Easy to fault find	Complex fault finding
More expensive than others	Cost of the infrastructure is Medium	Bare minimum Low	High cost of the topology.

3.6 COMMUNICATION REDUNDANCIES USING PRP AND HSR TOPOLOGIES

Any protection system should have redundancy in protection scheme. Digital protection system is no exception and need reliability in protection by having building up redundancy features in the scheme. Two of the most common methods of providing redundancies in digital protection schemes are Parallel Redundancy Protocol (PRP) and High-Speed Seamless Redundancy Protocol (HSR).

The guiding standard for PRP and HSR protocols is IEC 62438-3. The fundamental concept of PRP protocol is that they possess two LANs [18]. Each LAN is independent to the other and operates separately but they are interlinked via IEDs. Source node sends the frame over the two LAN at any given time. The first frame is received by LAN A while the second frame is discarded by LAN B by virtue of having received a healthy frame. Although the two LANs are the same and the frames propagate on the same Ethernet, it could be possible that multivendor proprietary equipment nodes could block one of the frames. However, the smartness of the topology and device allow the frames to reorient themselves and overcome the deficiencies using Address Resolution Protocol (ARP) with a fail-independent ability. This topology and experimental research have been described in Chapter 4, elaborated with system modelling and practical testing. A typical PRP topology is shown in Fig. 3.11 where Single Attached Node (SAN) and Double Attached Node (DAN) devices have been connected. SAN devices have been connected via redundant (Red) boxes. PRP frames laced with Redundancy Control Trailers (RCT) differentiate PRP frames from Ethernet frames.

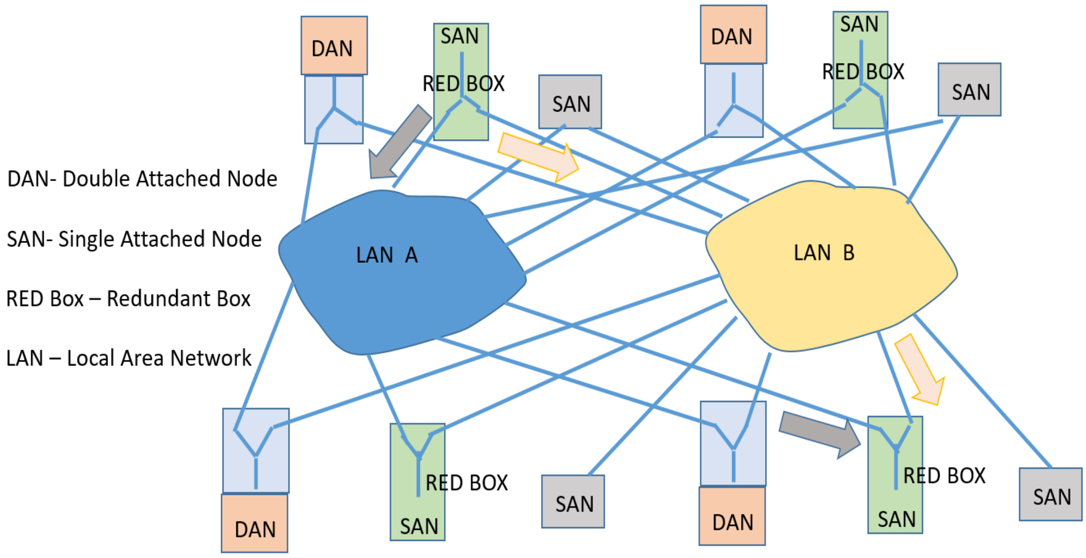


Fig. 3.11. PRP trailer with two LANs.

However, this topology is vulnerable to cyberattack, such as hackers could inject into a vulnerable switch, injecting frames with wrong sequence numbers and force them into IEDs. These IEDs receive and accept frames assuming them to be correct frames. It ends up having a Denial of Service (DoS) attack.

The advantage of PRP lies in being fault-tolerant, and transfer of one LAN to another in no time as it operates on two LANs. The faults could be physical damage of the cable or malfunction of the targeted IED or blockage by inadvertent insertion of incorrect VLAN. Nevertheless, it is clear that the PRP architecture provides a high degree of reliability and redundancies in the digital topology and reorients itself to packet losses and transmission latencies [21].

3.7 HSR TOPOLOGY

HSR is a ring structure topology that provides redundancies with transfer in the ring to another node at zero delay and frame losses. It transmits two copies of frames in two opposite directions via independent paths. Due to its ring structure, failure of one loop enables the frame to travel in the opposite direction and complete the loop. Introduction of link redundancy entity (LRE) in the HSR topology ensures that the redundancy is achieved by circulating the frame to its destination even during a link break. Fig. 3.12 exhibits the HSR topology where SAN, DAN and RED box have been installed [22].

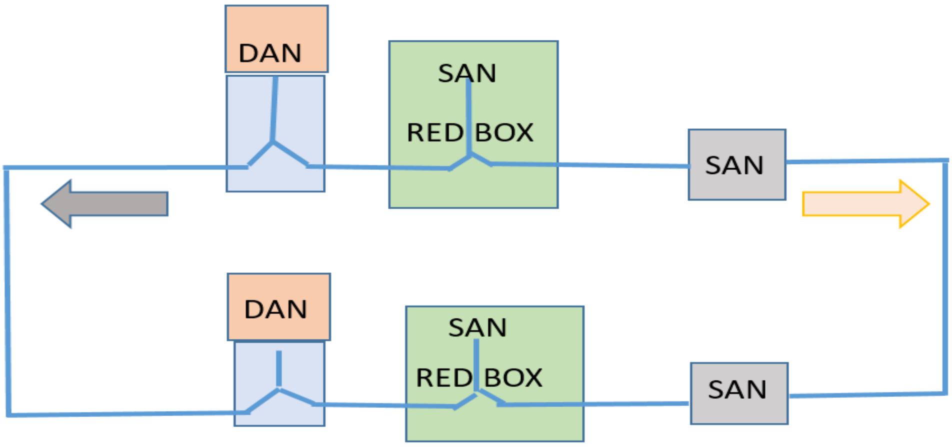


Fig. 3.12. HSR topology with frames circulating in the ring.

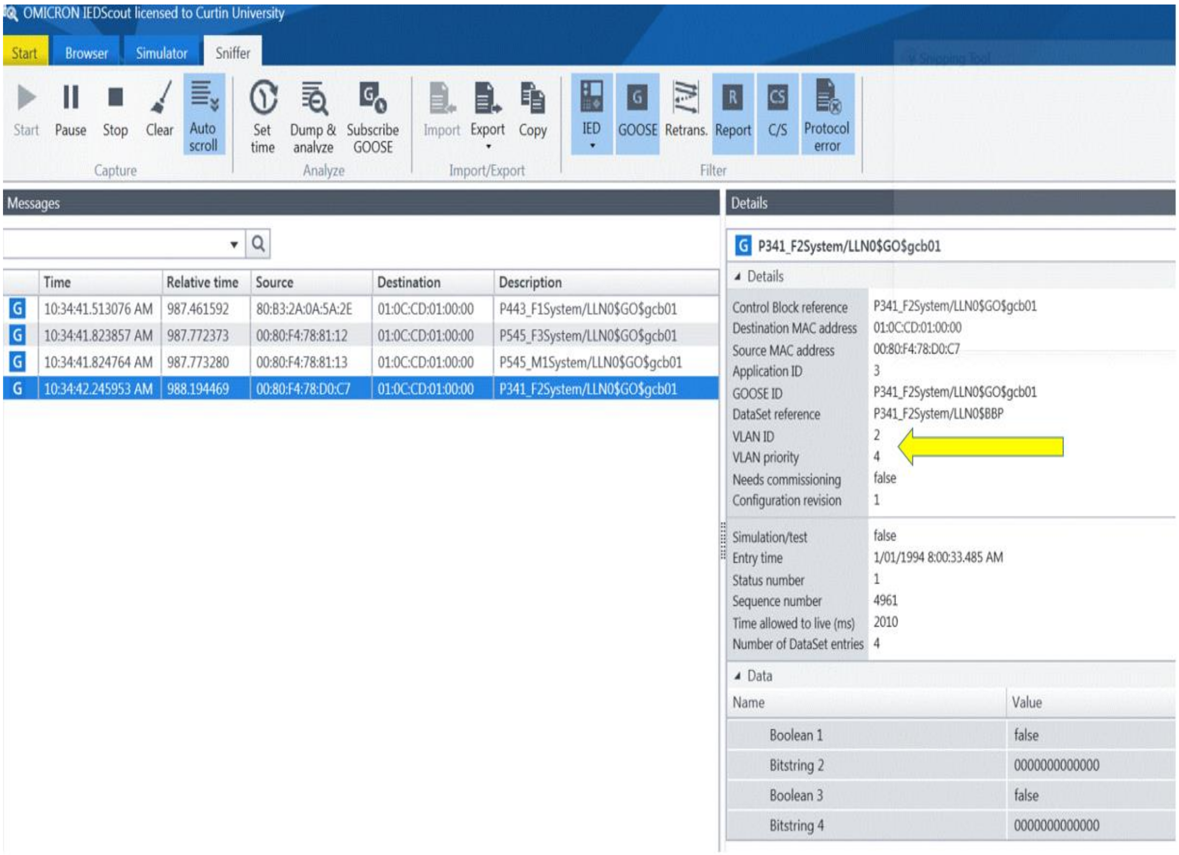
Although HSR topology is easy to implement, it has a few shortcomings such as it doesn't follow the same pattern as PRP frames. Also, all frames are not forwarded during a healthy or normal operation within the ring. In this topology, the frame sequence number and source address find out a duplicate address. This topology needs more computational capacity due to lean structure at nodes.

The huge advantage that HSR topology offers is related to economic considerations, ease of installation in a ring structure, ease of fault diagnostic due to less complication in the network, reduced latency due to no complication in wiring within the structure.

Chapter 4 reviews how these topologies could coexist and remain together in a hybrid operation and the importance of RED Box in the PRP/HSR topology.

3.8 APPLICATION OF VLAN IN A SAS NETWORK

The VLAN parameter setting is of critical importance in a topology as it allows passage of SV and GOOSE traffic. It allows data packets through different ports, performing the role of a gatekeeper, allowing SV and GOOSE via specific configured ports. In Fig. 3.13, VLAN settings range from 0 to 10. A “0” setting signifies that all data packets denoting SV and GOOSE could pass via the port. In this figure, GOOSE have been assigned a VLAN id 2 with VLAN priority being 4. This VLAN acts like a security gate for SV and GOOSE messages which are often kept separate.



	Time	Relative time	Source	Destination	Description
G	10:34:41.513076 AM	987.461592	80:B3:2A:0A:5A:2E	01:0C:CD:01:00:00	P443_F1System/LLN0$GO$gcb01
G	10:34:41.823857 AM	987.772373	00:80:F4:78:81:12	01:0C:CD:01:00:00	P545_F3System/LLN0$GO$gcb01
G	10:34:41.824764 AM	987.773280	00:80:F4:78:81:13	01:0C:CD:01:00:00	P545_M1System/LLN0$GO$gcb01
G	10:34:42.245953 AM	988.194469	00:80:F4:78:D0:C7	01:0C:CD:01:00:00	P341_F2System/LLN0$GO$gcb01

G P341_F2System/LLN0$GO$gcb01

Details

Control Block reference	P341_F2System/LLN0$GO$gcb01
Destination MAC address	01:0C:CD:01:00:00
Source MAC address	00:80:F4:78:D0:C7
Application ID	3
GOOSE ID	P341_F2System/LLN0$GO$gcb01
DataSet reference	P341_F2System/LLN0$BBP
VLAN ID	2
VLAN priority	4
Needs commissioning	false
Configuration revision	1
Simulation/test	false
Entry time	1/01/1994 8:00:33.485 AM
Status number	1
Sequence number	4961
Time allowed to live (ms)	2010
Number of DataSet entries	4

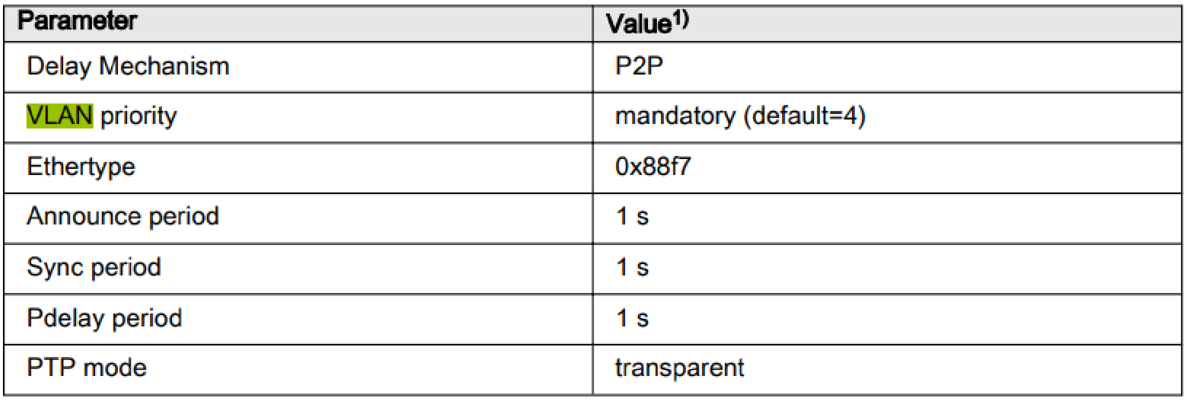
Data

Name	Value
Boolean 1	false
Bitstring 2	0000000000000
Boolean 3	false
Bitstring 4	0000000000000

Fig. 3.13. VLAN configuration using an Omicronenergy IED scout.

The VLAN character are HEX values and range from 000 to FFF. Mission-critical messages of SV and GOOSE pass through the VLAN gate depending on the priority. By default, the priority is set at 4 and the value range is 0 to 7, assigned to managed switches as shown in Table 3.3 [23].

Table 3.3. Power Profile Key parameters as per IEEE C37 and IEEE 802.Q [24].



Parameter	Value[1)]
Delay Mechanism	P2P
VLAN priority	mandatory (default=4)
Ethertype	0x88f7
Announce period	1 s
Sync period	1 s
Pdelay period	1 s
PTP mode	transparent

Table 3.3 guides the operator to set the parameters of all IEDs and switches that route the SV and GOOSE packet flow allowing interoperability to be effective and smooth. Each SV and GOOSE has VLAN identifier whose range is from 0-6 and A to F.

3.9 OPERATIONAL NETWORK TOPOLOGY (OPNET) TOOL

A typical desktop tool that is used to carry out analysis of a digital substation frame movement with respect to latencies, End-to-End delay, frame congestion etc. his been narrated below.

3.9.1 Experimental Scenario

Modelling a HV substation using an OPNET Modeller

Fig. 3.14 shows a typical utility substation operating at 132-kV having two-line incomers. It is stepped down to 22-kV via two power transformers. Both the transfers can take the entire plant load individually, but they mostly operate in parallel with tie breaker in closed position [23]. Physical equipment for SAS such as IEDs, NCITs, MU etc. has all been connected to the network and as shown in the SLD.

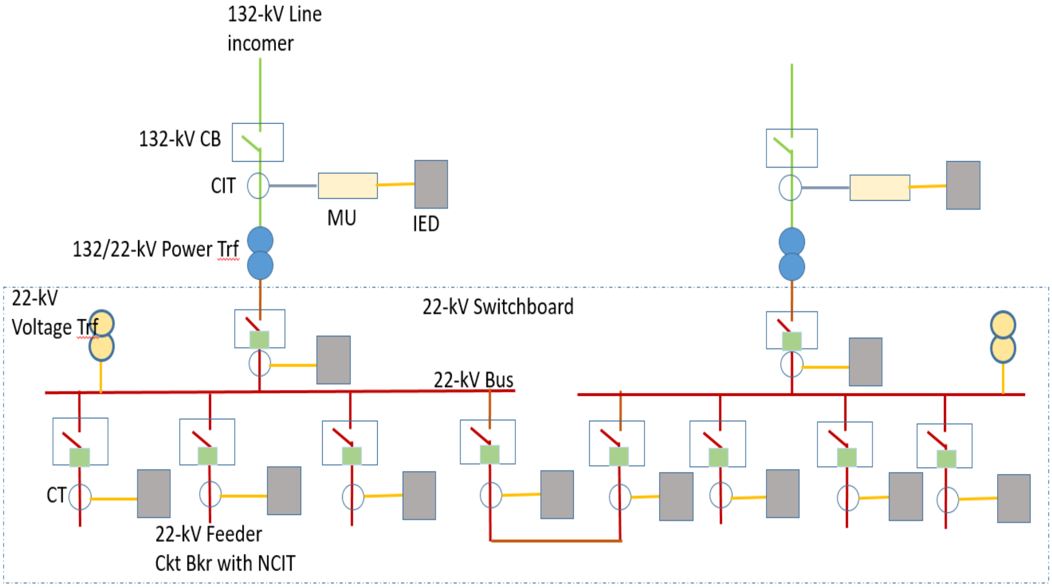


Fig. 3.14. A zone substation of a Utility network at 132-kV.

Fig. 3.15 shows OPNET model of the HV substation in star topology replicating the two buses named as A1 and A5. Initially these bus ties are in OPEN condition. “App” and “Profile” carry mathematical algorithms. The 12 nodes in each of the buses represent additional feeders that could be added to bus A1 and bus A2. Router 1 acts as the managed switch which carries the GOOSE frames.

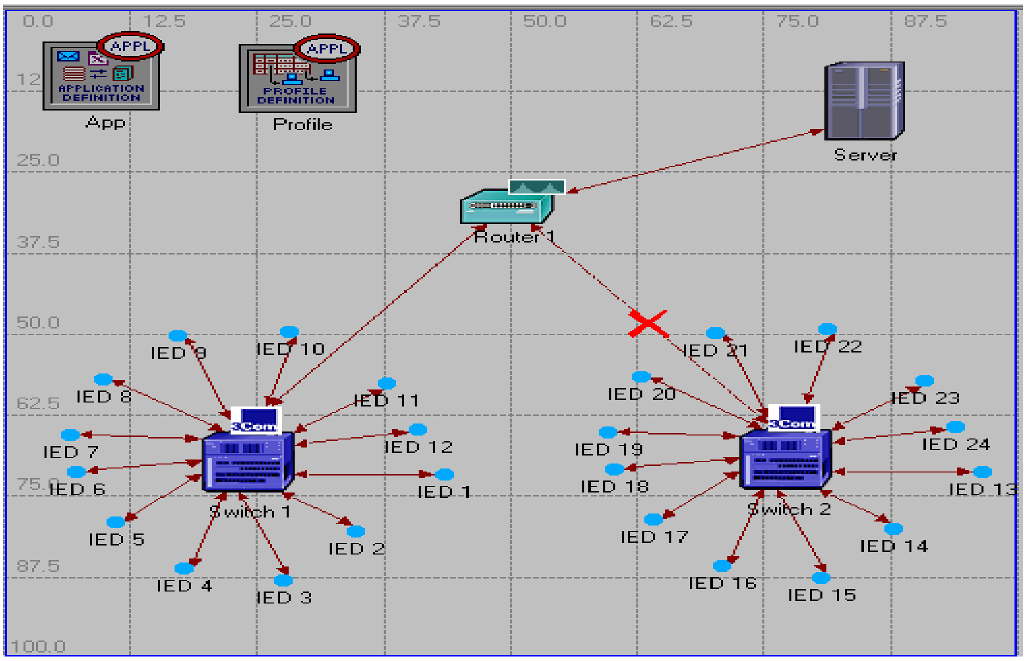


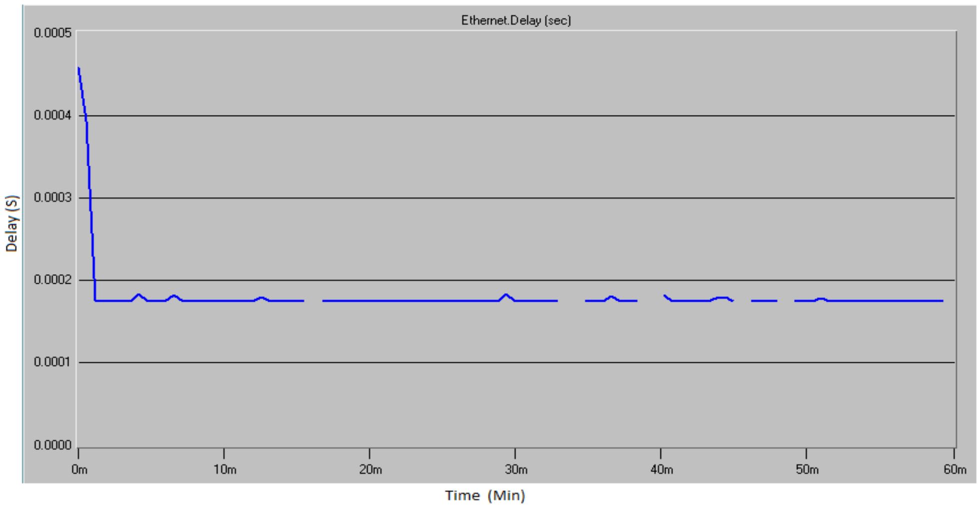
Fig. 3.15. Single process bus with bus tie in OPEN position.

When the bus ties are in CLOSED position, it is termed as double process bus. Table 3.4 gives the Average and maximum delay of the GOOSE messages having LAN speed 10 mbps.

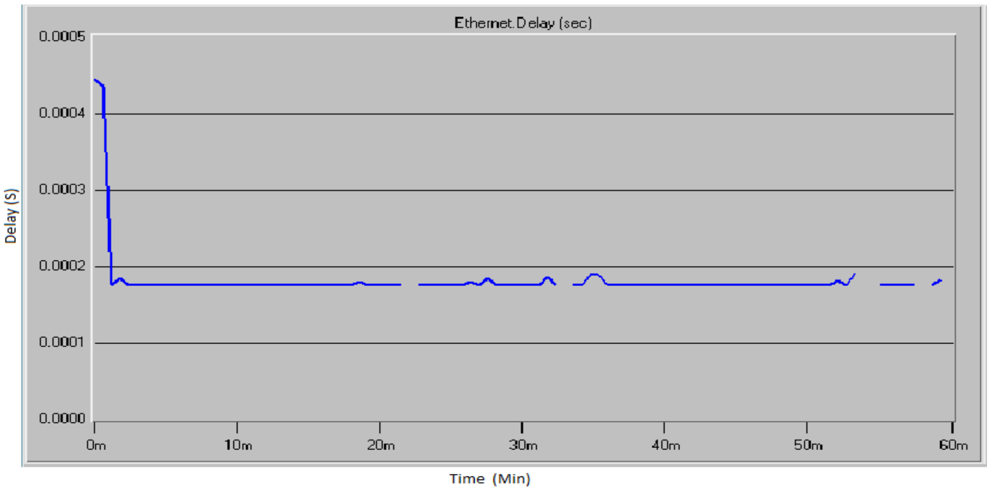
Table 3.4. GOOSE Message Delays in Single and Double Bus When LAN Speed is 10 MBs/s.

		A1 (bus tie OPEN)		A5 (bus tie CLOSED)	
Speed of LAN (Mb/s)	Speed of Sample (samples/s)	Av. system delay	Max. system delay	Av. system delay	Max. system delay
10	256	0.00017	0.0003	0.0005	0.0027
	480	0.00016	0.0005	.00039	0.0029
	960	0.00013	0.00047	0.0004	0.00213
	1920	0.00019	0.00048	0.0007	0.00315

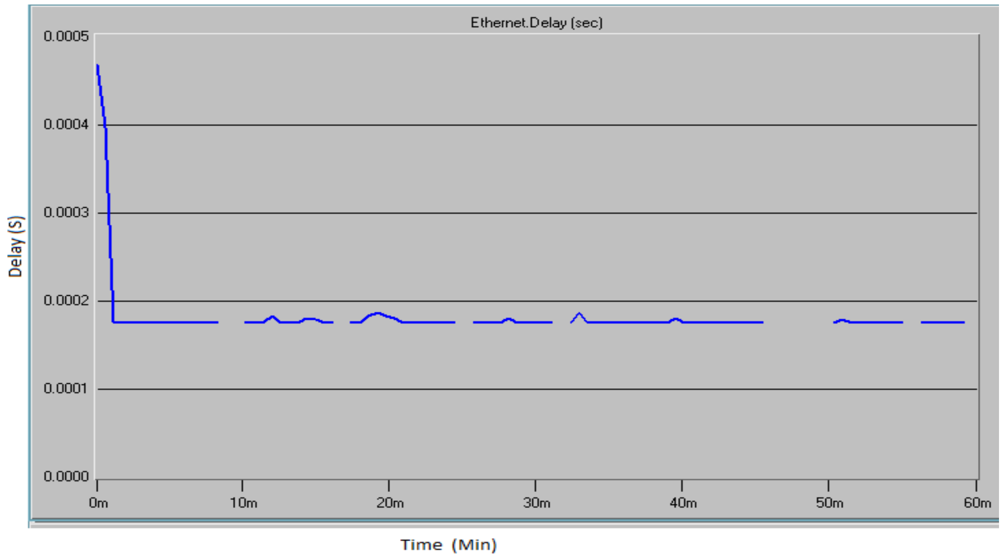
Figs. 3.16 (a-d) represents average and maximum delay of frames in reaching its destination at 4 different sampling speeds communicating at LAN speed 10Mb/s in a single bus topology.



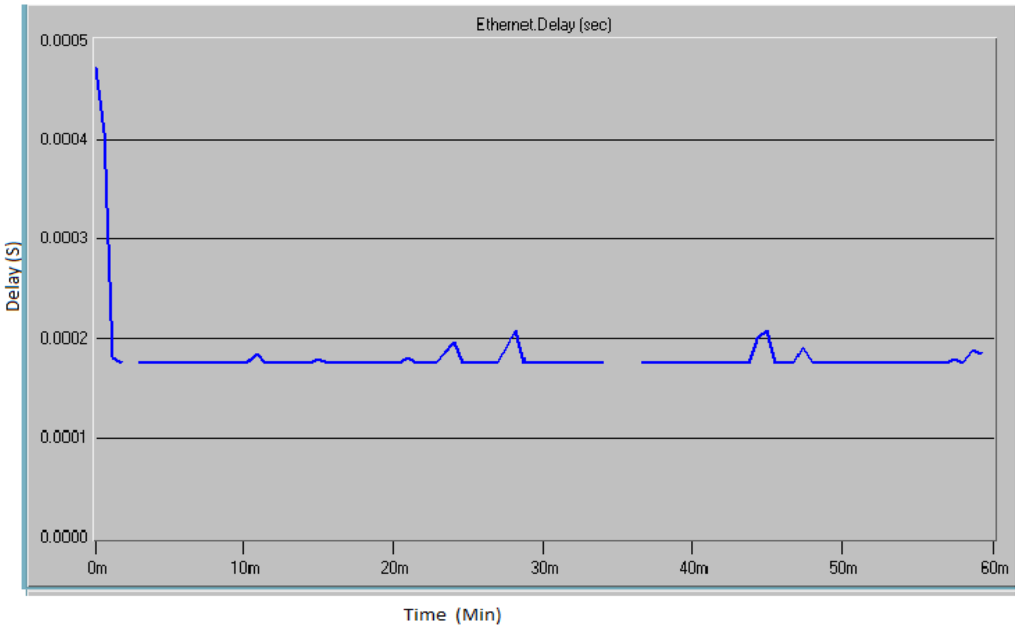
(a) When the sample/sec is 256.



(b) When the sample/sec is 480.



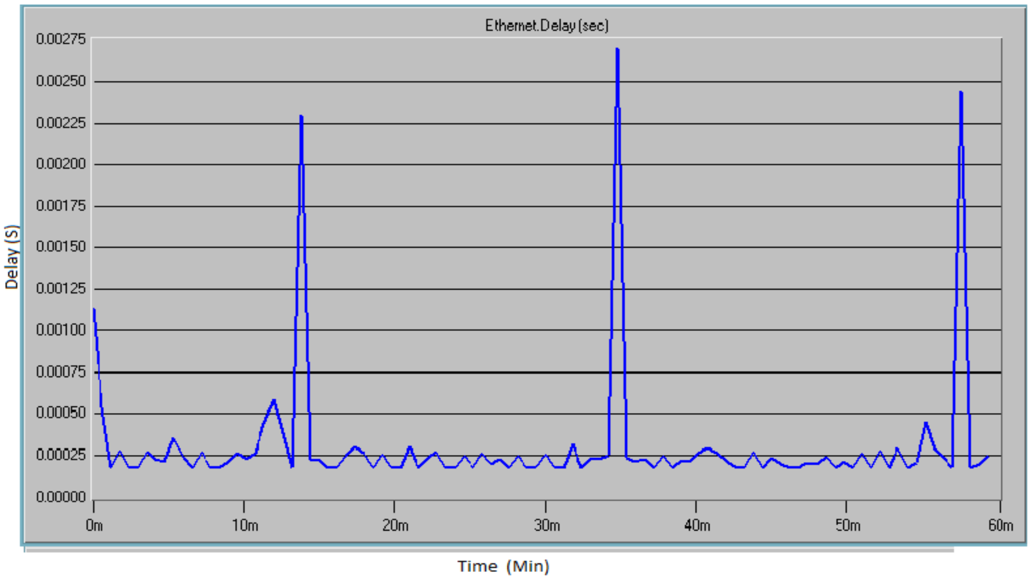
(c) When the sample/sec is 960.



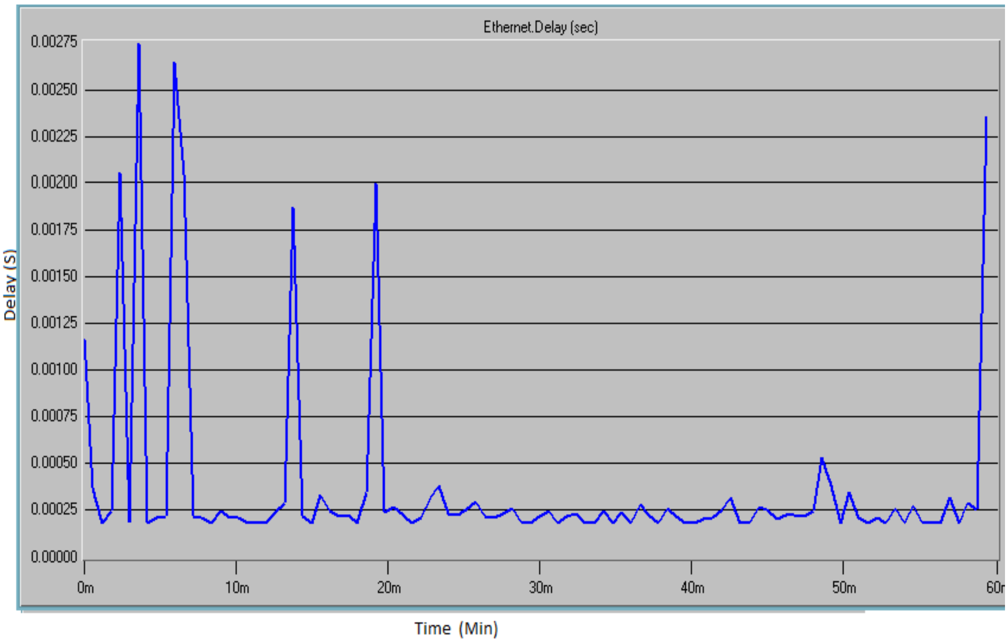
(d) When the sample/sec is 1920.

Figs. 3.16. (a-d): Delay in frame reaching its destination when LAN is 10Mb/s.

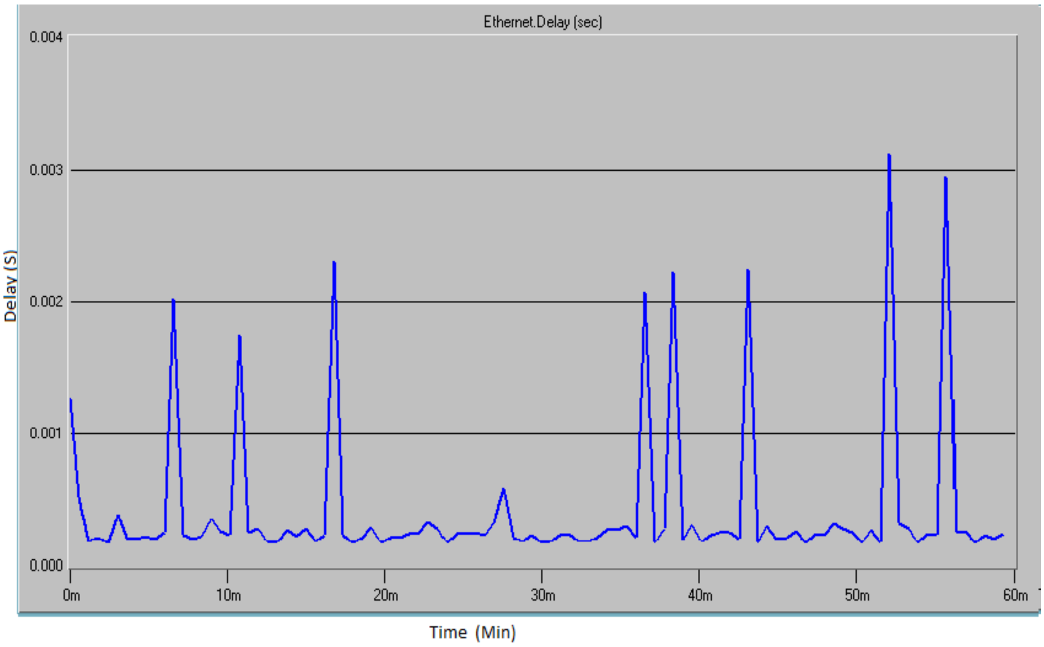
When the speed is increased to 100 Mb/s with bus tie OPEN and CLOSED, the results exhibited appreciable change and frames moved much faster in the star topology as shown in Fig. 3.17 (a-d).



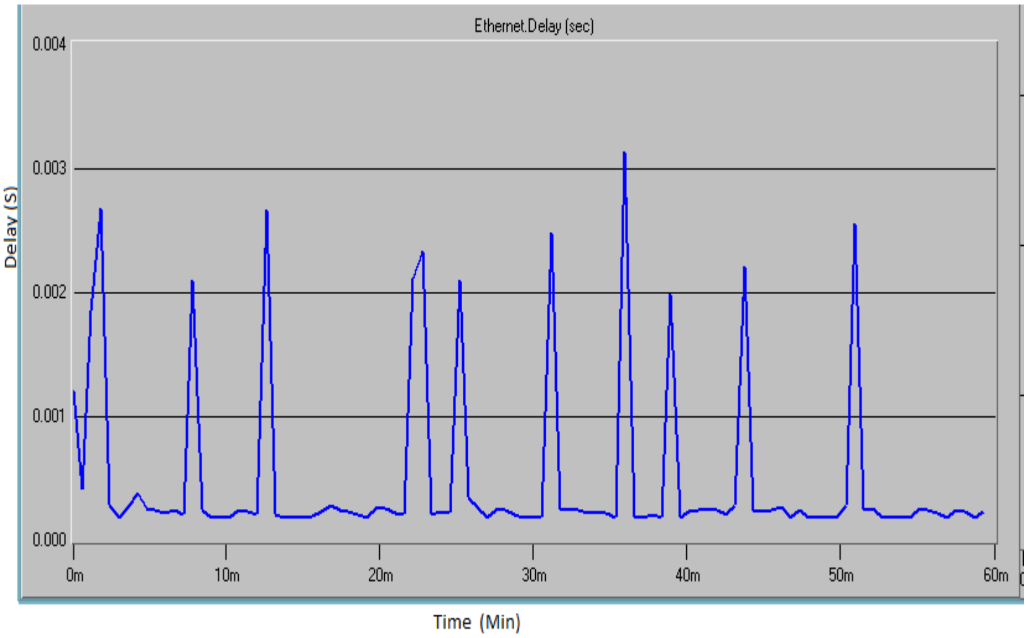
(a) When sample/sec is 256



(b) When the sample/sec is 480.



(c)When the sample/sec 980.



(d) When the sample/sec 1920.

Figs. 3.17. (a-d): With LAN speed increased to 100 Mb/s.

Fig. 3.18 shows a double bus arrangement with bus tie in CLOSED position when the LAN speed was maintained at 100Mb/s.

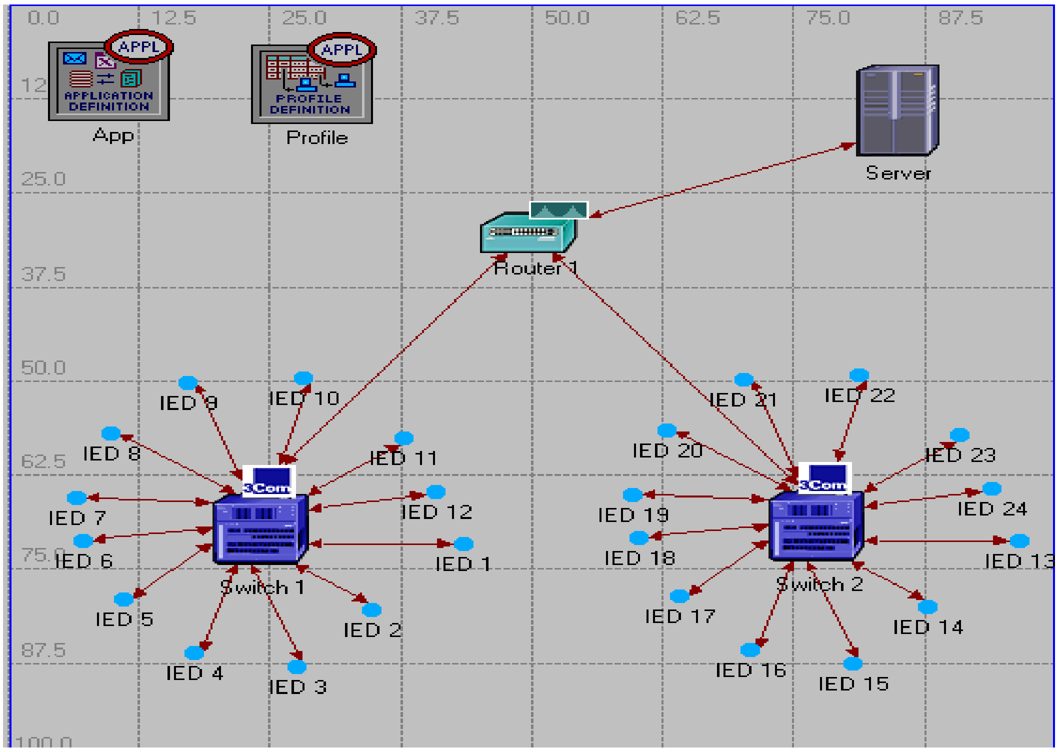
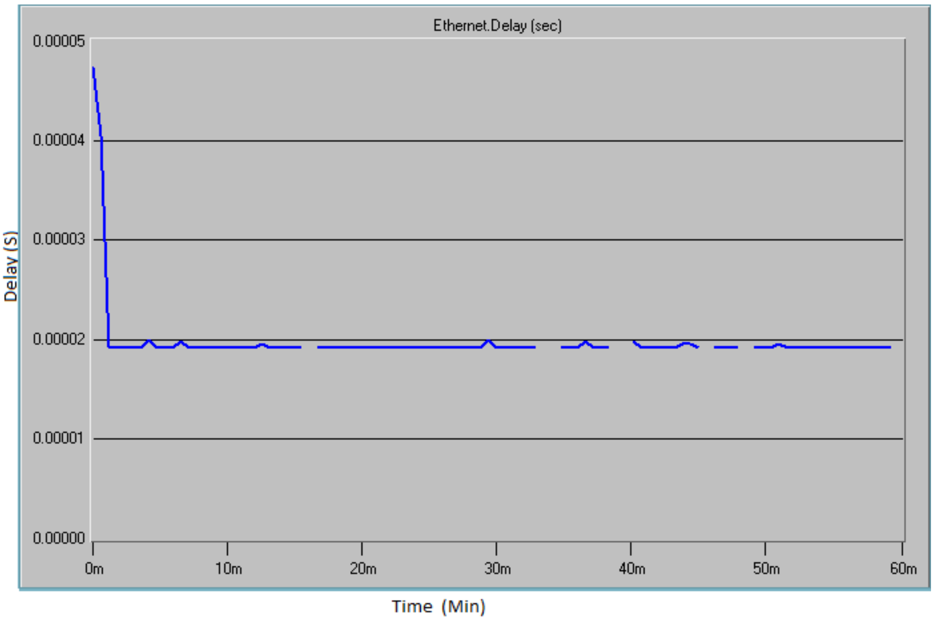


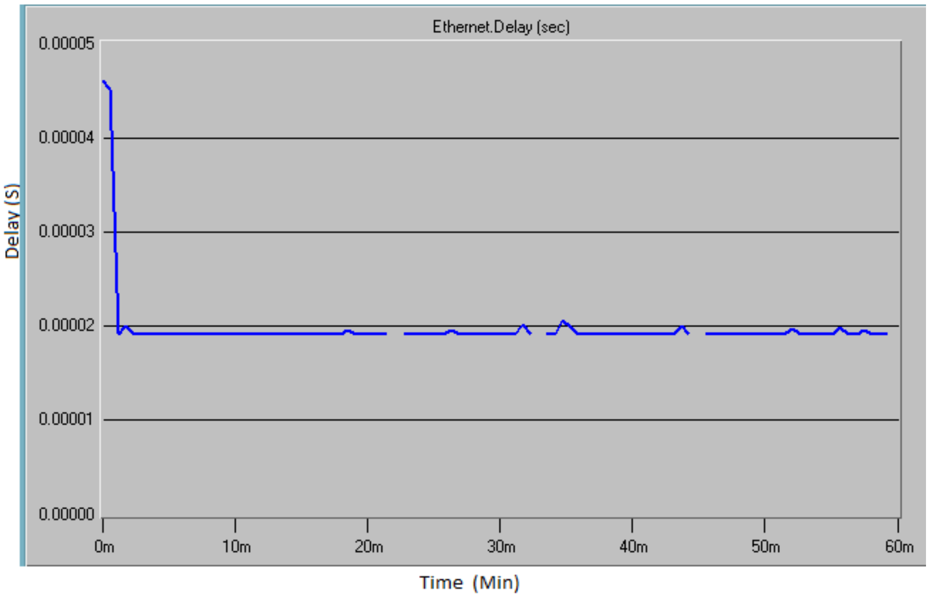
Fig. 3.18. A1 and A5 connected and bus tie in CLOSED position.

Table 3.5. GOOSE message delays in single and double process results with LAN speed of 100-Mb/s.

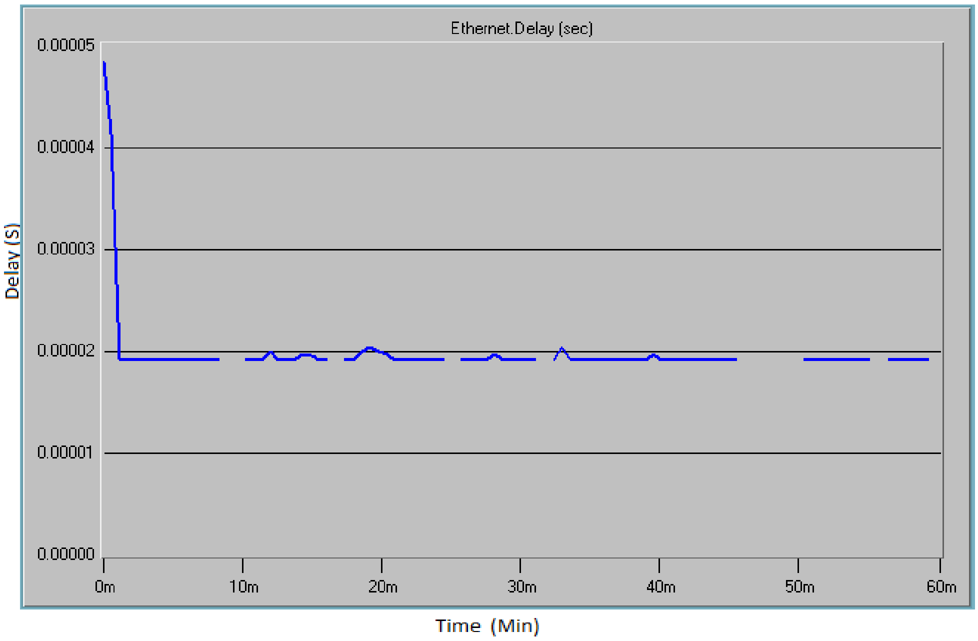
		A1 Bus (Bus tie OPEN)		A5 Bus (Bus tie CLOSED)	
Speed of LAN (Mb/s)	Speed of the Sample (samples)	Avg. system delay	Max system delay	Average system delay	Maximum system delay
100	256	0.00018	0.00037	0.0011	0.0025
	480	0.00014	0.00026	0.0017	0.0024
	960	0.00012	0.00035	0.0021	0.00329
	1920	0.00016	0.00029	0.0022	0.0027



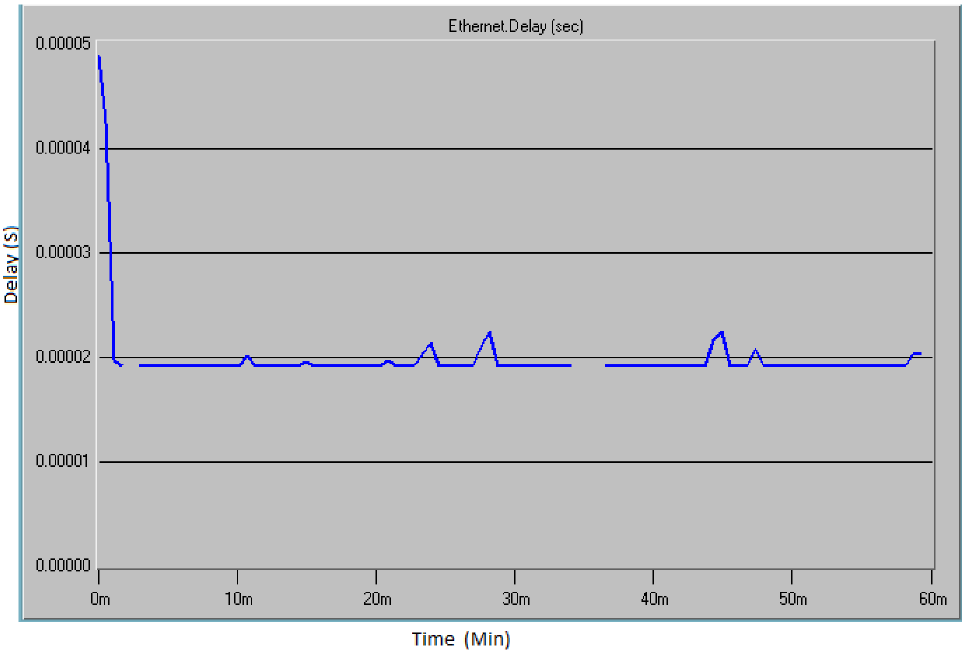
(a) When sample/sec is 256 with bus tie OPEN.



(b) When sample/sec is 480 with bus tie OPEN.



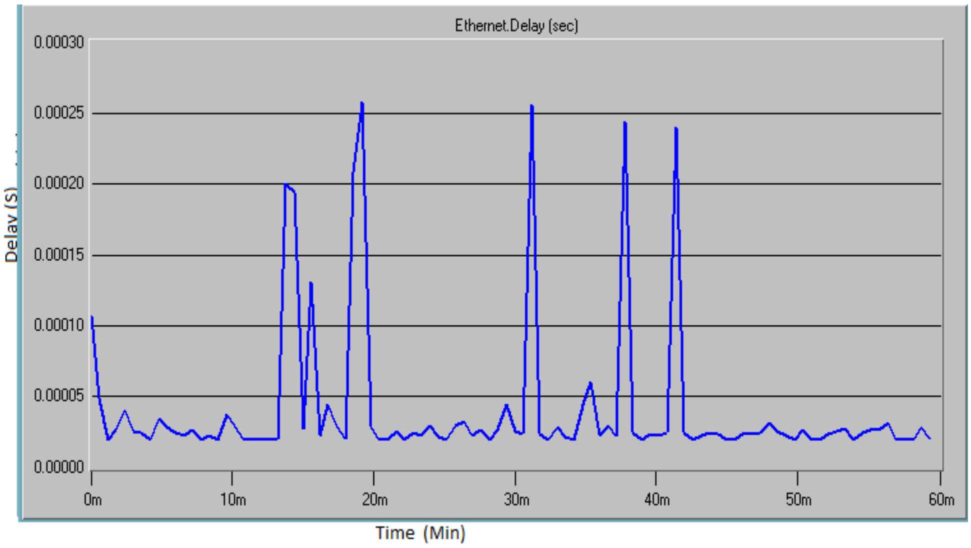
(c) When sample/sec is 960 with bus tie OPEN.



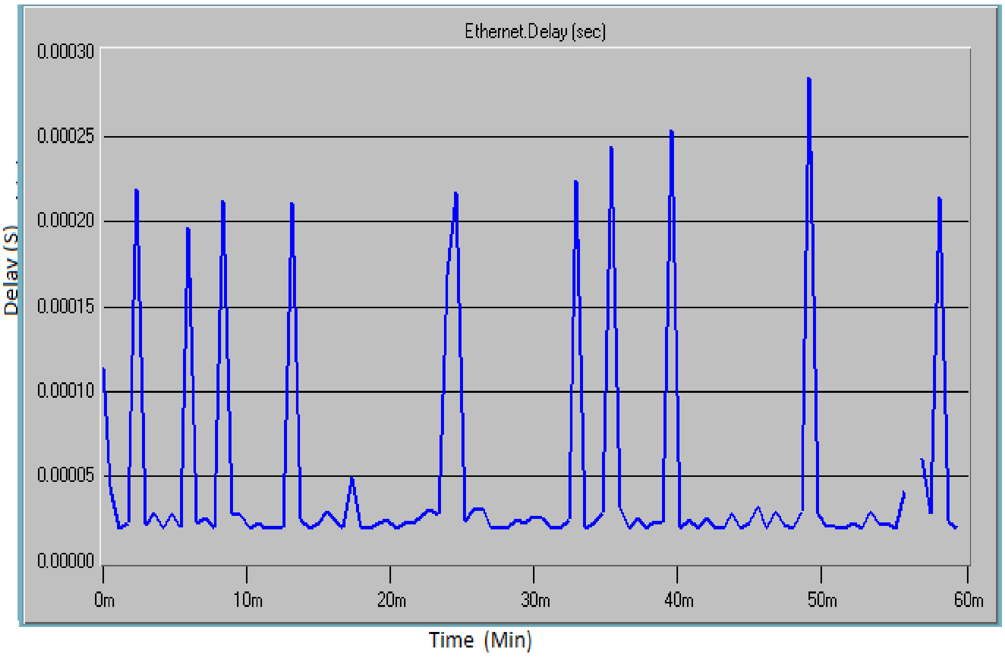
(d) When sample/sec is 1920 and bus tie OPEN.

Figs. 3.19. (a ~ d): Delay in frame reaching its destination with LAN speed 10-Mb/s.

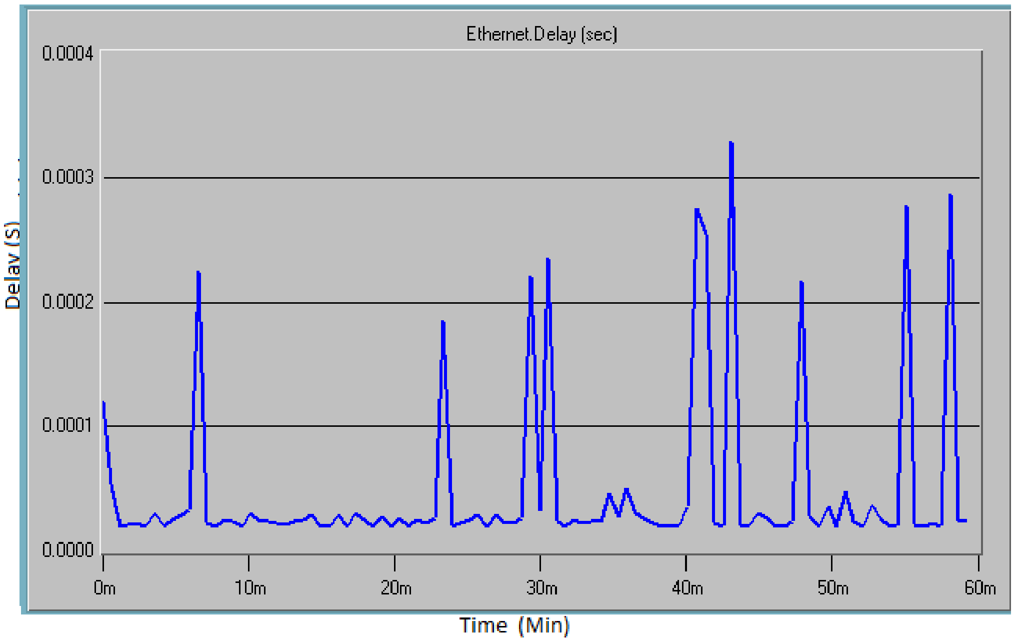
Figs. 3.20 (a ~ d) shows the result when LAN speed approached 100 Mb/s and bus tie was closed.



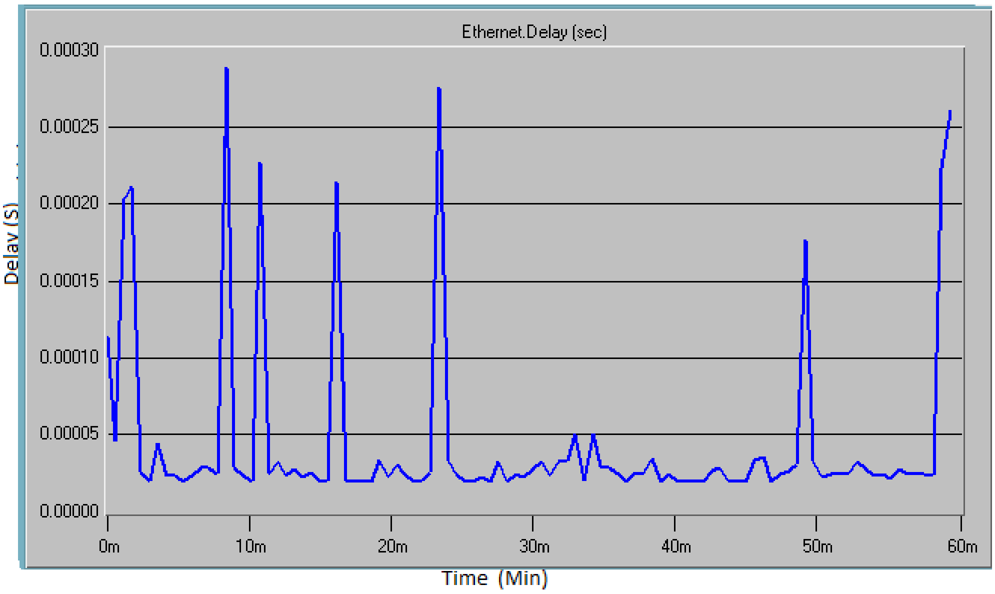
(a) When sample/sec is 256.



(b) When sample/sec is 480.



(c) When sample/sec is 960 with bus tie in CLOSED position.



(d) when sample/sec is 1920 and bus tie is CLOSED position.

Figs. 3.20. (a ~ d): Delay in frame transfer when LAN speed is 100Mb/s.

Summarising the desktop analysis using OPNET tool, speeds of 10 and 100 Mb/s were chosen. Variation of speed caused appreciable delaying issues in a SAS network with bus tie in OPEN and CLOSED position.

A) When it is A1 (with bus tie OPEN): Delay remained lowest when the speed was 10-Mb/s. the average maximum delay was approx 0.47ms. When the speed was increased to 100-Mb/s the average delay for the frame to reach its destination was approx. 0.51ms.

B) When it is A5 (with bus tie remaining CLOSED): The average delay time of message transfer increased considerably with bus tie in CLOSED position when the LAN speed was 10-Mb/s to approx. 0.43 ms but when the speed was increased to 100-Mb/s to the latencies rate decreased to 0.23 ms.

In a nutshell, operating at a LAN speed with bus tie in CLOSED position, provides optimum solution using a star topology. Fig. 3.20 exhibits the advantage of star over ring topology when simulated on an OPNET modeller. For the network described star topology with full power flow and maximum loading, the SAS network as shown in Fig. 3.21 of star topology (refer to blue waveform) performs better than ring topology (refer to red waveform)

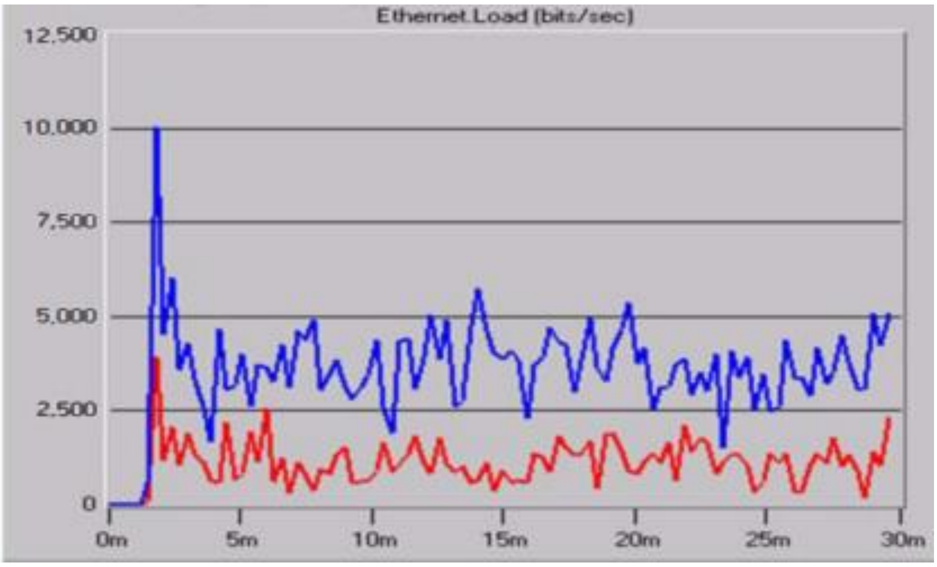


Fig. 3.21. Star (Blue) versus ring (Red) waveform – during maximum loading of the network.

3.10 CHAPTER SUMMARY

Different topologies have been explored in this chapter providing significant advantages in the network encompassing a digital substation. Usually, in a digital substation, we have IEDs, Switches and Ethernet and fibre optic cables. In an operational digital substation when frames from broadcasting devices circulate, there are latencies, delays and malfunctions etc. depending on whether GOOSE, SV or MMS frames are involved. Microprocessor-based IEDs with high computing power and managed switches play a pivotal role in digital substations alongside the architecture of the topology installed, which overcomes issues that occurs with legacy serial communication protocols.

Broadly, the main topologies used in digital substations are Bus Tree, Bus Mesh and Ring. These basic topologies can be installed as standalone or in combination of two or more depending upon operational requirement of being connected in Station or Process bus topology. Also, it depends upon the operational complexities and redundancy requirement of the substation i.e. GIS substation.

Desktop and practical assessment of multiple topologies in standalone mode as well as in combination of different topologies were carried out at the Curtin University laboratory. The author has also experimented with PRP and HSR topologies which provided seamless transfer of frames achieving not only redundancies within the digital topology but provided reliability leveraging on technology. These PRP and HSR topologies are discussed at length in Chapter 4. The real challenges lie in managing different SVs, GOOSE and MMS circulating. This is done by introducing VLANs in the switches which allows specific frame i.e. SV or GOOSE frame to pass through.

Fig. 3.22 exhibits the pictures at the Curtin University laboratory with IEDs and peripherals in the experimental set up mode.

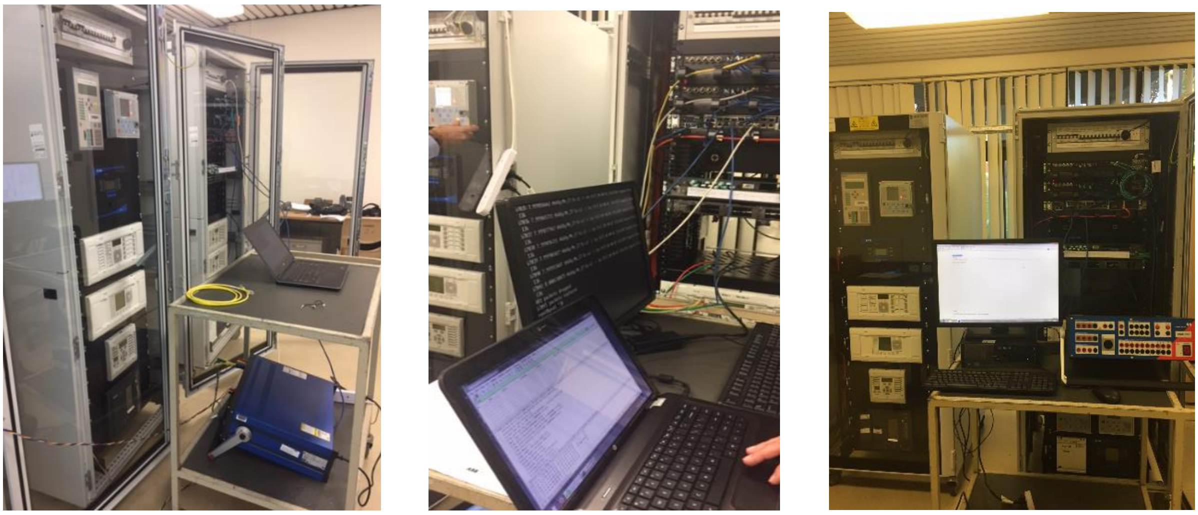


Fig. 3.22. Curtin University IEC 61850 Laboratory.

3.11 REFERENCES

[1] M.Rentschler and P.Laukemann, “Performance Analysis of Parallel Redundant WLAN,” in Proceedings *of the* 12th Conf. on Emerging Technologies & Factory Automation (ETFA), 2012, Sept. 17-21, Krakow, Poland, 2012.

[2] M.Rentschler and P.Laukemann, “Towards reliable Parallel Redundant WLAN Black Channel,” in Proceedings *of the* Factory Communication Systems (WFCS), 2012 9th IEEE International Workshop on *2012,* doi: 0.1109/WFCS.2012.6242573.

[3] M. Rentschler and H. Heine, “The parallel Redundancy Protocol for the Industrial IP Networks,” in Proceedings *of* Industrial Technology (ICIT), 2013 IEEE International Conference, doi: 10.1109/ICIT.2013.6505877.

[4] J. A. Araujo, J. Lazaro and A. Astarloa, “PRP and HSR for High Availability Networks in Power Utility Automation: A method for redundant frame discarding,” IEEE Transactions on Smart Grid, vol. 6, Issue: 5, Sept. 2015.

[5] C. Hoga, “Seamless Communication Redundancy of IEC 62439,” in *Proceedings of the International Conference on Advanced Power System Automation and Protection, 2011,* doi: 10.1109/APAP.2011.6180451.

[6] G. Antonova, L. Frisk and J. C. Tournier, “Communication Redundancy for Substation Automation,” in Proceedings *of* Protective Relay Engineers, 64th Annual Conference, *2011,* doi: 10.1109/CPRE.2011.6035636.

[7] J. A. Araujo, J. Lazaro, A. Astarloa, A. Zulonga and N. Moreira, “Duplicate and circulating frames discard methods for PRP and HSR (IEC 62439-3),, IEEE Transactions on Smart Grid, vol. 6, Issue: 5, Sept. 2015.

[8] IEC 61850-5: Communication requirements for functions and device models

[9] S. Kumar, N. Das and S. Islam, “High performance communication redundancy in a digital substation on IEC 62439-3 with a station bus configuration”, in *Proceedings of the AUPEC2015, Sept. 27~30, 2015,* University of Wollongong, Wollongong, NSW, 2015.

[9] S. Kumar, N. Das and S. Islam, “Performance evaluation of a process bus architecture in a zone substation based on IEC 61850-9-2,” in *Proceedings Of the IEEE-PES APPEEC 2015, Nov. 15~18, 2015,* The University of Queensland, Brisbane, Queensland, 2015.

[10] S. Kumar, N. Das, and S. Islam, “Performance analysis of substation automation systems architecture based on IEC 61850,” in *Proceedings of the AUPEC 2014, Sept. 28 ~ Oct 1, 2014,* Curtin University, Perth, Western Australia 2014.

[11] J. A. Araujo, J. Lazaro, A. Astaloa, A. Zuloaga and N. Moeira, “Duplicate and Circulating frames discard methods for PRP and HSR (IEC 62439-3).” in *Proceedings of the 2013 Electricity Distribution, CIRED 2013*, doi: 10.1049/cp.2013.0836, Stockholm, Sweden.

[12] C. Hoga, “Seamless Communication Redundancy of IEC 62439,” quoted in *Proceedings of the international Conference on Advanced Power System Automation and Protection 2011*Beijing, China, doi: 10.1109/APAP.2011.6180451.

[13] [24] T. S. Sidhu and Y. Yin, “*Modelling and Simulation Performance Evaluation of IEC 61850 Based Substation Communication System,” IEEE Trans. on Power Del.,* vol. 22, no. 3, 2007.

[14] G. Antonova, L.Frisk and J. C. Tournier, “Communication Redundancy for Substation Automation,” in *Proceedings of the 64th Annual conference for Protective Engineers, 2012*, doi: 10.1109/CPRE.2011.6035636, College Station, Texas, USA.

[15] International Standard IEC 62439-3, Edition 3.0, “Industrial Communication Networks High Availability Automation Networks – Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR),” 2012.

[16] H. Kirrmann, P. Rietmann and S. Kunsman, “Standard IEC 61850 - Network Redundancy Using 62439,” Offprint of article in PAC World, Fall 2008.

[17] Y. M. Allawi, D. Lee, K. Lee and J-K. K. Rhee, “Cost Effective Topology Design for HSR Resilient Mesh Networks,” in Proceedings of the Electricity Distribution (CIRED 2013), 22nd International Conference and Exhibition, 10.1049/cp.2013.0836, Stockholm, Sweden, 2013.

[19] S. Kumar, N. Das and S. Islam, “Causes and mitigation of sympathetic tripping phenomenon based on IEC 61850,” *Australian Protection Symposium 2014*, Sydney, New South Wales, 2014.

[20] S. Kumar, N. Das, S. Islam and A. Abu-Siada, "Verification of Latency and Delays Related to a Digital Topology based on IEC 61850," in *Proceedings of the 2019 29th Australasian Universities Power Engineering Conference (AUPEC)*, Nadi, Fiji, Nov. 26-29, 2019. pp. 1-6, doi: 10.1109/AUPEC48547.2019.211964.

[21] S. Kumar, N. Das, and S. Islam, "Implementing PRP and HSR Schemes in a HV Substation based on IEC62439-3," in *Proc. of the 2018 Condition Monitoring and Diagnosis (CMD),* Perth, Western Australia, 2018, pp. 1-5, doi: 10.1109/CMD.2018.8535663.

[22] S. Kumar, N. Das, and S. Islam, "Performance evaluation of two interconnected high voltage utility substations using PRP topology based on IEC 62439-3," 2017 Australasian Universities Power Engineering Conference (AUPEC), Melbourne, Victoria, 2017, pp. 1-5, doi: 10.1109/AUPEC.2017.8282401.

[23] N. Das, W. Ma, and S. Islam, “Comparison Study of Various Factors Affecting End-to-End Delay in IEC 61850 Substation Communication Using OPNET,” in *Proceedings of the Australasian Power Engineering Conferences 2012 (AUPEC 2012*), Bali, Indonesia, 26-29 Sept. 2012.

CHAPTER 4:

COMMUNICATION REDUNDANCY IN A DIGITAL SUBSTATION USING TWO SEAMLESS TOPOLOGIES

4.1 INTRODUCTION

Without substations, no generation, transmission or distribution system could exist as these nodal points exchange huge power. Substations transport bulk power and at transmission level these are often called transmission substations, and at zone level they could supply power to few suburbs termed as the zone substation at utility level. Protection of power transformers, circuit band transmission lines during a fault is of key interest to the operator. This is achieved by fast-acting, sensitive protection schemes located at a local control room or remote-control room. Utility transmission or zone substations have X protection and Y protection is applied to zone substations. Similarly in digital protection we need two sets of protection with one set being ‘main’ and other being ‘standby’, to take over should the main fail to isolate the CB within the stipulated time. This is achieved by PRP and HSR topologies guided by IEC 62439-3 which complement the shortfall experienced in IEC 61850 [1]. However robust testing and validation involving software and hardware level has been carried out at laboratory level prior to the deployment of two mentioned topologies, due to the challenges posed by latencies, end-to-end (ETE) delays and interoperability issues during frame transfer between network devices and requirement to meet the redundancy [2].

IEEE C37.100 standard defines redundancy as: *The quality of a relaying system that allows a function to operate correctly, without degradation, irrespective of the failure or state of one portion, since another portion performs the same function (not to be confused with backup)* [3]. Hence, digital devices need to have redundancies inbuilt within their hardware architecture and to follow the technical rules of transmission and distribution (T&D) networks. The two topologies that provide redundancies to a digital network at hardware and operational level are termed as PRP and HSR. They offer seamless redundancy and enable migration to another network at the fastest possible time when compared to a similar conventional setup [4]. By

’seamless redundancy, it means that during a fault, the digital frames broadcast to another network without disrupting the power in an extremely rapid burst [5]. In this chapter, investigation and testing were carried out on the mentioned topologies by performing desktop studies using an OPNET modeller tool followed by practical experiment involving IEDs and managed switches.

As mentioned in previous chapters, high-speed communication in SAS networks is of critical importance. IEC 61850 communication has a few shortcomings in providing redundancies which led to further research and development in creating a new guideline i.e. IEC 62439-3 guideline. Some of the issues encountered in IEC 61850 were data clogging, frame corruption and errors, data losses during peak traffic and proprietary features of multivendor equipment that led to the creation of the newer guideline [6].

IEDs with Doubly Attached Node (DAN) and Single Attached Nodes (SAN) devices that are compliant with PRP and HSR, provide redundancy to a SAS network. These smart equipment in the network broadcast active frames circulating in a LAN ring. Detection of the missing PRP and HSR frames triggers a trail of follow-up frames that reorients using an alternate route. This sort of orientation and condition within a network require comprehensive experimental verification and desktop study to shall gain confidence of the user in future deployment of redundant topologies in a digital network. It is envisaged that by adapting to these two topologies, one could receive a fast response time and reliability in a digital network in the event of a fault [7].

This chapter focuses on a desktop simulation and validation of the performance related to the two topologies within a station and ring bus architecture, based on the IEC 62439-3 guideline. This provides the operator with multiple advantages such as rapid change-over within a substation environment in microseconds as opposed to a conventional one in milliseconds. Further, the deployment of these topologies could reduce installation time, provide accurate and reliable fault diagnostics in a secondary system and provide backup protection when the main protection fails. The few digital substations currently operating as pilot projects around the globe on IEC 62439-3 seem to have easier fault diagnostic, and superior performance as the equipment’s in operation have been condition monitored for frame flow and not just during a fault scenario [8].

Researchers are working towards testing multivendor compatible IEDs, switches and Red boxes digital packets to prove that compliant IEDs to these redundant protocols honour the guideline on speed of packet reaching its destination i.e.100µs related for a GOOSE and 4µs for SV frames, in order to prove overall reliability in digital protection [9]. Desktop and hardware tests carried out at Curtin University in wired and wireless mode have demonstrated overall performance of these two redundant topologies. The validation processes carried out included packet scheduling and monitoring of frames at regular intervals within the network due to the network technical rules requirement [10]. Often substations don't have the luxury of taking a shutdown for maintenance or diagnostics periodically as it could cause inconvenience to the end users. Hence condition monitoring of digital healthy frames is of high importance but for which the smart IEDs could cause power flow disruption [11]. Legacy digital protocols have a few challenges, such as failure of mission critical frames to arrive at the targeted IED due to delay or malformation of packets etc. Additionally, interlocking and blocking being critical and following the technical rules of digital protection, the communication recovery time after a failure are as exhibited in Table 4.1 and as guided by IEC 61850 standard.

Table 4.1. Communication recovery time based on IEC 61850-5 [12].

Communication methodology	Application recovery time (ms)	Communication recovery time (ms)
Client-Server SC to IED	600	400
IED to IED, reverse blocking, interlocking	12	4
Trip GOOSE	8	4
Bus bar protection	< 1	seamless
Sampled values	Less than a view consecutive sample	seamless

Following the recent research and further development in IEC 62439-3, the technical committee identified the need for redundancies at various node and peripheral level which could fail and just not at IED or switch alone [13]. Often a digital network is scanned for healthy frames at 1ms. This scanning at regular interval ensures that the network always has healthy frames that can carry out a "bump-less" and "seamless" transfer during a fault scenario. This migration to a healthy network satisfies the condition of zero recovery time as stipulated in IEC 62439-3 [14]. Based on the standard, condition monitoring at every 1ms of the network at nodes and peripherals ensures redundancies are available in the digital network on all occasions. However, the infrastructure cost could go up due to double LAN for PRP but the reliability in protection is ensured [15].

Not many manufacturers have their smart devices compliant with the new technology and hence performance validation has been carried out in the laboratory with the available device. The basic principle on which PRP topology operates relates to having two independent LANs. Failure of LAN A could still ensure full protection functionality of the topology to the network. The topology provides full redundancy and switch-over to LAN B during a link failure. Smart devices connected to a PRP network have DANP IEDs, subscribing frames at both nodes in order that malformation or error in frame arriving at one port doesn't impede or compromise the redundancy features at device or peripheral level [16]. Blockage or interruption at one port opens up the second link which ensures zero interruption to the traffic flow of frames. This provides redundancy in protection.

While PRP and HSR topologies are both important and could have huge application, PRP with its two LAN structure is more complex. With its two LAN structures, it provides smooth transition in microseconds as a part of seamless changeover, while HSR frames takes to alternative path to route frames during disruption. The uniqueness of these two topologies depends on the size and type of octets and bytes each topology carry [17]. Traffic jam and excessive queuing in a HSR topology makes it less acceptable in important utility substation. It is observed that due to bi-directional data communication by its smart devices, the frames don't stop moving and keep propagating an alternative route. The study in this chapter primarily focuses using an OPNET tool to evaluate ETE delays and latencies encountered in ring and tree topology configuration using GOOSE and SV frames. Also, a comparative study has been carried out between wired versus wireless modes of frame transmission, using PRP topology for network traffic and bandwidth [18].

4.2 STRUCTURE OF PRP AND HSR FRAMES

4.2.1 PRP node structure

The node structure of a PRP frame is exhibited in Fig. 4.1. Ethernet adapters of a PRP node of a DANP device is seen, with MAC and IP addresses. Redundancy is achieved with frame circulation in two LANs. By circulation of frames in two different LANs, a bumpless and seamless transfer occur with zero delays in the event of a link failure. Blockage at LAN A node opens up alternative route i.e., LAN B for the frame to travel under certain strict timing conditions in a different bus topology such as station or process bus. As stipulated in IEC 61850-5 technical standard, it is acceptable to have up to 100ms delay, while only 4ms is acceptable for reverse blocking for communication recovery time shown in Table 1 [19].

Deployment of PRP has multiple advantages such as a PRP compatible device will work well with the Rapid Spanning Tree Protocol (RSTP) device from SAS perspective. The standalone protocol and transfer from one LAN to another in microseconds makes it ideal as a redundant protocol and it is sought after transparent topology in a digital substation under fault condition. The redundancy feature of PRP topology allows it to tolerate single component failure and time synchronisation with other RSTP devices [20].

Fig. 4.1 shows the block diagram of a PRP device structure. Its adapter has a set of Medium Access Control (MAC) and Internet Protocol (IP) addresses. Its Link Redundancy Entity (LRE) which is sandwiched between upper layer and ports allows duplication of frames as well as monitoring of the duplicate frames. The errors frame with typical signature are monitored and filtered out by LRE. To modify or insert additional features, one needs to modify its processor. As mentioned in the previous section PRP offer multiple advantages in a digital system such as extremely quick response to change over to alternative network absolutely at zero seconds and adaptability to communicate with RSTP devices using Red box. With its support towards peer-to peer communication and faster data exchange with compatible device, this protocol is likely to be favoured in a digital SAS network.

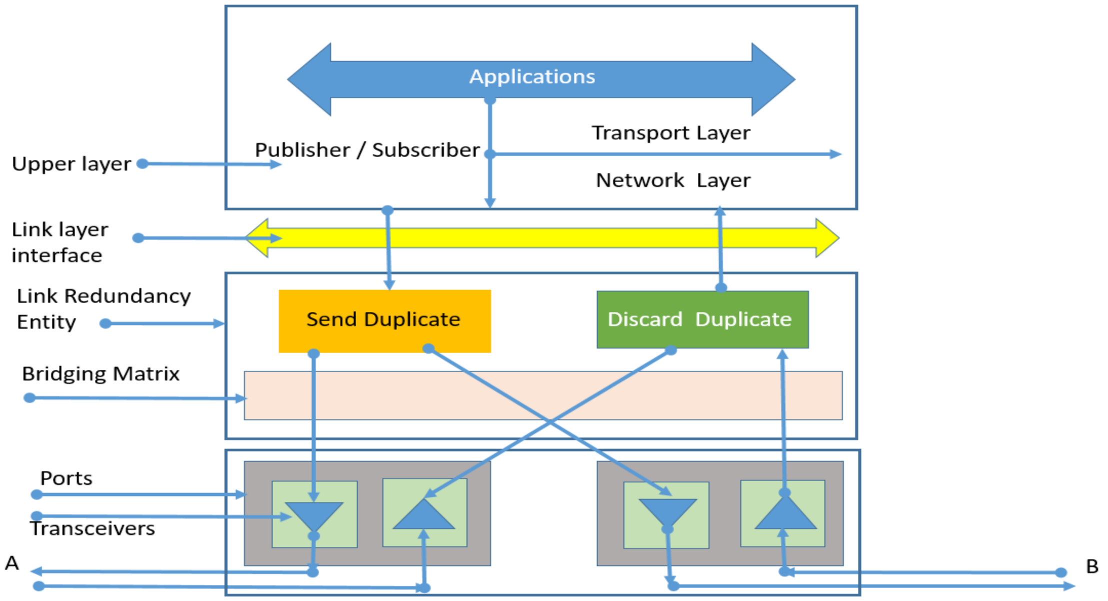


Fig. 4.1. A block diagram of PRP node.

In Fig. 4.2, are LRE layer upper and lower layers of a DANP device that handles redundancies within the network. The LRE layer manages to monitor this duplication using a series sequence number and mapping it onto an inbuilt Redundancy Check Trailer (RCT). Circulating frames are identified for its errorfree situation using a LAN identifier. It is expected to have the frames reaching its destination at the same time in port A and port B, but there could be number of reasons for not reaching its destination due to complexity in the network or proprietary features of the devices or smartness of the adapter device that makes variation of speed of the circulating digital frame. LRE continuously supervises the frame movement as it arrives at the node. It is observed from Fig 4.1, when two frames reach LRE level, one of the most acceptable frames is escalated to a higher level while the second one is discarded along with its RCT [21].

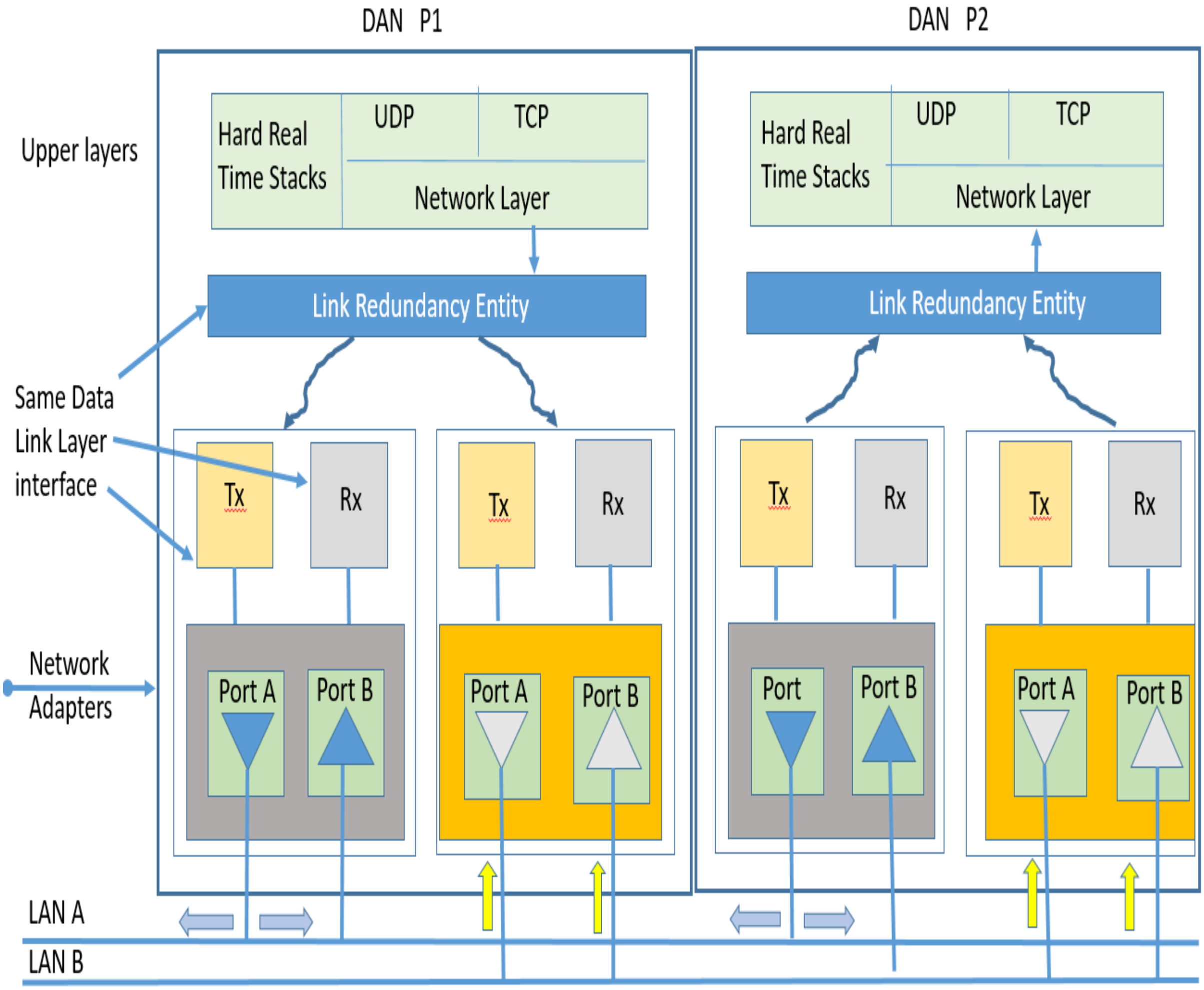


Fig. 4.2. Movement of frames in a DANP node of PRP topology.

Fig. 4.3 shows a PRP/HSR Red box device internal structure based on IEC 62439-3 protocol. Red Box or redundant box allows SANP devices to be expanded by daisy chaining IEDs and expanding a tree network, thus giving flexibility to the topology. Using a Red box, a number of SAN devices compliant to IEC 61850 protocol devices can be linked. The circulating frames pass via these Red boxes and broadcast to the intended devices in the network initiating a trip. Red boxes have the ability to filter out error-prone frames and stop them from progressing in the network while sending an alarm signal to HMI. All frames passing via this Red box having MAC addresses are identified sequential of a typical Red box; shown in Appendix 1. There are VLAN settings inbuilt in a Red box that allows GOOSE and SV frames to pass through its port.

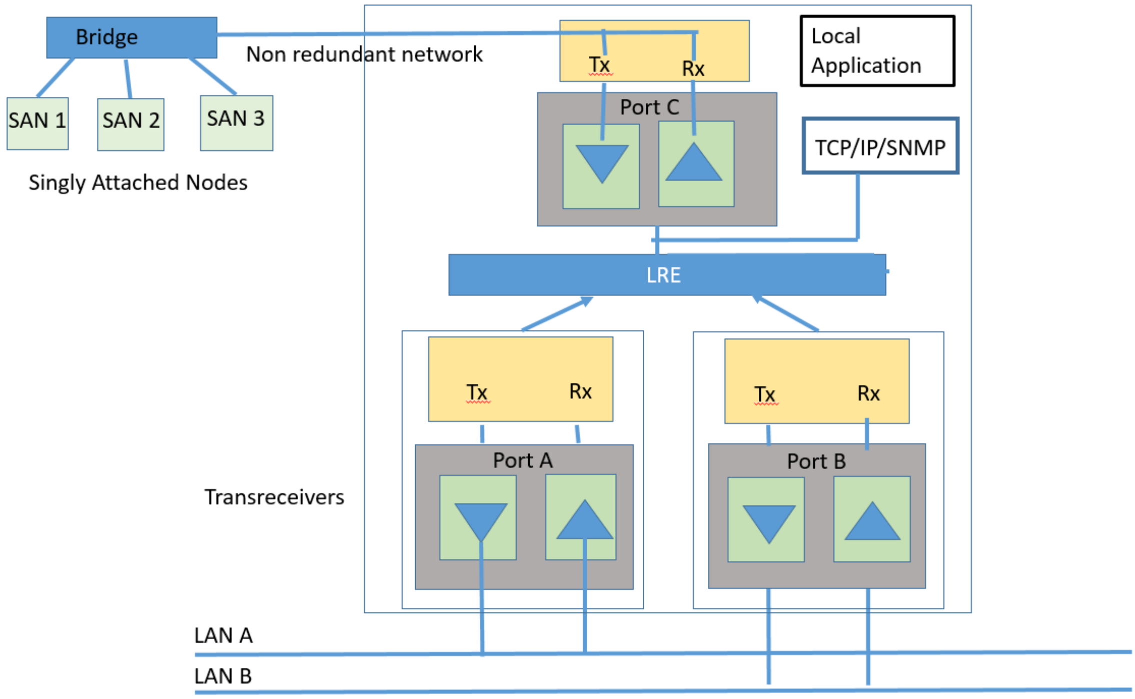


Fig. 4.3. Block diagram of a Red box.

A typical PRP frame is expected to exhibit the following traits:

- 16 bit sequence number (Seq. Nr.)
- 4 bit LAN identifier (Lanid)
- 12 bit frame size (LASDU size)
- 16 bit suffix (PRP suffix)

Any deformity in the above PRP frames results in the mal-operation of network IEDs and is deemed as a fault. Hence, it is important to have every beat of the PRP network periodically monitored. The constant parameters exhibited in a PRP network have been given in Table 2.

Table 4.2. PRP Constants [22].

Constant	Description	Default value
Lifecheck interval	Time interval between one PRP frame to another	200ms
NodeForget Tme	Time to clear a faulty node entry	6000ms
EntryForget Tme	Time taken to discard a duplicate entry	400ms
Noderebootinterval	Interval of rebooting	500ms

Prior to commissioning PRP devices in a network, they are usually tested by checking for frame’s duplicate acceptance and discard mode. These tests encompassing a PRP network give the operator confidence regarding whether the frames are actually duplicating or not in the network. Checking of the frames transmission in the network is of importance from a redundancy point of view, as the receiver supervises periodically over multiple channels which accepts or rejects duplicates. The RCT frames linked to DANP frames follow guidelines of IEEE 802.1Q related to tag frame format, management of circulating frames, encoding of congestion in the network etc. [23].

4.2.2 High Availability HSR Node Structure

HSR topology as mentioned in previous sections has a ring structure with switches, IEDs and Red boxes, all connected in a ring. As in PRP topology and in the event of a fault scenario, an HSR ring topology allow frames to circulate in an alternate path without stoppage and adaption to SAS. HSR network commands attention as it broadcasts frames in bidirectional paths and these unicast frames have high probability of getting acceptance by one of the targeted IEDs. It is stipulated in IEC 62439-3 that forwarding or propagating of frames shall occur at every 4 µs which makes the protection system really fast as compared to a conventional system. With bursts of HSR frames in the loop at a zero-fault recovery time, the isolation of the fault is rapid which ensures safety of the substation operator. This rapid isolation of fault finds application in Arc Fault protection of non-arc contained switchgears which is a gain from a safety perspective. Notwithstanding its merits, HSR ring topology has a few issues related to traffic and queuing that could slow down or cause spurious tripping of IEDs.

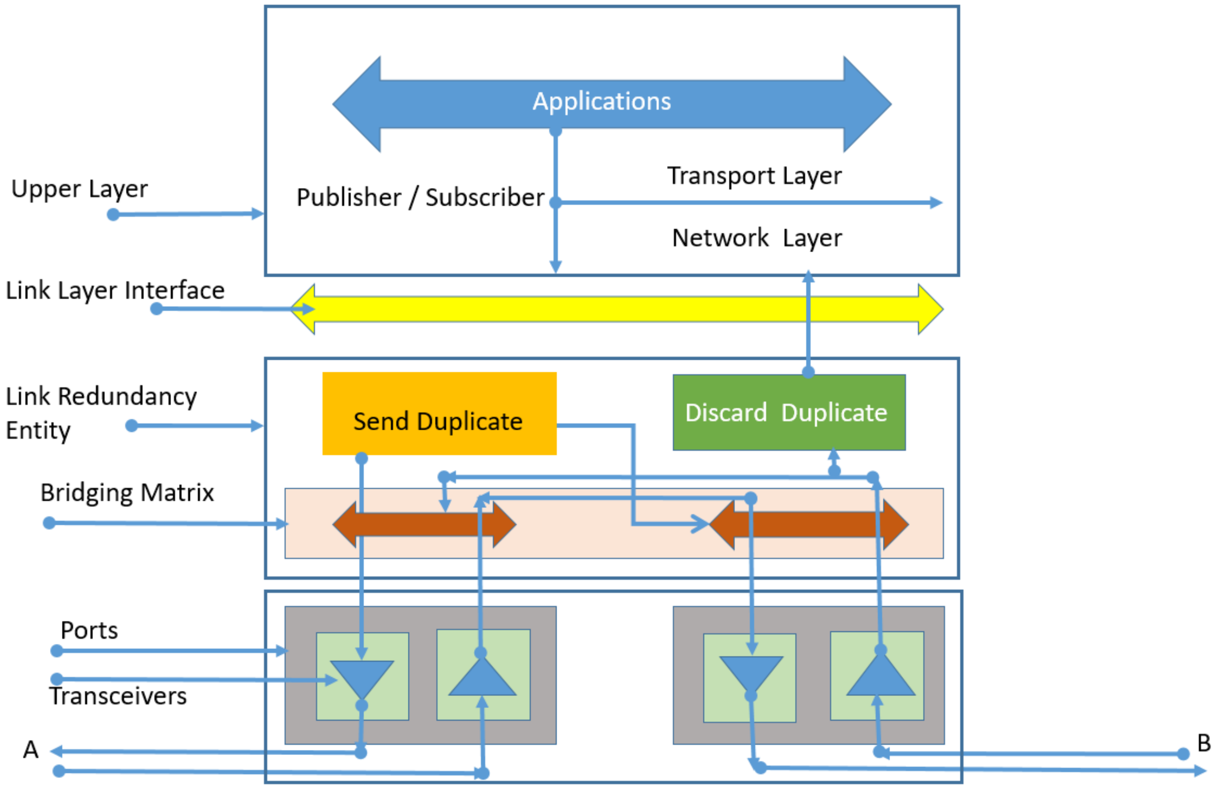


Fig. 4.4. Block Diagram of a HSR Ring Node.

In Fig. 4.4, a HSR device block diagram has been exhibited that has a bridging matrix which forwards frames to port B from port A upon its arrival. Once port B accepts and propagates it, forward LRE filters out error-prone frames and sends it to the network layer for its further application. In the above sequence, the SV frame flow is governed by IEEE 1588 V2 time synchronization guidance [24]. Although HSR provides effective SAS topology, it needs further investigation of its performance as traffic jam or latencies at nodes could cause delay in tripping the CB.

4.3 EXPERIMENTAL VERIFICATION USING OPNET TOOL

Fig. 4.5 exhibits a single line diagram (SLD) of a typical HV substation at 132/22-kV. Assumptions have been made that the SAS of this substation is of a digital network having its main protection as PRP and backup being HSR topology. The field devices have been connected in process mode and IEDs in station bus mode via switches.

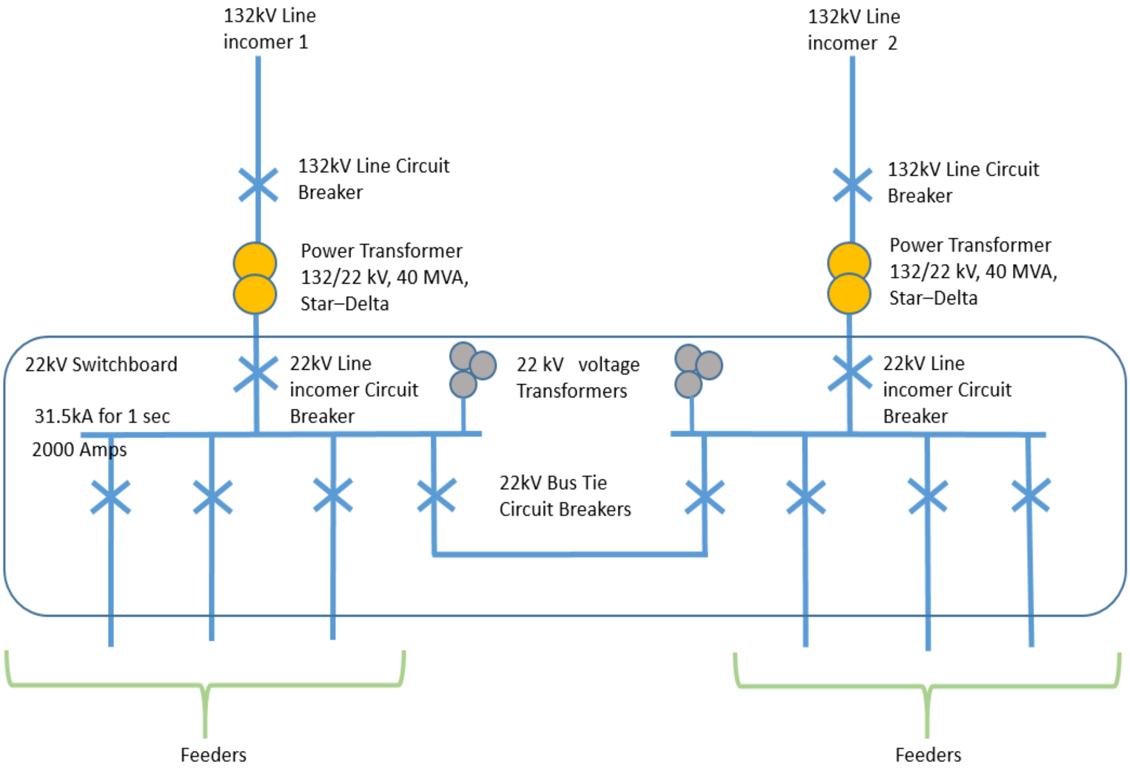


Fig. 4.5. A typical SLD of a 132/22-kV zone substation.

4.3.1 Desktop Analysis of Latencies and ETE Delays in a PRP Topology

Fig. 4.6 exhibits two LANs connected in a meshed topology with LAN A representing X and backup being Y protection, as it would usually happen in a similar conventional protection within a utility substation. Both the LANs have managed switches which have DANP and SANP devices connected via Red boxes. Field devices are connected to Mus embedded within the two LANs producing SVs. These SV frames, even if interrupted at one LAN, still could find alternate path via LAN B without interrupting the network thus achieving redundancy. All error-prone frames are filtered out by the LRE as narrated in the previous section. Internally LRE tracks and monitors PRP frames for its quality. Should a port of a PRP device get damaged, LRE shall continue to receive frames from another port while providing redundancy in protection [25].

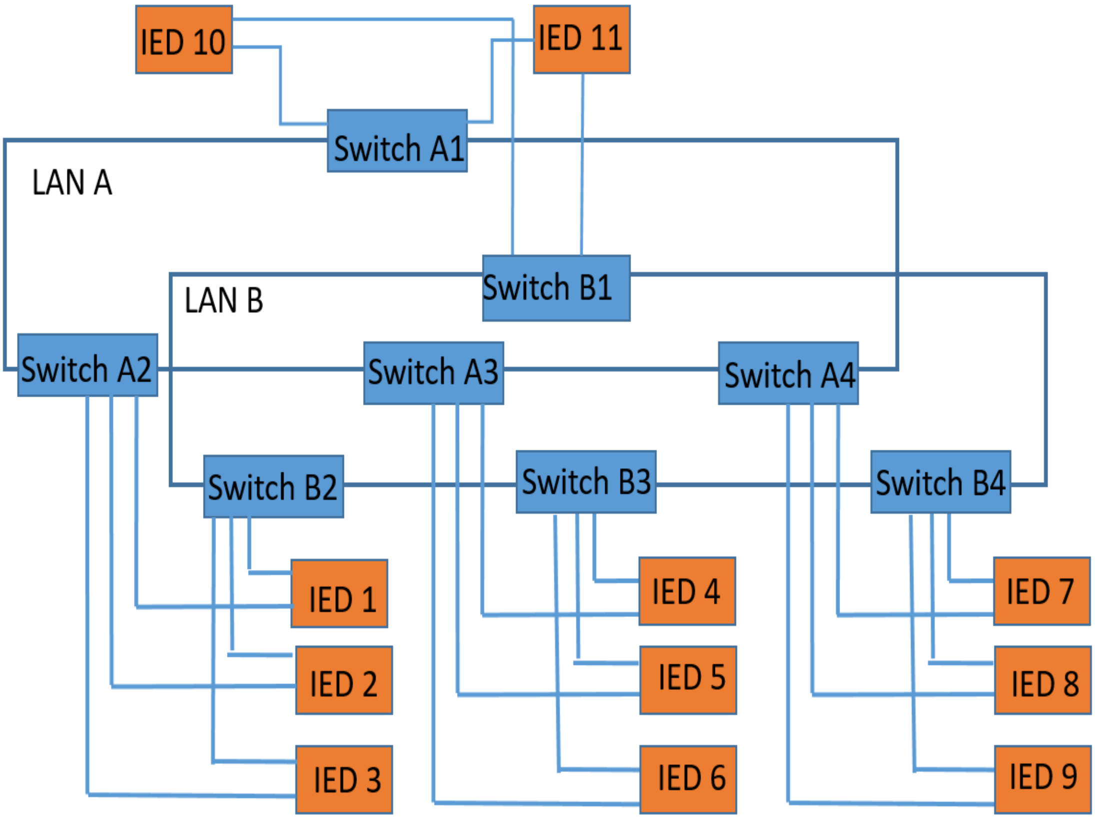


Fig. 4.6. PRP topology with two LANs offering redundancy in protection.

4.3.2 Desktop analysis of latencies and delays in HSR Topology

Fig. 4.7 exhibits an HSR topology, with its IEDs connected in DAN and SAN via a Red box in a ring structure. Broadcasting of GOOSE and SV is routed via managed switches by the subscribing IEDs. The loop is completed when the frames reach the targeted IEDs. The loss of frames is checked by the smart devices in the network at regular interval as a part of condition monitoring of the network. The bi-direction movement of frames using this protocol in high availability mode ensures redundancy has been achieved. Zero recovery time is an important feature in HSR as blockage or break in the ring causes frames to alter route and reach targeted devices, ensuring redundancy in a SAS has been achieved with no downtime.

As mentioned in the previous section, HSR ring could have issues with traffic frame flow in the ring compromising the protection of critical assets, but the compliant devices have the ability to monitor frames by scanning the network every 4 µs for error or malformed packets.

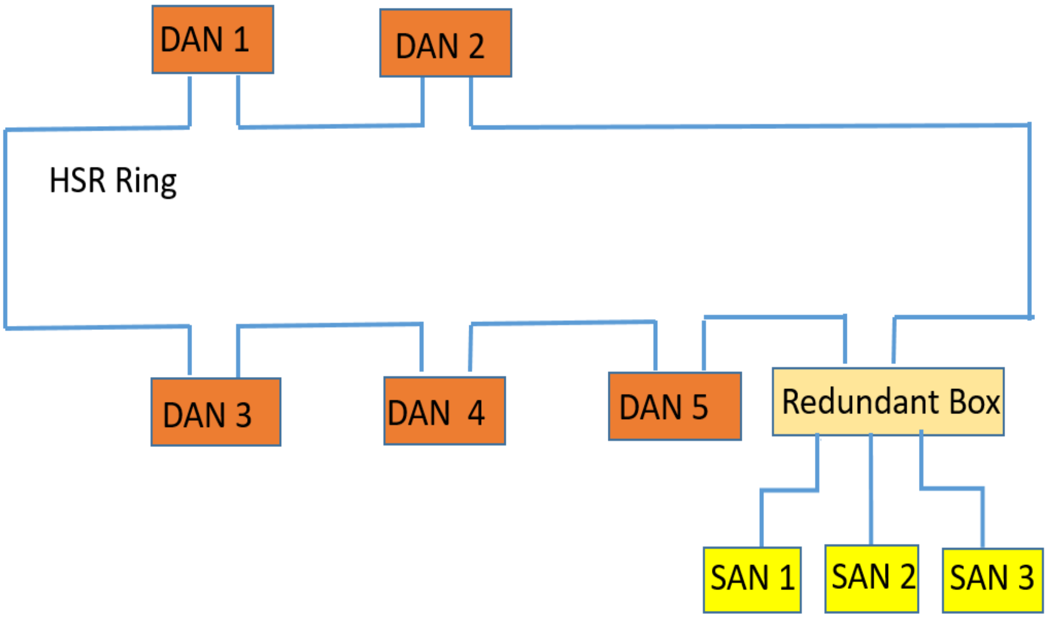


Fig. 4.7. HSR Topology connected to DAN and SAN IEDs and Red Box.

4.4 SIMULATION AND DISCUSSION

4.4.1 PRP Simulation

Fig. 4.8 shows delay in GOOSE messages when frames travel in LAN A and LAN B on an Ethernet network passing via managed switches to IEDs. In this setup GOOSE messages pass via a number of switches and devices that could cause delay during high traffic [26].

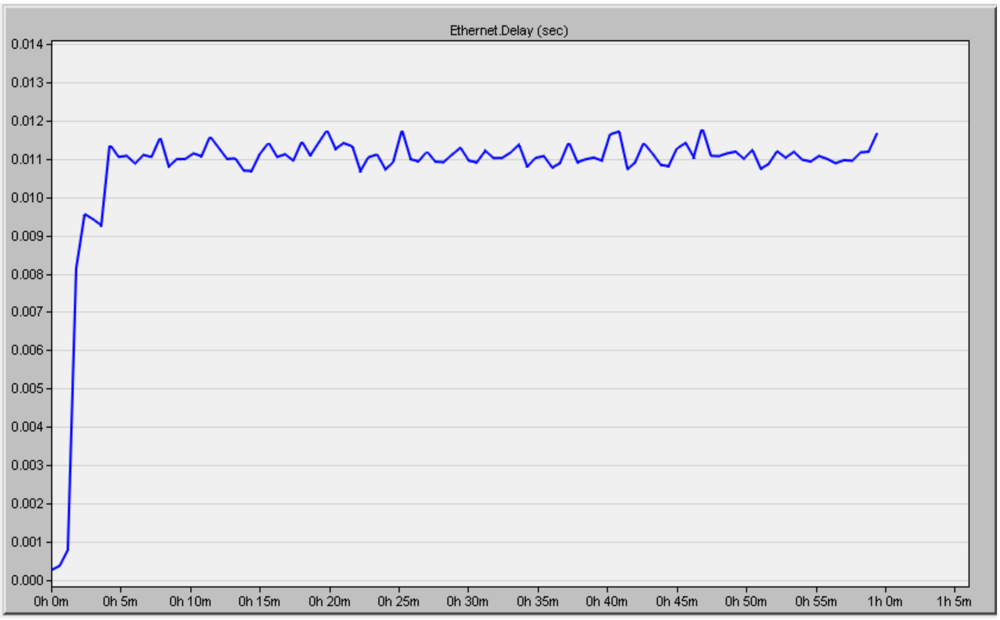


Fig. 4.8. PRP topology- Average Ethernet delay.

Fig. 4.9 exhibits overall End-to-End (ETE) delay of GOOSE frames captured by an OPNET simulator.

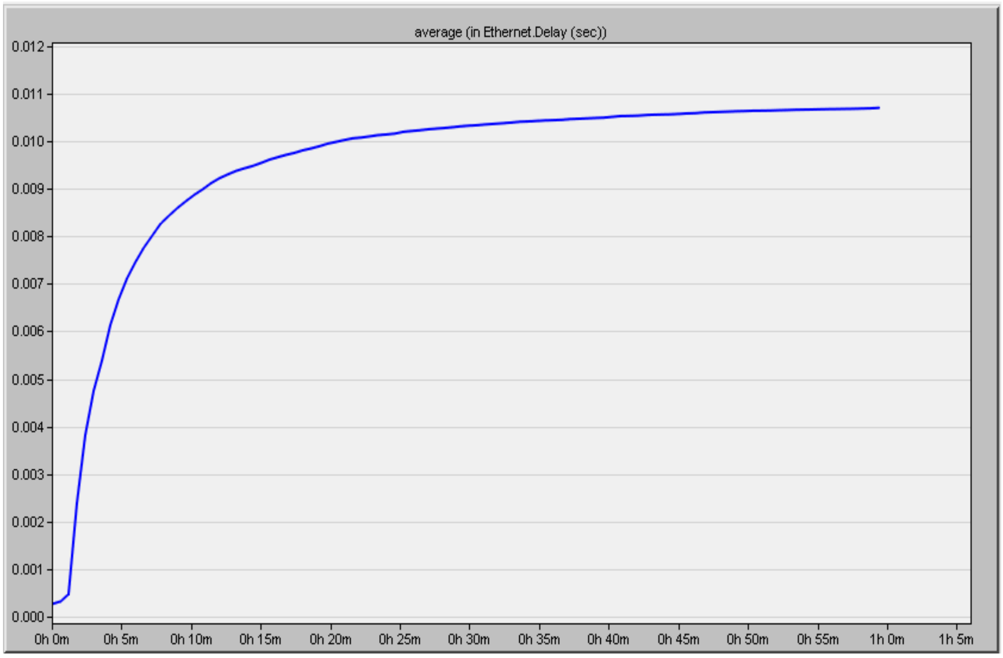


Fig. 4.9. PRP topology – ETE delay.

4.4.2 HSR Simulation

Figs. 4.0 and 4.11 exhibit average and ETE delays of GOOSE when frames circulate in a ring topology and pass via DAN and SAN devices. A Red box connected with SAN devices checks for network compatibility with IEC 61850 devices.

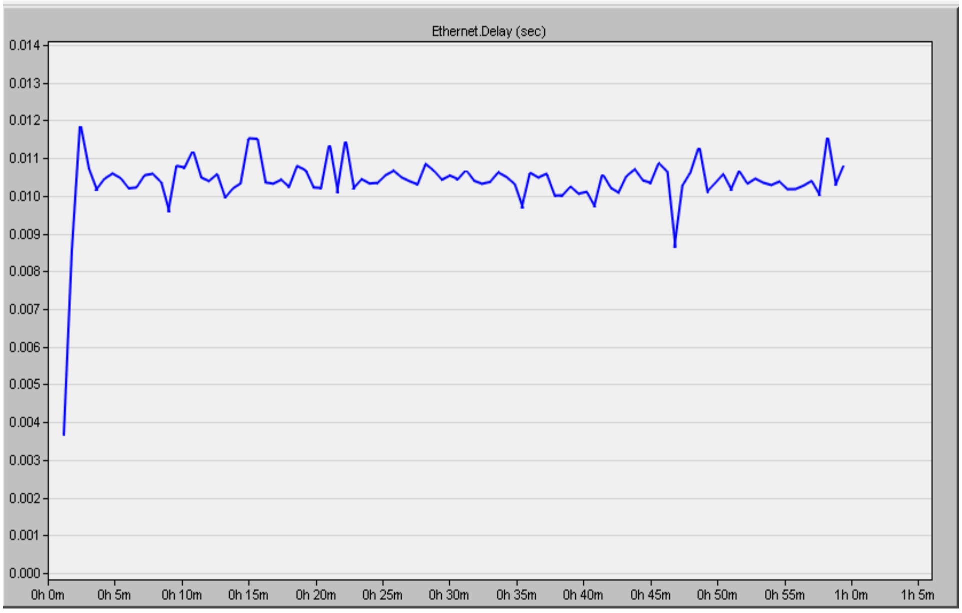


Fig. 4.10. HSR topology – average Ethernet delay.

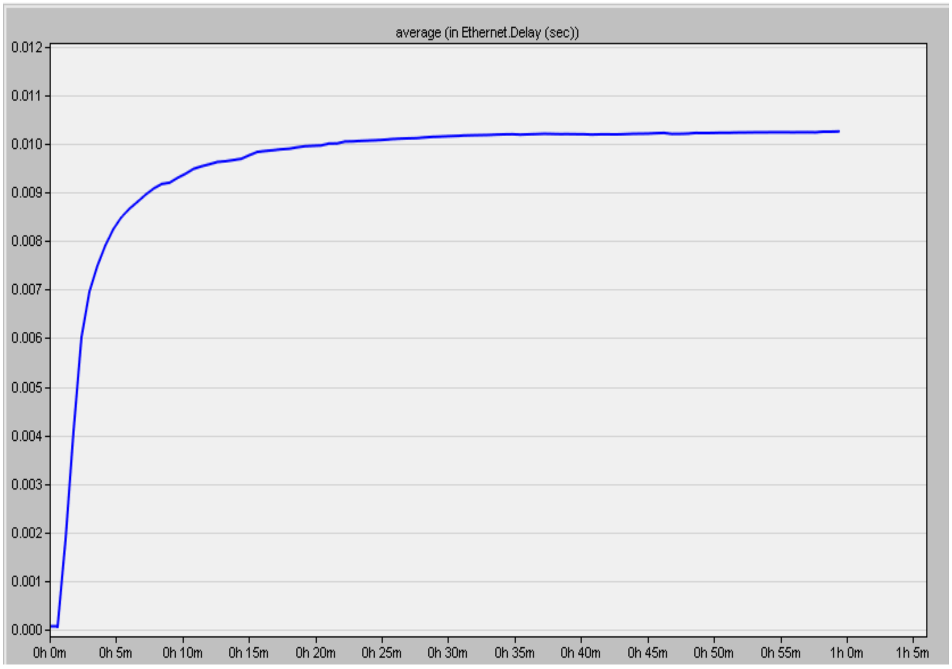


Fig. 4.11. HSR topology – average ETE delay.

The parameters that were set for GOOSE frame simulation have been exhibited in Table. 4.3.

Table 4.3. Parameters used in OPNET simulation in PRP and HSR topologies.

	PRP	HSR
Events	3,001,723	2,233,179
Average Speed (events/sec)	669,454	675,155
Time elapsed (sec)	3.3	3.1
Duration of simulation (hrs)	1	1
DES Log	5 entries	5 entries

The analysis shows that GOOSE frame passages to targeted IEDs are faster in HSR than PRP owing to less complexity of the infrastructure. However, HSR topologies' reliability is less as compared with PRP. Duplication of ring in the form of two LANs gives the option of redundancies to a PRP topology but is more complex than HSR with a number of managed switches in the nodes providing redundancies and resilience to the network. HSR is more applicable in industries and process plants where redundancy is of lesser concern while PRP could be applied in utilities were redundancy and fault tolerance of high importance. Red boxes exhibited in previous Fig. 4.6 ensure compatibility with IEC 61850 devices and provide flexibility to the network while ensuring Zero delay to changeover at the time of interruption of the frame satisfying the SAS requirement [27].

The study and desktop research were carried out with an assumption of GOOSE frames travelling in a station bus topology. The tolerance to manage a frame arrival delay during a control and measurement event is 100 ms while for a fault event it is 5 ms. The simulation demonstrated the importance of Red box in the network from an expandability perspective; without compromising the digital protection features and proved resilient to single network component failure while redundancy is maintained. Time synchronization modules could be added to the simulation while carrying simulation in LANs involved in PRP topology.

4.5 EXPERIMENTAL RESULT USING A PRP TOPOLOGY (WIRED) VERSUS WIRELESS (LINUX)

This section of the chapter focuses on practical experimental research involves process bus topology based on IEC 62439-3. In order to compare the advantages of wired vs wireless topology, the practical experiment was set up with PRP topology in wired mode for protection at substation A and wireless protection in substation B with both substations being 5 kms apart as shown in Fig. 4.12 of these two wide area substations (WAN). As per the IEC 62439-3 guideline, As mentioned in previous sections, PRP with fast-acting changeover at zero time and bumpless recovery time during a fault, provides superior redundancy features in a SAS network; this was experimented practically to validate its performance when a link failure occurred.

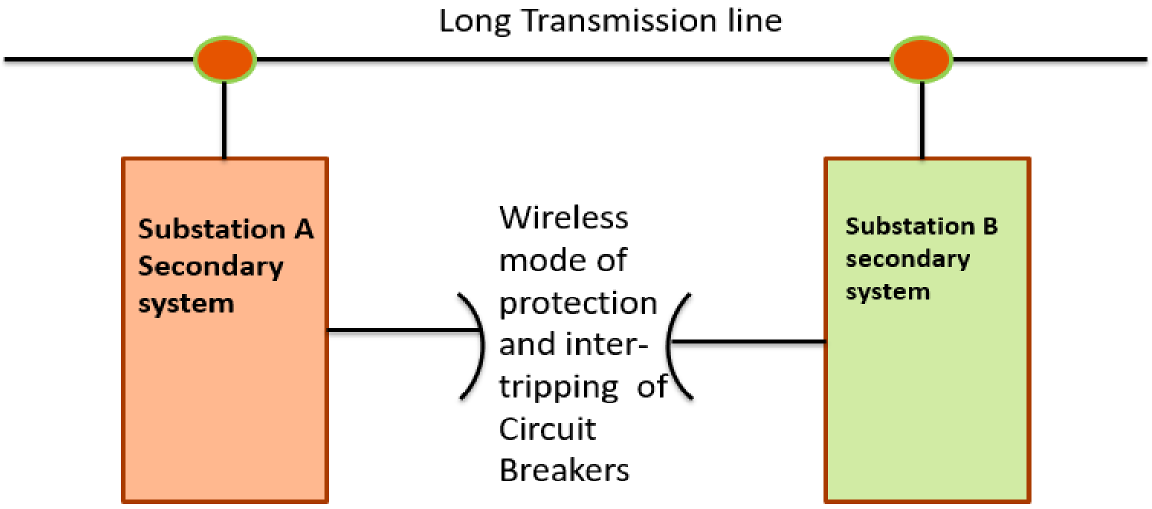

Long Transmission line
Substation A Secondary system
Wireless mode of protection and inter-tripping of Circuit Breakers
Substation B secondary system

Fig. 4.12. Wireless mode of communication between two substations.

Fig. 4.13 shows two substations connected in PRP topology in LAN A and LAN B. SAN devices compatible to IEC 61850 protocol have been used in this topology along with DANP devices and managed switches. The experimental setup exhibits time taken to switch over from wired to wireless mode of protection in the event of fault. Time synchronization has been linked to IEEE 1588 guideline.

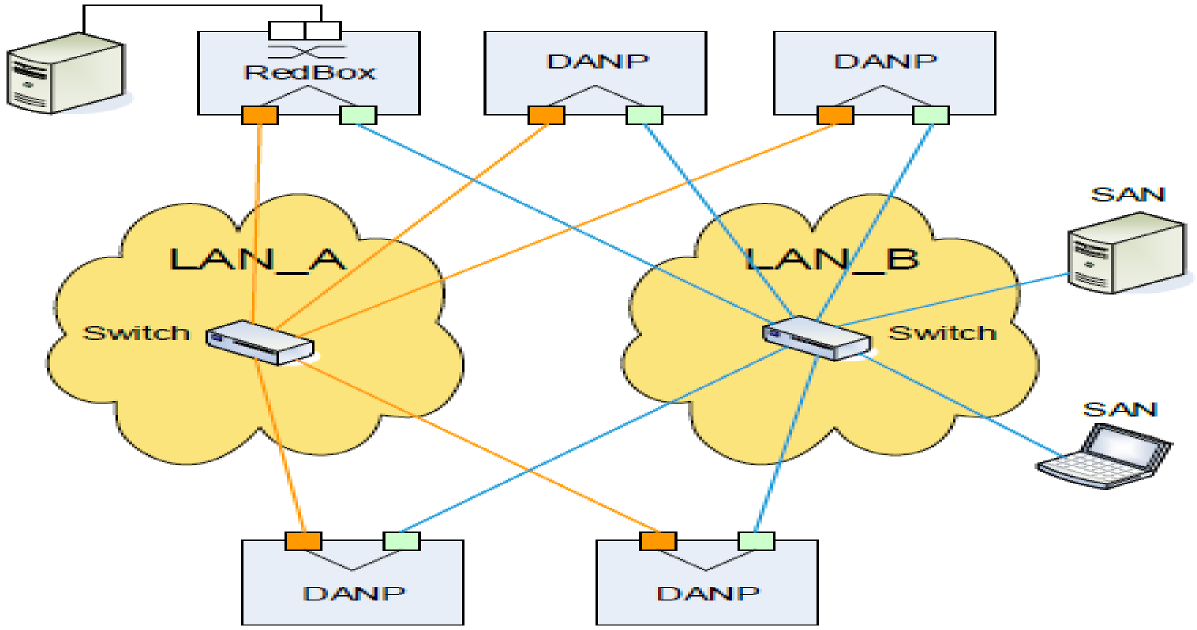


Fig. 4.13. Protection scheme using PRP topology.

The smartness of Red box ensures that error-prone frames are filtered out at the nodes for truncated and malformed frames. Media Access Controller (MAC) located in PRP-compliant devices with PRP topology consider byte sizes and sequence numbers to detect healthy frames and switch over to another LAN during a fault with zero frame loss. This experiment attempts to exhibit field conditions and prove practical situation which consists of impairments or errors upon reaching targeted nodes. The experiment highlights the impact of errors and impairment as it could have serious effects on the SAS network during a fault [28].

Redundancy Control Trailer (RCT) embedded within digital packet is an important feature of PRP topology. Change or malformation of a RCT packet could have serious repercussion on the protection scheme. Fig. 4.14 shows the structure of a RCT within PRP frame which consists of sequence number, LAN and LSDU

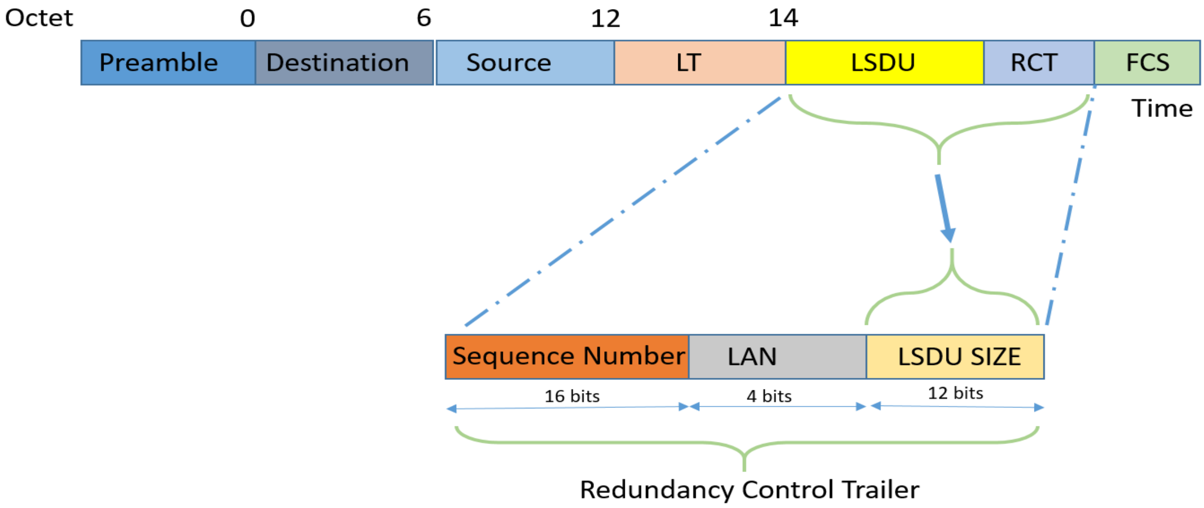


Fig. 4.14. Block diagram of PRP frame with RCT.

A laboratory experiment at Curtin University to IEC 62439-3 was conducted to test wired versus wireless mode of frame circulation and the arrival with time-based key messages. All type-1 messages have been outlined in the standard and the experiment validates the time-critical message arrival at destination.

Following scenarios for GOOSE and SV travelling in wired and wireless mode have been assumed:

- Delays in frame arrival at the destination node
- Circulating speed of SV frames in the SAS network
- Detection of errors and impairment of SV data packets
- Corrupted SV digital packets

Fig. 4.15 shows a practical lab set-up used for simulating tests on two WAN substations with the focus on errors and impairment using digital schemes [29].

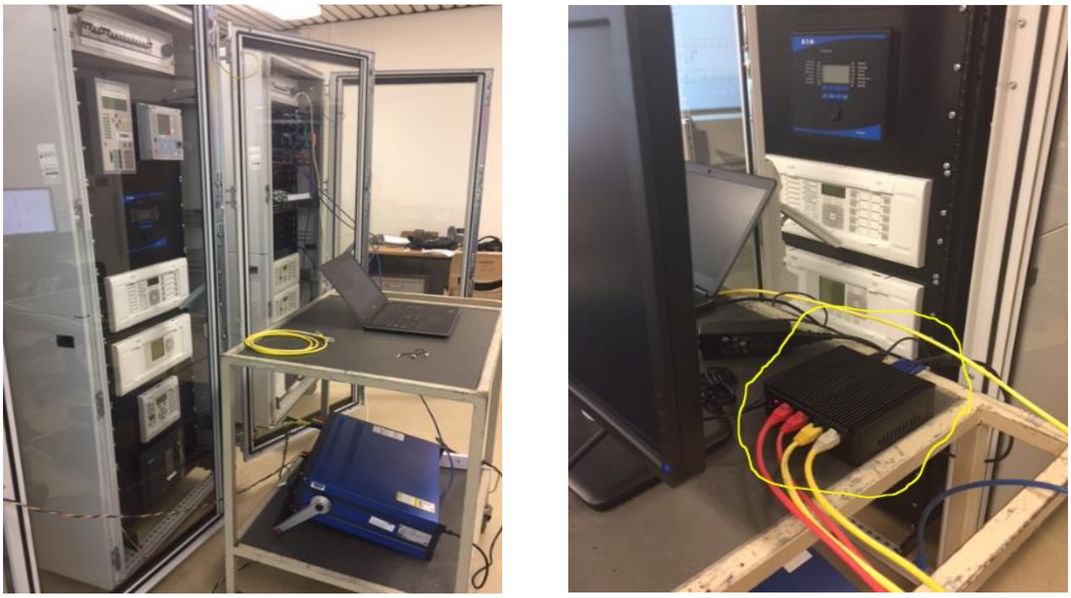


Fig. 4.15. Experimental set-up of the two WAN substation.

In Fig. 4.16 the test apparatus has been shown with an Omicron Energy CMC 356 (Blue box) kit performing as the secondary of voltage transformer (VT). In actual substation this VT would have a ratio of 110/√3 i.e., 63.5V. An under-voltage condition (ANSI code 27) was created and an injection of 90% of nominal voltage was carried out into an ABB make MU i.e., 57.15V. Tabulation of the delay at nodes and tripping time were recorded (Δ*t* in ms). The actual flow of this injection has been shown in Fig. 4.14 with number of IEDs shown. The total processing time involves time taken internally at the IED to process, travel over the Ethernet network, time of receiving at WAN substation B and time taken for the receiving IED to latch its trip contact.

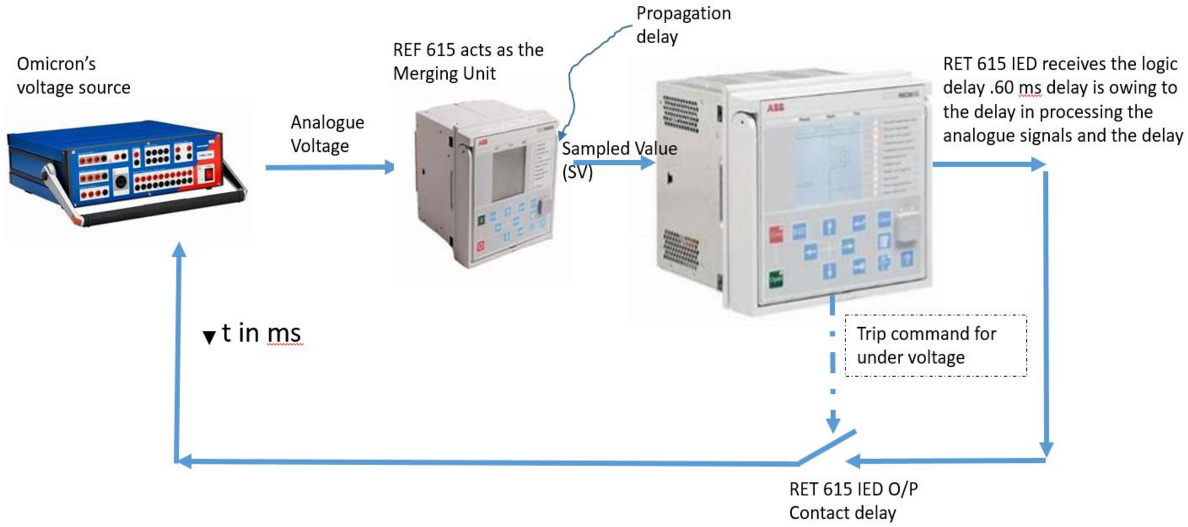

Propagation delay
Omicron's voltage source
REF 615 acts as the Merging Unit
RET 615 IED receives the logic delay .60 ms delay is owing to the delay in processing the analogue signals and the delay
Analogue Voltage
Sampled Value (SV)
▾t in ms
Trip command for under voltage
RET 615 IED O/P Contact delay

Fig. 4.16. Total time taken for an SV frame transmission over a wired network to reach WAN substation B.

Different scenarios were enacted to understand the delay.

Case 1: when the SV frame reach its destination without impairment or error.

Fig. 4.17 shows analogue signals from CMC 356 box converted by an ABB MU converting the packets to SV which travels over Ethernet wires as SV digital packets.

Fig. 4.17 exhibits transmission of frame packets from substation A over an Ethernet network connected to ABB make IED in substation B. As mentioned in previous section, latencies, delay, and impairment of the SV frames could have a serious effect on the IED and this is detected using a Wireshark tool linked to the managed SEL switch at point A or B or C depending upon different cases under review. Capturing of healthy SV frames were carried out using a Wireshark tool having a laptop connected to the network.

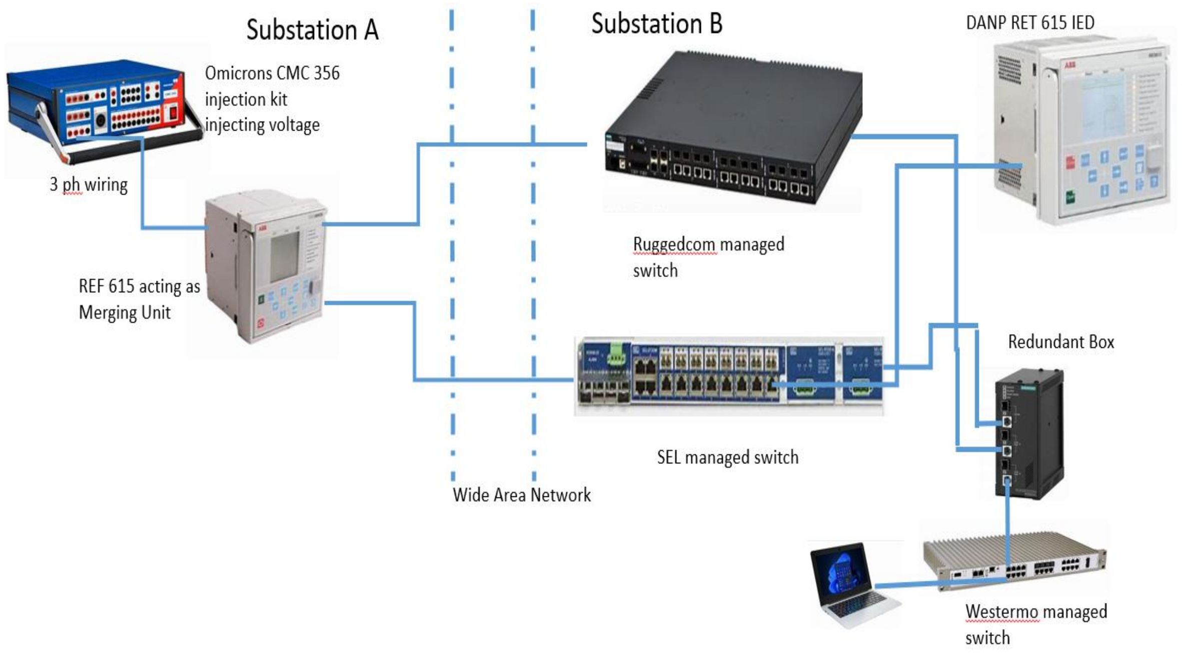
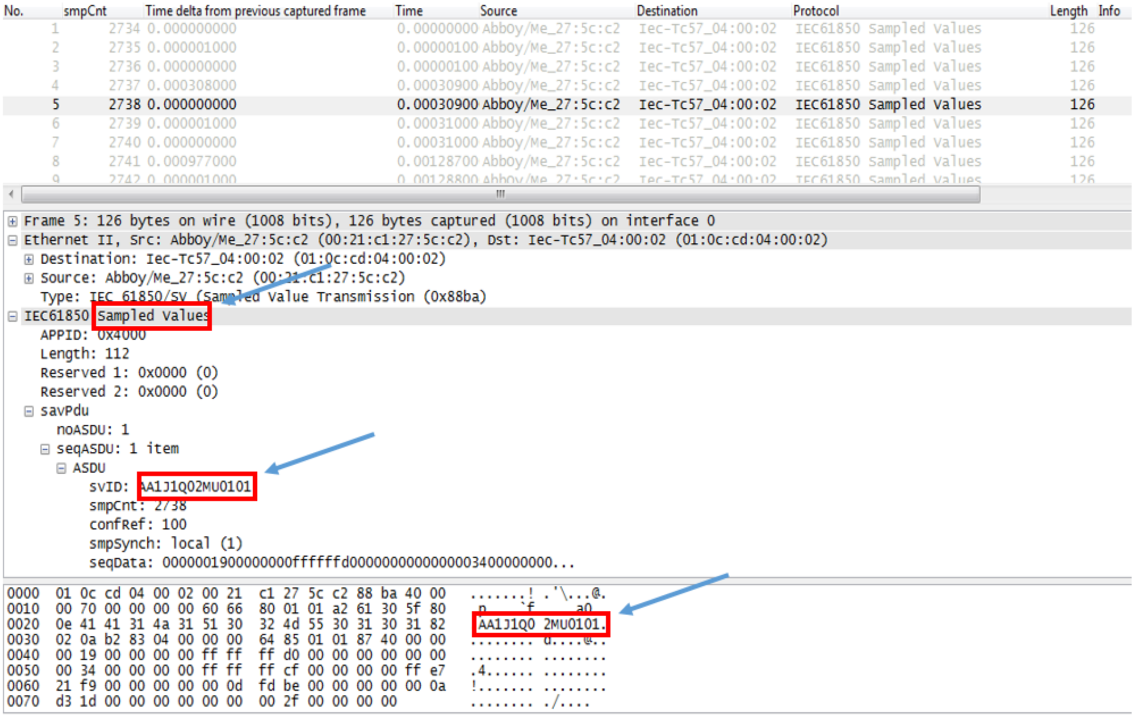


Fig. 4.17. Substation A and B with Linux tool in its system.

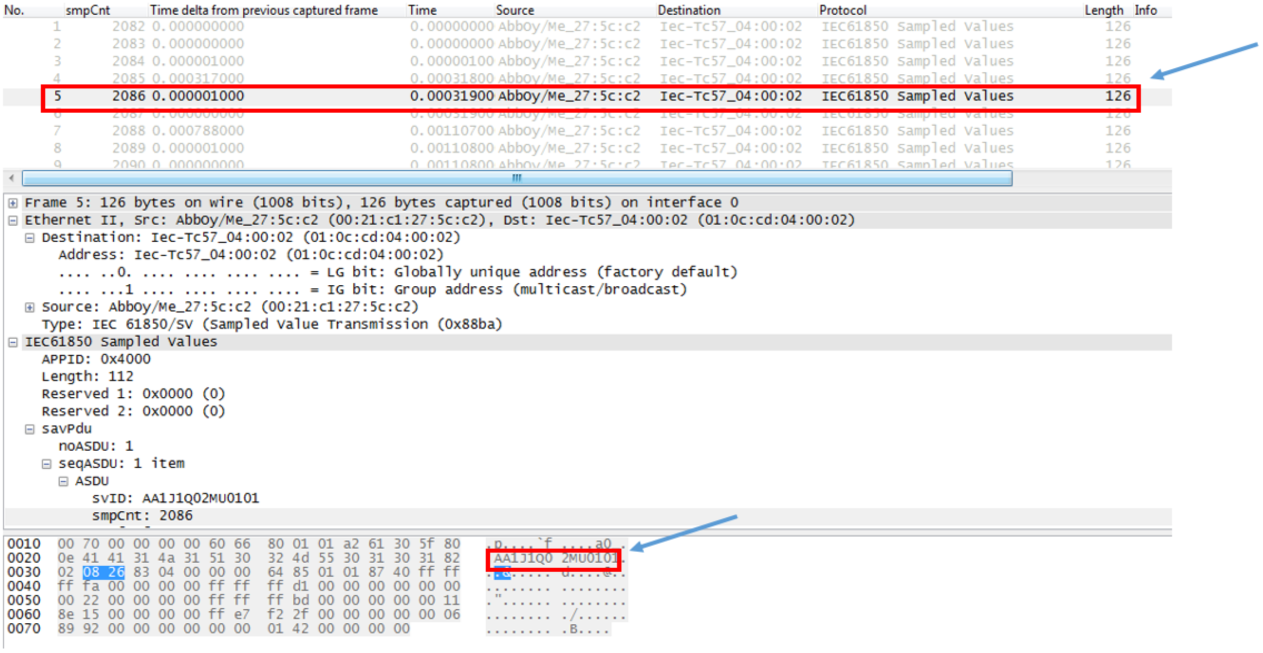
In the first case and as shown in Figs. 4.18 and 4.18 the network is error free, and frames are healthy. The technical keys of ABB MU and IED and flow of SV frames are shown in the screenshot in the WAN substation A.



```
No.   smpCnt  Time delta from previous captured frame   Time       Source              Destination         Protocol                 Length  Info
   1    2734 0.000000000                                0.00000000 Abboy/Me_27:5c:c2   Iec-Tc57_04:00:02   IEC61850 Sampled Values    126
   2    2735 0.000001000                                0.00000100 Abboy/Me_27:5c:c2   Iec-Tc57_04:00:02   IEC61850 Sampled Values    126
   3    2736 0.000000000                                0.00000100 Abboy/Me_27:5c:c2   Iec-Tc57_04:00:02   IEC61850 Sampled Values    126
   4    2737 0.000308000                                0.00030900 Abboy/Me_27:5c:c2   Iec-Tc57_04:00:02   IEC61850 Sampled Values    126
   5    2738 0.000000000                                0.00030900 Abboy/Me_27:5c:c2   Iec-Tc57_04:00:02   IEC61850 Sampled Values    126
   6    2739 0.000001000                                0.00031000 Abboy/Me_27:5c:c2   Iec-Tc57_04:00:02   IEC61850 Sampled Values    126
   7    2740 0.000000000                                0.00031000 Abboy/Me_27:5c:c2   Iec-Tc57_04:00:02   IEC61850 Sampled Values    126
   8    2741 0.000977000                                0.00128700 Abboy/Me_27:5c:c2   Iec-Tc57_04:00:02   IEC61850 Sampled Values    126
   9    2742 0.000001000                                0.00128800 Abboy/Me_27:5c:c2   Iec-Tc57_04:00:02   IEC61850 Sampled Values    126

⊞ Frame 5: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits) on interface 0
⊟ Ethernet II, Src: Abboy/Me_27:5c:c2 (00:21:c1:27:5c:c2), Dst: Iec-Tc57_04:00:02 (01:0c:cd:04:00:02)
  ⊞ Destination: Iec-Tc57_04:00:02 (01:0c:cd:04:00:02)
  ⊞ Source: Abboy/Me_27:5c:c2 (00:21:c1:27:5c:c2)
    Type: IEC 61850/SV (Sampled Value Transmission (0x88ba)
⊟ IEC61850 Sampled Values
    APPID: 0x4000
    Length: 112
    Reserved 1: 0x0000 (0)
    Reserved 2: 0x0000 (0)
  ⊟ savPdu
      noASDU: 1
    ⊟ seqASDU: 1 item
      ⊟ ASDU
          svID: AA1J1Q02MU0101
          smpCnt: 2738
          confRef: 100
          smpSynch: local (1)
          seqData: 0000001900000000ffffffd000000000000000003400000000...

0000  01 0c cd 04 00 02 00 21  c1 27 5c c2 88 ba 40 00   .......! .'\...@.
0010  00 70 00 00 00 00 60 66  80 01 01 a2 61 30 5f 80   .p....`f ....a0_.
0020  0e 41 41 31 4a 31 51 30  32 4d 55 30 31 30 31 82   .AA1J1Q0 2MU0101.
0030  02 0a b2 83 04 00 00 00  64 85 01 01 87 40 00 00   ........ d....@..
0040  00 19 00 00 00 00 ff ff  ff d0 00 00 00 00 00 00   ........ ........
0050  00 34 00 00 00 00 ff ff  ff cf 00 00 00 00 ff e7   .4...... ........
0060  21 f9 00 00 00 00 00 0d  fd be 00 00 00 00 00 0a   !....... ........
0070  d3 1d 00 00 00 00 00 00  00 2f 00 00 00 00         ........ ./....
```

Fig. 4.18. No errors having data transmitted with no errors from near end substation 1 to far end substation 2.

Fig. 4.19 is a screen dump of SV flow in the network captured using a Wireshark tool for the far end substation B identifying its technical keys, SV frames source and destination analysing frame 2086.



```
No.   smpCnt  Time delta from previous captured frame   Time       Source              Destination         Protocol                 Length  Info
   1    2082 0.000000000                                0.00000000 Abboy/Me_27:5c:c2   Iec-Tc57_04:00:02   IEC61850 Sampled Values    126
   2    2083 0.000000000                                0.00000000 Abboy/Me_27:5c:c2   Iec-Tc57_04:00:02   IEC61850 Sampled Values    126
   3    2084 0.000001000                                0.00000100 Abboy/Me_27:5c:c2   Iec-Tc57_04:00:02   IEC61850 Sampled Values    126
   4    2085 0.000317000                                0.00031800 Abboy/Me_27:5c:c2   Iec-Tc57_04:00:02   IEC61850 Sampled Values    126
   5    2086 0.000001000                                0.00031900 Abboy/Me_27:5c:c2   Iec-Tc57_04:00:02   IEC61850 Sampled Values    126
   6    2087 0.000000000                                0.00031900 Abboy/Me_27:5c:c2   Iec-Tc57_04:00:02   IEC61850 Sampled Values    126
   7    2088 0.000788000                                0.00110700 Abboy/Me_27:5c:c2   Iec-Tc57_04:00:02   IEC61850 Sampled Values    126
   8    2089 0.000001000                                0.00110800 Abboy/Me_27:5c:c2   Iec-Tc57_04:00:02   IEC61850 Sampled Values    126
   9    2090 0.000000000                                0.00110800 Abboy/Me_27:5c:c2   Iec-Tc57_04:00:02   IEC61850 Sampled Values    126

⊞ Frame 5: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits) on interface 0
⊟ Ethernet II, Src: Abboy/Me_27:5c:c2 (00:21:c1:27:5c:c2), Dst: Iec-Tc57_04:00:02 (01:0c:cd:04:00:02)
  ⊟ Destination: Iec-Tc57_04:00:02 (01:0c:cd:04:00:02)
      Address: Iec-Tc57_04:00:02 (01:0c:cd:04:00:02)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
  ⊞ Source: Abboy/Me_27:5c:c2 (00:21:c1:27:5c:c2)
    Type: IEC 61850/SV (Sampled Value Transmission (0x88ba)
⊟ IEC61850 Sampled Values
    APPID: 0x4000
    Length: 112
    Reserved 1: 0x0000 (0)
    Reserved 2: 0x0000 (0)
  ⊟ savPdu
      noASDU: 1
    ⊟ seqASDU: 1 item
      ⊟ ASDU
          svID: AA1J1Q02MU0101
          smpCnt: 2086

0010  00 70 00 00 00 00 60 66  80 01 01 a2 61 30 5f 80   .p....`f ....a0_.
0020  0e 41 41 31 4a 31 51 30  32 4d 55 30 31 30 31 82   .AA1J1Q0 2MU0101.
0030  02 08 26 83 04 00 00 00  64 85 01 01 87 40 ff ff   ..&..... d....@..
0040  ff fa 00 00 00 00 ff ff  ff d1 00 00 00 00 00 00   ........ ........
0050  00 22 00 00 00 00 ff ff  ff bd 00 00 00 00 00 11   ."...... ........
0060  8e 15 00 00 00 00 ff e7  f2 2f 00 00 00 00 00 06   ........ ./......
0070  89 92 00 00 00 00 00 00  01 42 00 00 00 00         ........ .B....
```

Fig. 4.19. Situation and SV packet flow at the far end substation detected by Wireshark tool.

Case 2: a radio wireless setup was carried out to understand the issues when there are errors and impairments while connecting through Ethernet and wirelessly. Fig. 4.20 exhibits two linked substations embedded with a Linux tool in a laboratory environment. Impairment and delay were observed when the switch was linked to a laptop having Wireshark tool. The performance of frame circulation with error and impairment scenario gave a reasonable understanding of the digital protection scheme as applicable by wired and wireless topology.

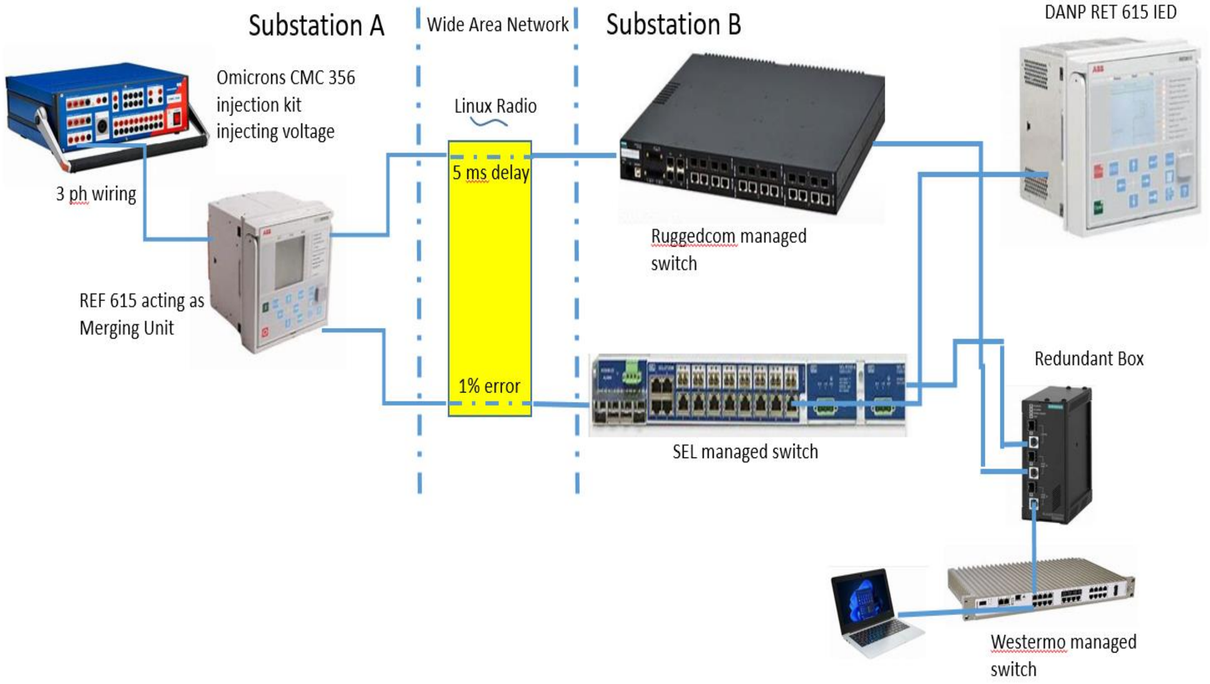
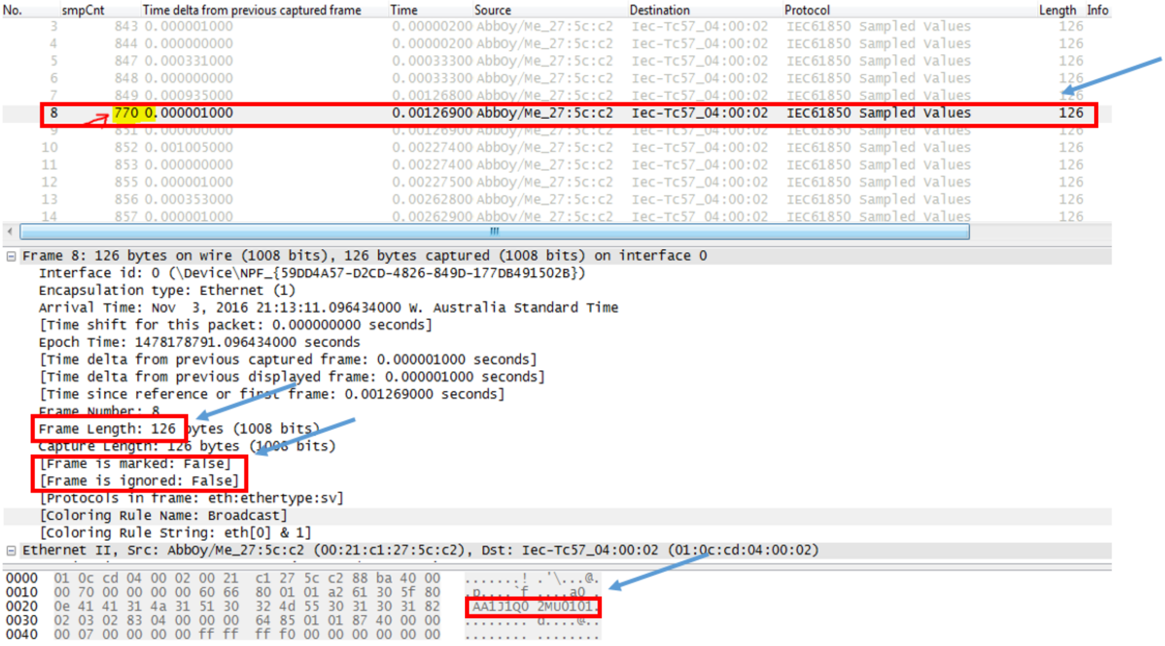


Fig. 4.20. Using Linus tool to analyse errors and impairment effect on protection scheme.

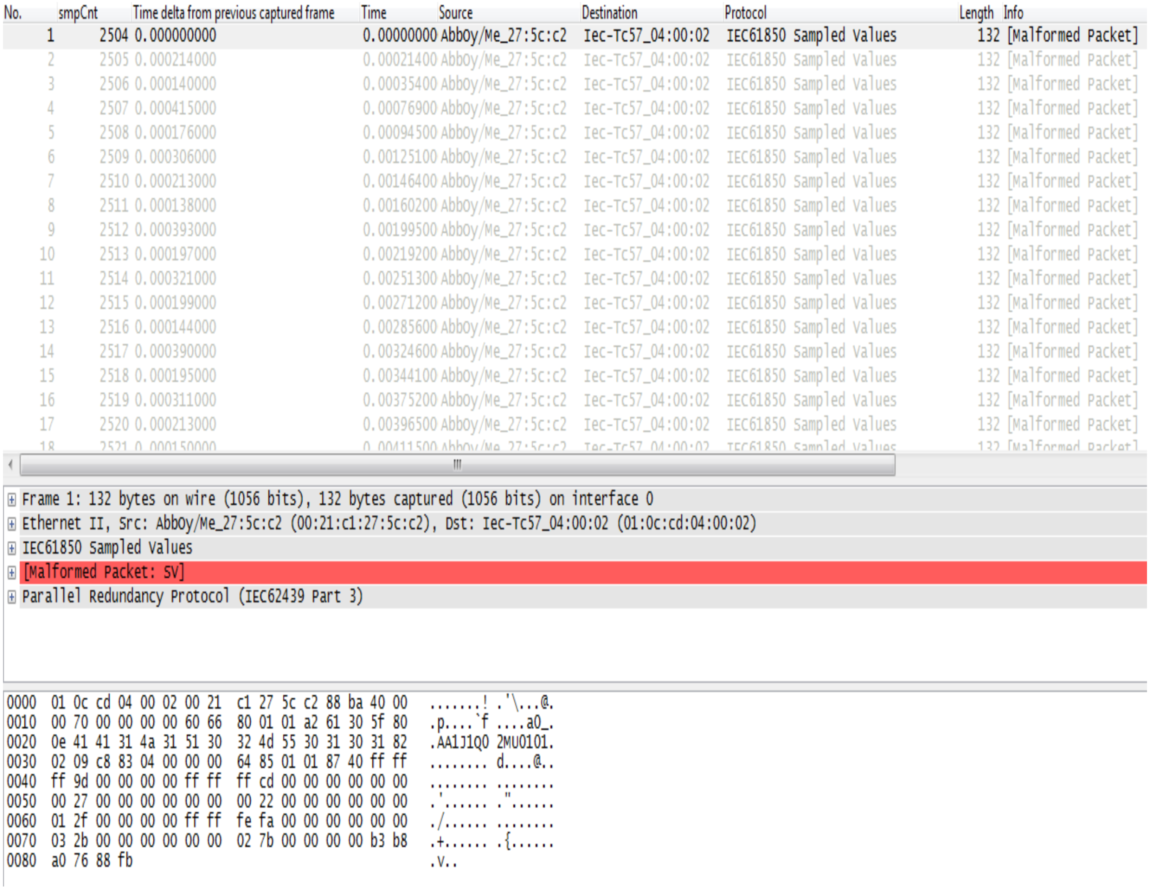
Fig. 4.21 is a screenshot using Wireshark tool when there are errors and impairment in frame transmitting towards substation B from A. The error in frames has been highlighted by frame, i.e., not correct and not healthy, is marked as 'False' indicated by a blue arrow.



```
No.   smpCnt  Time delta from previous captured frame  Time        Source                   Destination           Protocol                Length  Info
  3      843 0.000001000                               0.00000200 Abboy/Me_27:5c:c2  Iec-Tc57_04:00:02  IEC61850 Sampled Values     126
  4      844 0.000000000                               0.00000200 Abboy/Me_27:5c:c2  Iec-Tc57_04:00:02  IEC61850 Sampled Values     126
  5      847 0.000331000                               0.00033300 Abboy/Me_27:5c:c2  Iec-Tc57_04:00:02  IEC61850 Sampled Values     126
  6      848 0.000000000                               0.00033300 Abboy/Me_27:5c:c2  Iec-Tc57_04:00:02  IEC61850 Sampled Values     126
  7      849 0.000935000                               0.00126800 Abboy/Me_27:5c:c2  Iec-Tc57_04:00:02  IEC61850 Sampled Values     126
  8      770 0.000001000                               0.00126900 Abboy/Me_27:5c:c2  Iec-Tc57_04:00:02  IEC61850 Sampled Values     126
  9      851 0.000000000                               0.00126900 Abboy/Me_27:5c:c2  Iec-Tc57_04:00:02  IEC61850 Sampled Values     126
 10      852 0.001005000                               0.00227400 Abboy/Me_27:5c:c2  Iec-Tc57_04:00:02  IEC61850 Sampled Values     126
 11      853 0.000000000                               0.00227400 Abboy/Me_27:5c:c2  Iec-Tc57_04:00:02  IEC61850 Sampled Values     126
 12      855 0.000001000                               0.00227500 Abboy/Me_27:5c:c2  Iec-Tc57_04:00:02  IEC61850 Sampled Values     126
 13      856 0.000353000                               0.00262800 Abboy/Me_27:5c:c2  Iec-Tc57_04:00:02  IEC61850 Sampled Values     126
 14      857 0.000001000                               0.00262900 Abboy/Me_27:5c:c2  Iec-Tc57_04:00:02  IEC61850 Sampled Values     126

⊟ Frame 8: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits) on interface 0
    Interface id: 0 (\Device\NPF_{59DD4A57-D2CD-4826-849D-177DB491502B})
    Encapsulation type: Ethernet (1)
    Arrival Time: Nov  3, 2016 21:13:11.096434000 W. Australia Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1478178791.096434000 seconds
    [Time delta from previous captured frame: 0.000001000 seconds]
    [Time delta from previous displayed frame: 0.000001000 seconds]
    [Time since reference or first frame: 0.001269000 seconds]
    Frame Number: 8
    Frame Length: 126 bytes (1008 bits)
    Capture Length: 126 bytes (1008 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:sv]
    [Coloring Rule Name: Broadcast]
    [Coloring Rule String: eth[0] & 1]
⊟ Ethernet II, Src: Abboy/Me_27:5c:c2 (00:21:c1:27:5c:c2), Dst: Iec-Tc57_04:00:02 (01:0c:cd:04:00:02)

0000  01 0c cd 04 00 02 00 21  c1 27 5c c2 88 ba 40 00   .......! .'\...@.
0010  00 70 00 00 00 00 60 66  80 01 01 a2 61 30 5f 80   .p....`f ....a0_.
0020  0e 41 41 31 4a 31 51 30  32 4d 55 30 31 30 31 82   .AA1J1Q0 2MU0101.
0030  02 03 02 83 04 00 00 00  64 85 01 01 87 40 00 00   ........ d....@..
0040  00 07 00 00 00 00 ff ff  ff f0 00 00 00 00 00 00   ........ ........
```

Fig. 4.21. Malformed and error-prone data packets in the far end substation B.

Another case malformation of frames reaching substation B in wireless mode has been captured from a Wireshark screenshot as exhibited in Fig. 4. 22 and highlighted.



```
No.  smpCnt  Time delta from previous captured frame  Time        Source             Destination        Protocol                 Length  Info
  1    2504 0.000000000                               0.00000000 Abboy/Me_27:5c:c2 Iec-Tc57_04:00:02 IEC61850 Sampled Values    132 [Malformed Packet]
  2    2505 0.000214000                               0.00021400 Abboy/Me_27:5c:c2 Iec-Tc57_04:00:02 IEC61850 Sampled Values    132 [Malformed Packet]
  3    2506 0.000140000                               0.00035400 Abboy/Me_27:5c:c2 Iec-Tc57_04:00:02 IEC61850 Sampled Values    132 [Malformed Packet]
  4    2507 0.000415000                               0.00076900 Abboy/Me_27:5c:c2 Iec-Tc57_04:00:02 IEC61850 Sampled Values    132 [Malformed Packet]
  5    2508 0.000176000                               0.00094500 Abboy/Me_27:5c:c2 Iec-Tc57_04:00:02 IEC61850 Sampled Values    132 [Malformed Packet]
  6    2509 0.000306000                               0.00125100 Abboy/Me_27:5c:c2 Iec-Tc57_04:00:02 IEC61850 Sampled Values    132 [Malformed Packet]
  7    2510 0.000213000                               0.00146400 Abboy/Me_27:5c:c2 Iec-Tc57_04:00:02 IEC61850 Sampled Values    132 [Malformed Packet]
  8    2511 0.000138000                               0.00160200 Abboy/Me_27:5c:c2 Iec-Tc57_04:00:02 IEC61850 Sampled Values    132 [Malformed Packet]
  9    2512 0.000393000                               0.00199500 Abboy/Me_27:5c:c2 Iec-Tc57_04:00:02 IEC61850 Sampled Values    132 [Malformed Packet]
 10    2513 0.000197000                               0.00219200 Abboy/Me_27:5c:c2 Iec-Tc57_04:00:02 IEC61850 Sampled Values    132 [Malformed Packet]
 11    2514 0.000321000                               0.00251300 Abboy/Me_27:5c:c2 Iec-Tc57_04:00:02 IEC61850 Sampled Values    132 [Malformed Packet]
 12    2515 0.000199000                               0.00271200 Abboy/Me_27:5c:c2 Iec-Tc57_04:00:02 IEC61850 Sampled Values    132 [Malformed Packet]
 13    2516 0.000144000                               0.00285600 Abboy/Me_27:5c:c2 Iec-Tc57_04:00:02 IEC61850 Sampled Values    132 [Malformed Packet]
 14    2517 0.000390000                               0.00324600 Abboy/Me_27:5c:c2 Iec-Tc57_04:00:02 IEC61850 Sampled Values    132 [Malformed Packet]
 15    2518 0.000195000                               0.00344100 Abboy/Me_27:5c:c2 Iec-Tc57_04:00:02 IEC61850 Sampled Values    132 [Malformed Packet]
 16    2519 0.000311000                               0.00375200 Abboy/Me_27:5c:c2 Iec-Tc57_04:00:02 IEC61850 Sampled Values    132 [Malformed Packet]
 17    2520 0.000213000                               0.00396500 Abboy/Me_27:5c:c2 Iec-Tc57_04:00:02 IEC61850 Sampled Values    132 [Malformed Packet]
 18    2521 0.000150000                               0.00411500 Abboy/Me_27:5c:c2 Iec-Tc57_04:00:02 IEC61850 Sampled Values    132 [Malformed Packet]

⊞ Frame 1: 132 bytes on wire (1056 bits), 132 bytes captured (1056 bits) on interface 0
⊞ Ethernet II, Src: Abboy/Me_27:5c:c2 (00:21:c1:27:5c:c2), Dst: Iec-Tc57_04:00:02 (01:0c:cd:04:00:02)
⊞ IEC61850 Sampled Values
⊞ [Malformed Packet: SV]
⊞ Parallel Redundancy Protocol (IEC62439 Part 3)

0000  01 0c cd 04 00 02 00 21  c1 27 5c c2 88 ba 40 00   .......! .'\...@.
0010  00 70 00 00 00 00 60 66  80 01 01 a2 61 30 5f 80   .p....`f ....a0_.
0020  0e 41 41 31 4a 31 51 30  32 4d 55 30 31 30 31 82   .AA1J1Q0 2MU0101.
0030  02 09 c8 83 04 00 00 00  64 85 01 01 87 40 ff ff   ........ d....@..
0040  ff 9d 00 00 00 00 ff ff  ff cd 00 00 00 00 00 00   ........ ........
0050  00 27 00 00 00 00 00 00  00 22 00 00 00 00 00 00   .'...... ."......
0060  01 2f 00 00 00 00 ff ff  fe fa 00 00 00 00 00 00   ./...... ........
0070  03 2b 00 00 00 00 00 00  02 7b 00 00 00 00 b3 b8   .+...... .{......
0080  a0 76 88 fb                                        .v..
```

Fig. 4.22. Wireshark capture of malformed packet at substation B.

A 10% error and 20 ms delay were deliberately injected in the laboratory setup network with laptop connected to a switch C. It was observed that errors and delays were well within the acceptable limit, as tabulated in Table 4.4.

A summary of different cases has been tabulated in Table 4.4 in a wireless and wired set up for the two substations.

Table 4.4. Tabulation of delay propagation with frames having errors, delay, and impairment under different cases in two HV substations.

Multiple Scenarios	**Delay in propagation (∆t in ms)**
a) when two substations are in WAN connection without errors in packets	11
b) with Ethernet and Fibre optic links have been disconnected during a fault	17
c) When frames arrive at substation B IED after 7 ms delay (wirelessly) while substation A frames arrive at IEDs with no errors.	15
d) When frames arrive at substation B IED after 5 ms delay (wirelessly) while substation A frames arrive at IED with errors.	19
e) When frames arrive at substation B IED after 19 ms delay (wirelessly) while substation A frames can't reach due to disconnection.	33
f) When frames arrive at substation A and B after 19 ms delay but having no error in frames	19
g) When frames arrive at substation A & B with 9% error and 19 ms delay	23
h) When frames arrive at substation A IED 9% error and a 19 ms delay (wirelessly) at LAN B.	incorrect and malfunction of IED results

4.6 RESULTS AND DISCUSSION ON WIRED VERSUS WIRELESS PROTECTION USING PRP TOPOLOGY

The expectation of operators has always been such that the SAS works reliably and quickly during a fault event. In digital systems data packets suffer from errors, impairment, traffic congestion which is experimentally proven to retain the confidence of the operator. Table 4.4 summarises the different scenario of errors, latencies, and impairment in a wired and wireless mode when an experimental setup was conducted in a laboratory environment.

In spite of tabulating all kinds of scenarios in Table 4.4 the net result due to impairment and errors worked out to be 17ms. With the IEDs with proprietary features available at Curtin lab, the IED at the far end substation B couldn't handle errors and mal-operated. It was observed that by introducing delays and latencies, the IED mal-operated when operated wirelessly. PRP topology used in this lab setup not only provided back up protection but also analysed the performance of the frames circulating in a wired and wireless mode. With average delay and latency time being 17 ms under different scenarios (exhibited in Table 4.4), it is possible to transmit frames wirelessly to a far-end substation digitally without having to dig trenches and lay secondary copper wires as outlined in Table 4.5, depending upon its criticality as shown in Table 4.6 [30].

Table 4.5 Recovery time of a topology after a fault.

Time taken to recover from a fault in a digital network as per the standard		
Protocol	Standard applicable	Allowable time taken to recover
STP	801.1D	= 1s
RSTP	801.w and 801. 1D	= 500ms
PRP	IEC 61439-3	0ms
HSR	IEC 61439-3	0ms

Table 4.6: Response time of a IEDs for critical and non-critical messages [31]

Message type	**Time**	**Application**
Noncritical	>10ms	Building Automation
Normal Healthy frames	< 800ms	Used in SCADA/ HMI and Substation
High	<100ms	Control network
Critical	0 to < 10ms	PRP and HSR protocol

4.5. CHAPTER SUMMARY

PRP and HSR are newer topologies in a digital SAS system and there are very few substations in the world operating that leverage on IEC 62439-3 guideline. As there are very few substations based on this topology, it is necessary to validate its performance using practical and desktop modelling which is what has been this chapter's highlight. Laboratory experiments conducted to study the errors, latencies and mal-operation of digital packets indicate that protection could be achieved digitally using these topologies. Application wireless technology could provide huge benefit from the engineering and maintenance point of view. The chapter highlight has been to provide PRP and HSR protection to future substation with redundancy in SAS.

Experimental results exhibit encouraging trends in both topologies but in the opinion of the author and after verifying the results, PRP topology should be installed where redundancy is the key issue while HSR topology is best suited for industrial application where blackout for a few hours is tolerable. Regarding wireless technologies application in a SAS network, a few more tests need to be carried out due to cybersecurity and proprietary features of incompatible devices, having version and firmware upgrade issues.

Further research work has been proposed in understanding the behaviour and stability of the network during error and malformation of frames arriving at nodes. Future research work on hybrid network encompassing combination of PRP and HSR network have been recommended for faster protection and automation in Chapter 7.

4.7 REFERENCES

[1] J. A. Araujo, J. Lazaro, A. Astaloa, A. Zuloaga and N. Moeira, “Duplicate and Circulating Frames Discard Methods for PRP and HSR (IEC 62439-3),” in Proceedings of the 2013 Electricity Distribution, CIRED 2013, doi: 10.1049/cp.2013.0836, Stockholm, Sweden, 2013.

[2] C. Hoga, “Seamless Communication Redundancy of IEC 62439," in *Proceedings of The International Conference on Advanced Power System Automation and Protection 2011*, doi: 10.1109/APAP.2011.6180451, Beijing, China, 2011.

[3] "IEEE Standard for Common Requirements for High-Voltage Power Switchgear Rated Above 1000 V," in *IEEE Std C37.100.1-2018 (Revision of IEEE Std C37.100.1-2007),* vol., no., pp.1-99, 8 Feb. 2019, doi: 10.1109/IEEESTD.2019.8649794.

[4] J. A. Araujo, J. Lazaro, A. Astaloa, A. Zuloaga and A. Garcia, “PRP and HSR Version 1 (IEC 62439-3 Ed.2) Improvements and A Prototype Implementation,” in the Proceedings of 2013 Industrial Electronics Society, IECON 2013, doi: 10.1109/IECON.2013.6699845, Vienna, Austria, 2013

[5] D. N. M. Hoang and J. M. Rhee, "Comparative Analysis of IEC 62439–3 (HSR) and IEEE 802.1CB (FRER) Standards," 2021 Twelfth International Conference on Ubiquitous and Future Networks (ICUFN), Jeju Island, Korea, Republic of, 2021, pp. 231-235, doi: 10.1109/ICUFN49451.2021.9528562.

[6] G. Antonova, L. Frisk and J. C. Tournier, “Communication Redundancy for Substation Automation," in Proceedings of the 64th Annual Conference for Protective Engineers, 2012, doi: 10.1109/CPRE.2011.6035636, College Station, Texas, USA, 2012.

[7] International Standard IEC 62439-3, Edition 3.0, “Industrial Communication Networks High Availability automation networks - Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR),” 2016.

[8] Y. M. Allawi, D. Lee, K. Lee and J-K. K. Rhee. “Cost Effective Topology Design for HSR Resilient Mesh Networks,” in *Proceedings Of the Electricity Distribution (CIRED 2013), 22nd International Conference an Exhibition*, 10.1049/cp.2013.0836, Stockholm, Sweden, 2013.

[9] H. Kirrmann, P. Rietmann and S. Kunsman, “Standard IEC 61850 - Network redundancy using 62439,” Offprint of article in PAC World, Fall, 2008.

[10] S. Kumar, N. Das and S. Islam, “Causes and Mitigation of Sympathetic Tripping Phenomenon Based on IEC 61850,” *Australian Protection Symposium 2014*, Sydney, Australia, 2014.

[11] Y. M. Allawi, D. Lee, K. Lee and J-K. K. Rhee. “Cost Effective Topology Design for HSR Resilient Mesh Networks,” in Proceedings of the Electricity Distribution (CIRED 2013), 22nd International Conference an Exhibition, 10.1049/cp.2013.0836, Stockholm, Sweden, 2013.

[12] S. Kumar, N. Das and S. Islam, “Performance Evaluation of A Process Bus Architecture In A Zone Substation Based On IEC 61850-9-2,” in *Proceedings of the IEEE-PES APPEEC 2015,* Nov. 15~18, 2015, The University of Queensland, Brisbane, Queensland, Australia.

[13] S. Kumar, N. Das and S. Islam, “High Performance Communication Redundancy In A Digital Substation On IEC 62439-3 With A Station Bus Configuration,” in *Proceedings of the AUPEC2015, Sept. 27~30, 2015*, University of Wollongong, Wollongong, NSW, 2015.

[14] S. Kumar, A. Abu-Siada, N. Das and S. Islam, "A Fast and Reliable Blocked Bus Bar Protection Scheme Leveraging on Sampled Value and GOOSE Protection Based on IEC 61850 Architecture," *2021 31st Australasian Universities Power Engineering Conference (AUPEC)*, 2021, pp. 1-5, doi: 10.1109/AUPEC52110.2021.9597736.

[15] S. Kumar, N. Das and S. Islam, "Performance Evaluation of Two Interconnected High Voltage Utility Substations Using PRP Topology Based on IEC 62439-3," *2017 Australasian Universities Power Engineering Conference (AUPEC)*, 2017, pp. 1-5, doi: 10.1109/AUPEC.2017.8282401

[16] S. Kumar, N. Das and S. Islam, "Software Implementation of Two Seamless Redundant Topologies in A Digital Protection System Based on IEC 62439-3," *2016 Australasian Universities Power Engineering Conference (AUPEC)*, 2016, pp. 1-5, doi: 10.1109/AUPEC.2016.7749323

[17] S. Kumar, N. Das and S. Islam, "Implementing PRP and HSR Schemes in a HV Substation Based on IEC62439-3," *2018 Condition Monitoring and Diagnosis (CMD)*, 2018, pp. 1-5, doi: 10.1109/CMD.2018.8535663

[18] C. P. Teoh, P. Newman, G. Lloyd, H. Qin, R. Hunt, J. Mendez and T. Smith, "Process Bus Busbar Protection - A Stepping-stone Towards Digital Substations," in *PAC Worlds 2018*, Sofia, Bulgaria, 2018.

[19] G. Antonova, L. Frisk and J. C. Tournier, "Communication Redundancy for Substation Automation," 2011 64th Annual Conference for Protective Relay Engineers, 2011, pp. 344-355, doi: 10.1109/CPRE.2011.6035636.

[20] IEC 62439-3:2016 “Industrial Communication Networks — High Availability Automation networks — Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR).”

[21] Kirrmann, K. Weber, O. Kleineberg and H. Weibel, “Seamless and Low-Cost Redundancy For Substation Automation Systems (High Availability Seamless Redundancy, HSR),” in *Procedures, IEEE Power Energy Soc. Gen. Meeting, San Diego, CA, USA, Jul. 2011, pp. 1–7,* San Diego, USA, 2011.

[22] "IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems," in *IEEE Std 1588-2008 (Revision of IEEE Std 1588-2002)*, vol. no. pp.1-269, 24 July 2008, doi: 10.1109/IEEESTD.2008.4579760.

[23] Zuloaga, A. Astarloa, J. Jiménez, J. Lázaro and J. A. Araujo, “Cost-effective Redundancy for Ethernet Train Communications Using HSR,” in *Proceedings, IEEE 23rd Int. Symp. Ind. Electron. (ISIE)*, pp. 1117–1122, Istanbul, Turkey, 2014.

[24] IEC 62439-2:2010 “Industrial communication networks — High availability Automation networks — Part 2: Media Redundancy Protocol (MRP).”

[25] “Industrial Communications Networks—High Availability Automation Networks—Part 3: Parallel Redundancy Protocol (PRP) and High-Availability Seamless Redundancy (HSR), IEC Standard 62439-3", 2012.

[26] “Communication Networks and Systems for Power Utility Automation—Part 90–4: Network Engineering Guidelines, IEC Standard 61850-90-4", 2013.

[27] J. Á. Araujo, J. Lázaro, A. Astarloa, A. Zuloaga and J. I. Gárate, "PRP and HSR for High Availability Networks in Power Utility Automation: A Method for Redundant Frames Discarding," in *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2325-2332, Sept. 2015.

[28] S. Lee, J. Kang, S. S. Choi and M. T. Lim, "Design of PTP TC/Slave Over Seamless Redundancy Network for Power Utility Automation," in *IEEE Transactions on Instrumentation and Measurement*, vol. 67, no. 7, pp. 1617-1625, July 2018.

[29] S. Kumar, N. Das and S. Islam, "Comparison Between Wired Versus Wireless Mode of Digital Protection Scheme Leveraging on PRP Topology," *IEEE Sustainable Power Conference (ISPEC)*, pp. 1-5, Perth, Australia, 2022.

[30] S. Hong and I. Joe, “A Novel Packet Transmission Scheme with Different Periods According to the HSR Ring Direction in Smart Grid,” in *Proceedings, 4th Int. Conf. Future Gener. Inf. Technol. (FGIT),* Gangneug-si, Korea, Dec. 2012, pp. 95–102, Gangneug-si, Korea, 2012.

[31] IEC 61850, “Communication networks and systems in substations, Part 5: Communication requirements for functions and device models,” 1st ed., 2003.

CHAPTER 5:

IMPACT AND OPTIMISATION OF NCIT ON A DIGITAL SAS BASED ON IEC 61850

5.1 INRODUCTION

Advancement in SAS technology are having a huge impact on the modern power systems particularly on zone and transmission substations. IEC 61850 standards ensure consistent communication and integration between Process bus equipment in the field and IEDs in the control room in a substation environment. One of the key process plant equipment that have a huge impact on SAS has been identified to be instrument transformers. Issues with Conventional Instrument Transformers (CIT) suffering catastrophic failure due to open circuit of secondary terminals cause safety hazards and lead to explosions, significant environmental effects due to release of mineral insulating oil or release of SF6 gas into the atmosphere, time-consuming diagnostics etc. As a result, researchers have come up with novel solutions [1]. While experimental results recommend NCIT being superior in performance to CIT, additional tests are required before its mass deployment across utilities and industries.

Through experimental research, validation, application in the network, NCIT shall gain over the confidence of operators from improved safely, decreased project cost, and optimised maintenance cost from a substation environment perspective. In this chapter a real-life SAS simulation involving NCIT at the Curtin University laboratory, testing and interoperability checks with network IEDs and switches, were evaluated including latencies and delays. Also, a simulation has been conducted on a desktop model using an OPNET tool to validate the delay and latencies as the frames circulate in the digital network. The results seem to be encouraging and within the laboratory environment and these experimental results recommend its installation in a HV substation.

5.2 BACKGROUND OF NCIT AND PROCESS BUS

Fault identification and fast isolation of a healthy network from the faulted one is the essence of any protection scheme. In a fault scenario the circuit must be isolated in the fastest possible time. Usually, a root cause analysis and 5 “why” technique is carried out by the reliability team to learn the lesson [2]. Traditional ways of fault recording, analysing, and conducting diagnostics have their own challenges and it becomes time-consuming to analyse faults in the protection circuit, locate the fault and the devices etc. Additionally, it poses environmental issues with many utilities having reported catastrophic failure of their CIT containing oil and SF6 as insulating medium [3]. It not only causes unnecessary power outages but also decreases the confidence of the consumers in the utility operator. Some utilities have reported that their CITs had catastrophic failures and the blast knocked off the instrument transformer's head, causing it fall into a public domain and creating a safety and environmental hazard. Advances in digital technology and use of Ethernet and FO wires in the substation technology is a promising new trend in SAS with smarter tools to address issue faced using CITs. NCIT is indeed a good substitute for CIT, but it needs rigorous testing to prove it performance such as bandwidth, ratio errors, frequency response etc. [4].

NCIT leverages on IEC 61850-9-2 communication protocol and connects with smart IEDs, managed switches and MU. NCIT could directly link up with IEDs from the field or link to a MU like the CITs would do, to produce SV in a Process bus environment. In this Process bus environment, the heavy secondary copper cables are replaced by Ethernet and FO wires and achieve better performance [5]. In-depth OPNET modelling and practical experiments have been conducted at Curtin University laboratory to validate the test results of NCIT. Understanding ETE delays and Average delays in propagating SV and GOOSE frames is the key feature of desktop modelling applying OPNET tool.

Some of the main reasons for NCIT being a good substitute over CIT are [6]:

- No iron core present. Hence there was no saturation effect.
- Dielectric losses are higher in HV during extreme climatic condition. NCIT have no such issues of having dielectric losses due to absence of iron core.
- CITs have either gases or mineral insulating oil which is not the case for NCIT. There is no heating of its elements due to absence of iron core.
- Chances of explosion when secondary circuit is open as the core doesn't saturate.
- CITs are bulky and require large footprint while NCIT are 1/3rd the weight of CIT.
- CIT have multiple terminations using copper wires. It has difficulty in fault diagnostics and condition monitoring.
- CITs have mineral insulating oil which could leak.

Fig. 5.1 exhibits the physical dimension of a 11-kV current transformer (CT). In comparison NCIT with a smaller footprint and encapsulating current and voltage transformer is almost 1/3rd the weight of CIT and it is located within the switchboard. This attractive proposition helps operators to consider NCIT over CIT that could accrue savings in the project. A CIT having current transformer at 11-kV is approx. 33 kg as opposed to a similar NCIT being 11 kg. Additionally, in a typical HV switchboard, CT and voltage transformer (VT) are two different equipments in every cubicle. This increases the weight of the switchboard [7].

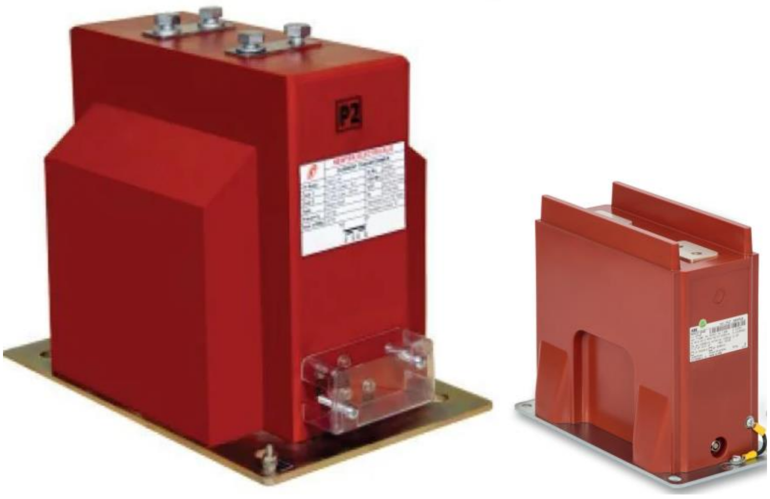


Fig. 5.1. A comparison of CIT vs NCIT equipment.

Other than as stated in previous section, NCIT offers the following product features [8]:

- safety in operation
- better current measurement and frequency response
- environmental friendliness due to non-use of gas or insulating oil
- ease of fault diagnostic
- very low maintenance
- high bandwidth and better frequency response
- ease of adaptability with digital process bus
- low inductance; hence it can respond to fast-changing currents
- high linearity due to lack of iron core even when subjected to large currents
- no effect on NCIT when secondary winding is open.

In Fig. 5.2, the sketch exhibits NCIT connection with the IED and MU via managed switch in a Process bus environment based on IEC 61850-9-2 [9].

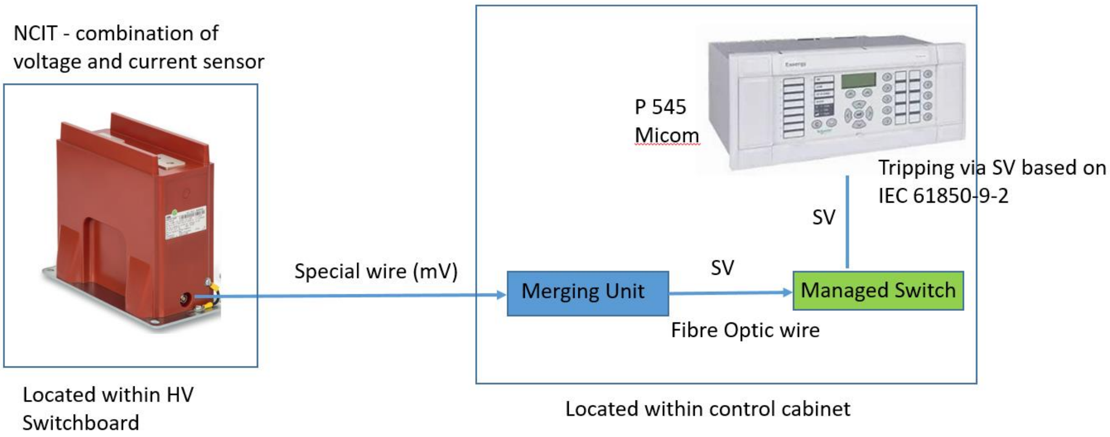

NCIT - combination of voltage and current sensor
Located within HV Switchboard
Special wire (mV)
P 545 Micom
Tripping via SV based on IEC 61850-9-2
SV
SV
Merging Unit
Managed Switch
Fibre Optic wire
Located within control cabinet

Fig. 5.2. NCIT connection in a HV Transmission substation.

In a Process bus topology, all GOOSE and SV messages must follow IEC 61850-5 standard for the SAS to perform [10].

Table 5.1. Message Recovery Time as per IEC 61850-5.

Type of message	Speed of Message	Requirement (in ms)
1	High Speed	<3 to <10
2	Medium Speed	<100
3	Low speed	<500
4	Sample of Raw data	<3 to <10
5	File transfer function	>1000

In today's world most of the utilities have DNP3 as their main protocol but it suffers from few short comings such as poor network security and incompatibility with some of the secondary protection equipment [11]. Moreover, this conventional communication technology slows down further, when used with FO or Ethernet mode, having more secondary cables, and requiring more engineering effort as opposed to a digital protection scheme [12].

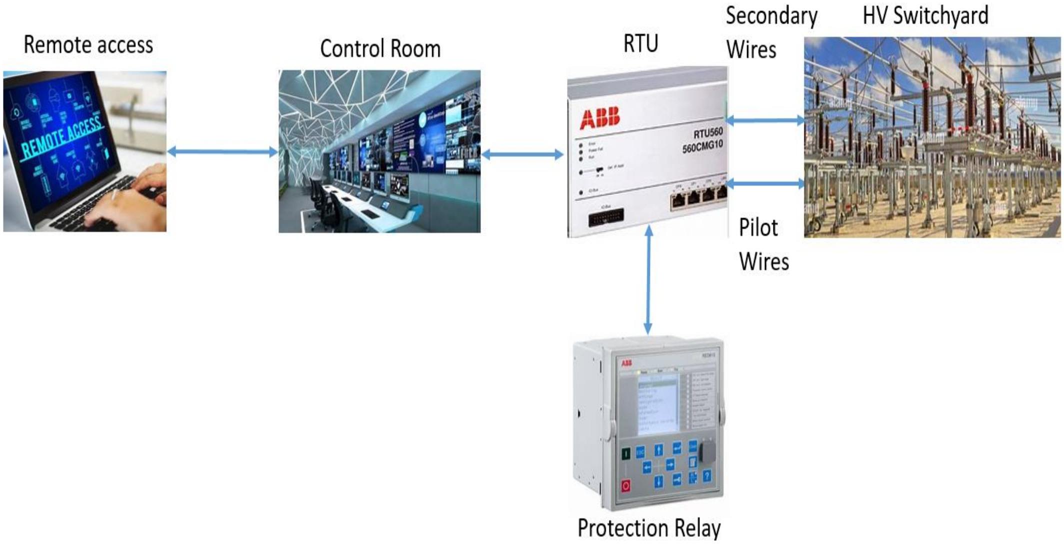


Fig. 5.3. Conventional control room with DNP3 architecture.

To mitigate issues arising with CIT and with availability of optical sensors, the paradigm of SAS has been changing dramatically. NCITs promise to provide dependable protection to primary plant using significantly reduced wires and associated complexity. Application of NCIT is seen as a part of the solution to safety and an innovative solution towards improved fault diagnostics and condition monitoring. It decreases maintenance costs in conventional or Gas Insulated Substation (GIS). With fewer failures, reduced ratio errors, and huge bandwidth, NCITs are expected to be installed in large scale in the next decade but they do have a few challenges related to interoperability and delay in receiving communication packets due to latency [13].

Following IEC 61850-9-2 standard, fault events trigger a trip response in the network IEDs which is similar to an analogue signal to conventional relay [14]. However, many of the CITs are electromechanical type and have been continuing for over two to three decades. With reliability of protection being of main concern these relays could trip spuriously or CITs could blow up. This could not only cause unnecessary disruption in power, but also pose significant serious hazards to members of the public and substation operators. Fig. 5.4 exhibits the linearity of NCIT without saturation effect which is a huge advantage over CIT due to absence of iron core.

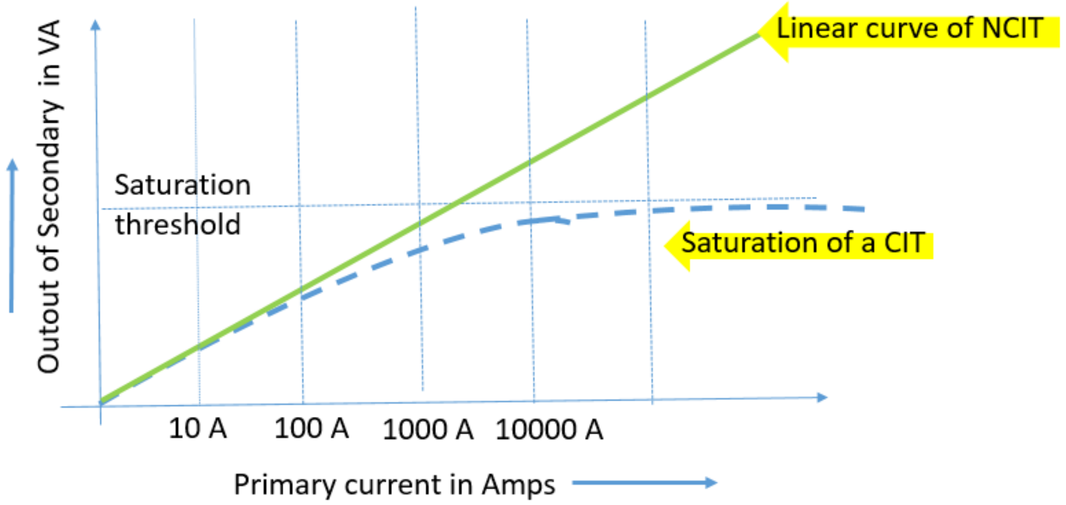


Fig. 5.4. Linearity of NCIT versus saturation of CIT.

The issue encountered due to CIT iron core saturation largely vanishes with the introduction of CIT. The root cause of introduction of errors and inaccuracies CIT is mainly due to ferro-magnetization. As shown in Fig 5.3 with no saturation effect NCIT offers superior bandwidth, high accuracy, immunization against thermal and mechanical stresses, and could operate at different operating temperature [15]. From a safety perspective, the huge advantage that NCIT offer could motivate operators to prevent a blowout even if the secondary circuit remained open unlike CITs which could cause catastrophic failure. Fig. 5.5 exhibits the basic principle of a sensor with magnetic field passing via the primary conductor. The magnetic sensor sends digital signals over the FO wires as GOOSE or SV frames into an IED. In light of its lightweight dimension and superior electrical features NCIT should find more acceptability with the operators [16].

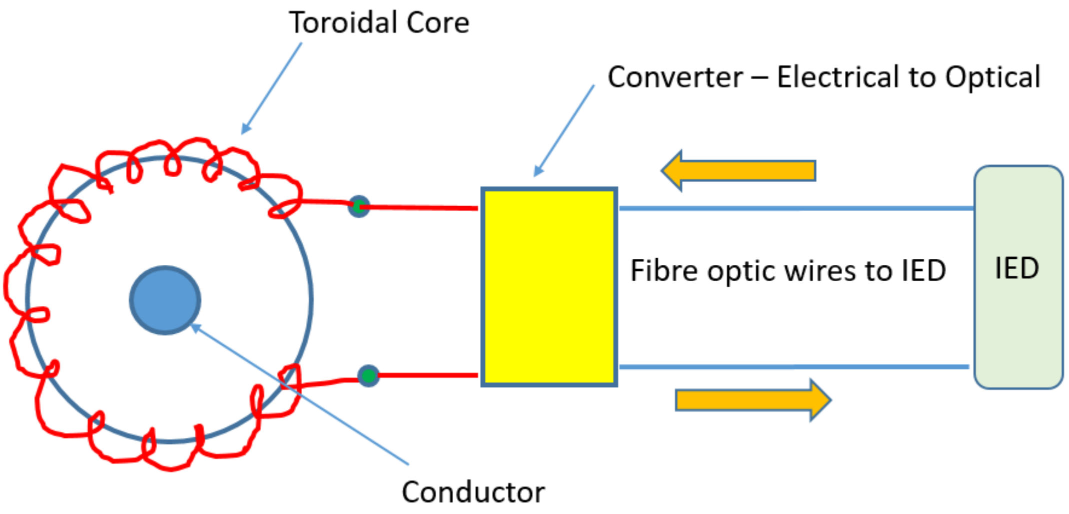


Fig. 5.5. Schematic of the basic principle of NCIT.

A few utilities have been complaining about the hazard these CITs pose due to catastrophic failure operating on oil and SF6 insulating media. Advancement in digital technology and use of FO wire indicates that the operators will apply NCIT more in substation circuits as a substitute for CIT [17]. However, validating the NCIT by testing it in a laboratory environment will provide more acceptability by utilities in a dynamic environment by addressing issues related to safety, environmental stability, and ease of engineering operation. This has motivated researchers to work on sensors and NCITs that could offer significant reduction in cabling and wiring in the panels. Fig. 5. 6 exhibits the huge difference in wiring between CIT and NCIT in a substation environment. Switchboards fitted with NCITs sends the signals in mili Volts to IEDs which convert the analogue signals to SV frames and transmits them over a SAS network. GOOSE frames have been used to trip the circuit breakers in a Station bus topology. SV and GOOSE frames move with a particular speed in the network as per IEC 61850-5 standard [18]. However, these bytes sizes change during a fault scenario. These abnormal byte sizes send a trip command to the circuit breaker with an encrypted data which is difficult to hack in a cybersecurity scenario [19]. These encrypted data packets are broadcast to various subscribing IEDs at a specific frequency. The values of sample per period (SPP) have been outlined in IEC 61850-9-2-LE guideline at 1/50/80 which when converted reads 250 µs. The SV packets usually circulate within the LAN or WAN [20].

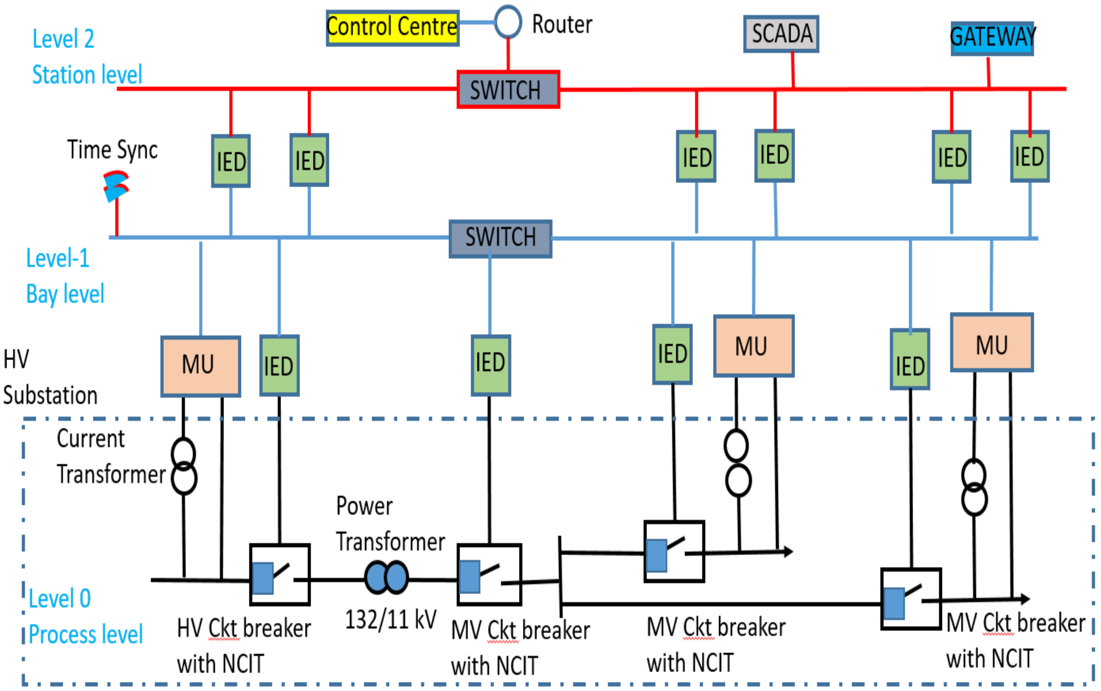
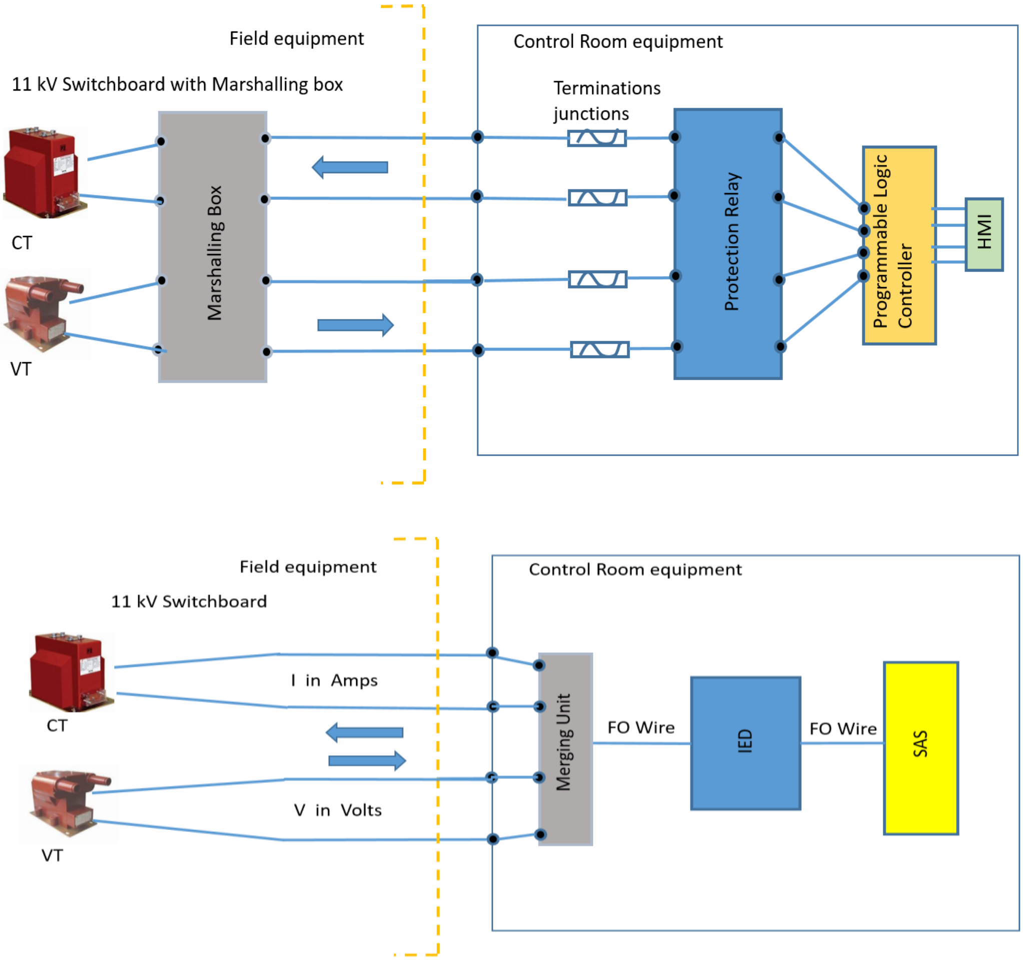


Fig. 5.6. NCIT and MU in Process and Station bus topology [21].

Fig. 5.7 (a) exhibits CIT wirings routed to relay terminals at 1A and 110V in switchyard trenches, which is complex and messy. With a number of terminations involved at various nodes, the fault diagnosis to trace the exact fault location is very difficult. On the other hand, Fig. 5.7 (b) shows the advantages of having NCITs wherein engineering, and project challenges could be addressed better whereas in most instances CIT could send analogue value to field MU which in turn can send SV to IED in the control room [22]. However, any new technology doesn't gain acceptance unless supported by test results and this chapter focuses on providing some test results.

A major utility operator in New South Wales, Australia has garnered substantial savings by implementing process bus topology in its entirety [23]. The project at Avon, NSW, Australia, demonstrated substantial savings in real estate, cable trenches, switchboard dimension etc. With zero maintenance cost and non-involvement of oil or SF6 gas, there is a merit in using NCIT over CIT [24].



Figs. 5.7. (a) CIT wiring from field to the control room, and (b) NCIT wiring from field to control room.

Fig. 5.8 represents a typical SAS in a HV substation equipped with HV apparatus. This is labelled as 1. These field equipment's communicate with analogue signals via MU to digital devices in process, designated function label 2. Broadcasting and subscribing of frames are deemed as function label 3 while events such as fault, CB status, CB availability and controls are deemed as function 4 which could simultaneously be viewed from a remote-controlled room which is designated as function label 5. This could control CB open and close, Isolator open and close control being at function label 5 [25].

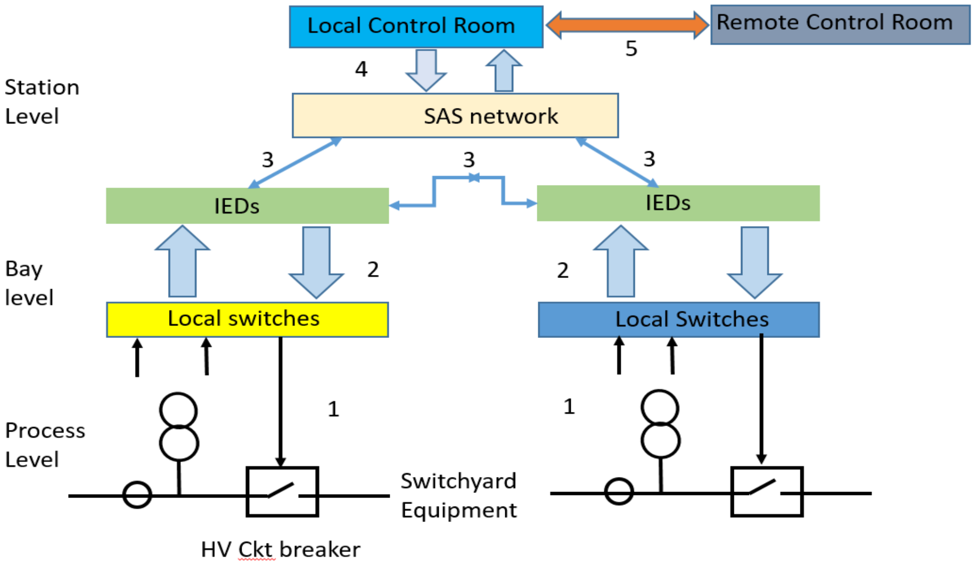


Fig. 5.8. Commands at various functional level in a SAS architecture [25].

Table 5.2 is summary of various functional labels identified in Fig. 5.7 which originated from field devices to control room [25].

Table 5.2. SAS Network from Field to Control Room.

Function label	Name of the function
1	Field equipment such as HV CB, Power Transformers, CT, VT
2	Communication at the bay level with field equipment
3	Communication between bay and station level
4	Communication and data exchange between station level and Local control room
5	Communication between remote control room field equipment such as breaker availability and CB interlock

Speed, size and particular events govern the type of messages circulating in the system and are categorised from Type 1 to Type 6; these have been narrated in a previous chapter. Usually, three types of communication exchange that takes place in a Process bus architecture i.e., periodic, random, and burst data.

Periodic data provides information regarding switch status and the actual value of analogue input in a process bus topology. Usually monitoring devices and data transmission depends upon the topology, traffic queue, interoperability of multi-vendor equipment within the SAS network. On the other hand, for a random data stream time stamping is of critical importance and it is based on time synchronisation with IRIG-B or PTP signal. The time stamping allows the operator to understand the time and duration of the fault on IED or closing a HV CB in two geographical isolated substations at the same time based on WAN. Time synchronization allows exact tripping of IEDs (i.e., upstream incomer and downstream feeder) and its on-effect interlocks with other IEDs. The requirement of frames to reach the destination at a particular speed is given as per Table 5.3 [26].

Table 5.3. Frame Speed to Arrive at Subscribing IED.

Type of messages	Guideline as per IEC 61850-9-2 (ms)
Type 1 fast messages	<10
Type 2 medium speed messages	<100
Type 3 low speed messages	<500
Type 4 Raw data	<700
Type 5 file transfer	>1000
Time synch messages	<50

5.3 TIME SYNCHRONISATION

Time synchronisation in a substation is an important event as IED precisely compute the inception and duration of the fault. Inaccuracy in different IEDs related to time synchronisation could malfunction interlocks or tripping of incomers or feeders leading to catastrophic failure of the electrical primary plant asset. Some of the commonly used time synchronisation protocols in digital circuits are Network Time Protocol (NTP), Inter Range Integrated Group

(IRIG) and Precision Time Protocol (PTP). All these three protocols on time synchronisation have been elaborated in the following subsections.

5.3.1 Network Time Protocol

Network peripherals and computers in the LAN usually suffer from jitters and latencies due to congestion, malformation or burst of frames. This results to slow down flow of frames from 1 to 2 ms and necessitates the use of additional cables and clocks. It relies on radio or atomic clock for time attached to the main server which distributes time over the LAN. The complexity of the network cabling and addition of peripherals to get the LAN up to fast synchronization makes less popular and outdated. This protocol is synchronized with the main devices that is not synchronized by itself. This protocol has older devices supporting it which may not be possible in modern day context [27].

5.3.2 IRIG-B Protocol

This protocol relies on coaxial cable for transporting timing signals and follows IRIG guidelines developed by Rockwell Automation at 100 pulse per seconds and it is a point-to-point connection. It provides time synchronization with the device with 1 microsecond accuracy. This protocol carries information on date in yy-mm-dd in binary code format. To run this protocol, it needs adaptability to accept coaxial cables to connect with IEDs or managed switches which needs a number of additional adapters for hardware changes. This protocol has found some acceptance in mining and communication infrastructure but seems outdated in today's scenario and not many manufacturers provide channels for coaxial cables in their devices [28].

5.3.3 PTP Protocol

Most of the utilities prefer time synchronisation in digital SAS and usually there is provision to accept cluck pulses in switches and IEDs in many multi-vendor equipment. It follows IEEE 1588-2008. It works over Ethernet and FO cables and synchronises devices to a very high degree of accuracy. IEEE 1588 guideline lays down the foundation of synchronisation with different devices operating on different nodes with its clock in a master-slave communication mode with the grandmaster device controlling and monitoring all clocks across the nodes. With suitable adapters and tools, old digital devices without PTP still could communicate with PTP enabled devices for synchronisation for accuracy and precision. However, a hybrid mode of NTP or IRIG with PTP should be used for smaller LANs and this needs rigorous testing as NTP and IRIG are slow compared to PTP in terms of time synchronisation which is in microseconds [29].

Table 5.4. Summarising the Different Time Synchronisation Protocols.

	NTP	IRIG-B	PTP
Cabling	Ethernet	Dedicated Coaxial cables required	Ethernet or FO
Accuracy	80-100 mili seconds	1-10 microseconds	50-100 nano second
Infrastructure	Slow to synchronization and could give errors if used in conjunction with PTP devices in hybrid mode	Not all devices are manufactured with coaxial adapters. Need dedicated circuit.	Works better when all devices are PTP
Mode of communication	Master-slave	Client-server	Master-slave
Latency	Yes, and depends upon the frames size and traffic queue	No latencies due to signal transmission over coaxial cables	Yes, and depends upon the frames size and traffic queue
Scan of the network	Every minute and process bus traffic remains affected	Every second and process bus traffic remains unaffected	Every 10-1 milisecond with process bus traffic affected

The highlight of this chapter has been to carry out a desktop study related to ETE and Average delays using NCIT. Further, analysis of practical tests on HV NCIT has been carried out in a SAS network to understand its performance and highlight its advantage over CIT.

5.4 Experimental Research on NCIT in a Process Bus Environment in a Laboratory Set-up

Prior to retro-fitment of NCIT in a HV switchgear, a laboratory experiment was undertaken in line with IEC 61850-5 guideline, with SV frames reaching its destination within 2 µs, thus laying a foundation for high accuracy and data acquisition. However, digital frames have issues with clogging, traffic jam, queuing, ETE delay etc. due to frame passage via various nodes.

Additionally, there are issue with interoperability with multivendor equipment having proprietary features although individually this equipment obtains the necessary IEC 61850 compliant certificates. This could dampen the confidence of the end-user and prohibit digital substation from gaining ground [30].

Table 5.5 provides name plate rating of the NCITs under test at Curtin University laboratory. These combi-sensors are the combinations of Voltage and Current transformer encapsulated in one hermetically sealed module. These combi-sensors are 1/3rd the weight of normal CITs installed in a 11-kV switchboard.

Table 5.4 shows the 3 x ABB Make 11-kV KEVCD model Combi-sensors NCIT having the following data.

Table 5.5. Name Plate Rating of Donated NCIT by ABB

Sr. No. 1VLT5421006867	Sr. No. 1VLT54210068679	Sr. No. 1VLT5421006871
Order 1000060685	Order 1000060685	Order 1000060685
Upn : 11/ √3-kV	Upn : 11/ √3-kV	Upn : 11/ √3-kV
Ipr : 80A	Ipr : 80A	Ipr : 80A
Class 0.5/2P	Class 0.5/2P	Class 0.5/2P
50Hz	50Hz	50Hz
11 kG	11kG	11 kG
Isht ckt : 125kA	Isht ckt : 125kA	Isht ckt : 125kA

Fig. 5.9 exhibits the wiring of these combi-sensors which have been connected to an ABB make substation merging unit (SMU) which operates on the principle of Rogowiski coil with an inbuilt toroid without ferromagnetic material. The output of this KEVCD combi-sensor is a secondary voltage from a KEVCD equipment of 3 mV which is fed to SMU, and it replicates the primary voltage signal that could be the output of a CIT.

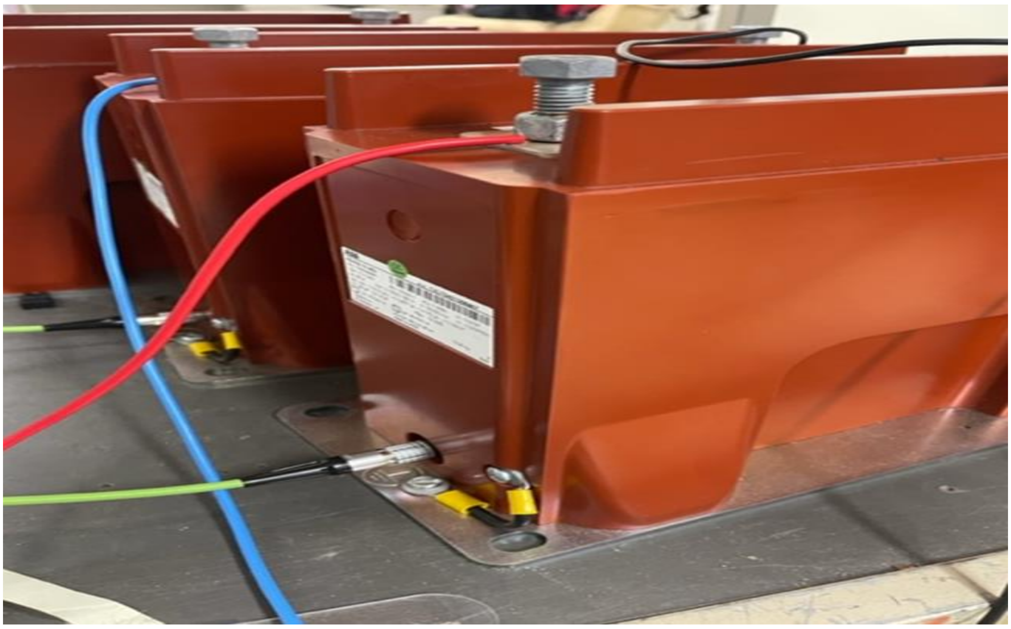


Fig. 5.9. NCIT – ABB make KEVCD combi-sensor.

Fig. 5.10 exhibits a SLD of an incomer and feeder protection using NCITs and 2 x ABB IEDs. A fault in the feeder NCIT creates spike in current which is sensed by the SMV 615 and the SV off-trips the ABB RET 615 which is much faster than conventional IED based on IEC 61850-9-2-LE guidelines, with accurate time synchronisation derived from PTP clock. It was observed that all equipment in the Process bus network accurately performed protection, control, and measurement functions with minimal hardwire terminations.

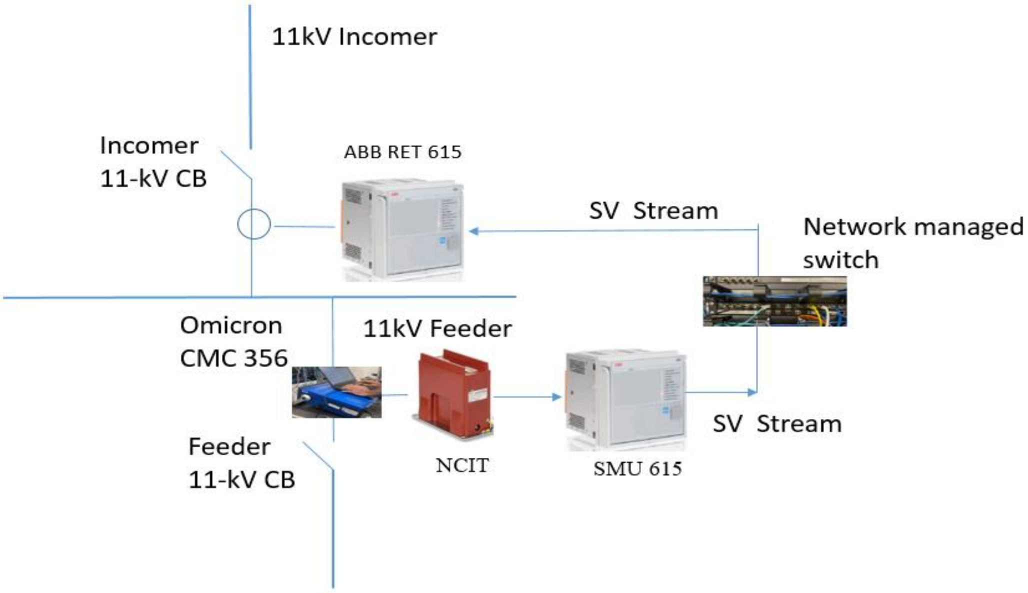


Fig. 5.10. SLD of a Feeder NCIT – SMU615 publishing SV frames to incomer protection IED.

The overall set-up in Fig. 5.11 using a Ruggedcom switch RSG 2488 with SMU 615 and a SEL 2407 clock is located at the Curtin University laboratory. Secondary injection is carried out via Omicron CMC 356 for 15A and the output results in a trip of the RET 615 based on IEC 61850-9-2. The combi-sensor used in the practical set up is a highly accurate voltage divider whose output is in mili Volts (mV). Fig. 5.10 shows the connection of laboratory equipment with a Ruggedcom RSG 2488 managed switch with a clock device i.e., SEL2407 from time synchronisation of a Process bus point of view. This equipment set-up shows the interoperability tests where output of the NCITs has been connected to Ruggedcom and SEL equipment besides ABB make SMU615.

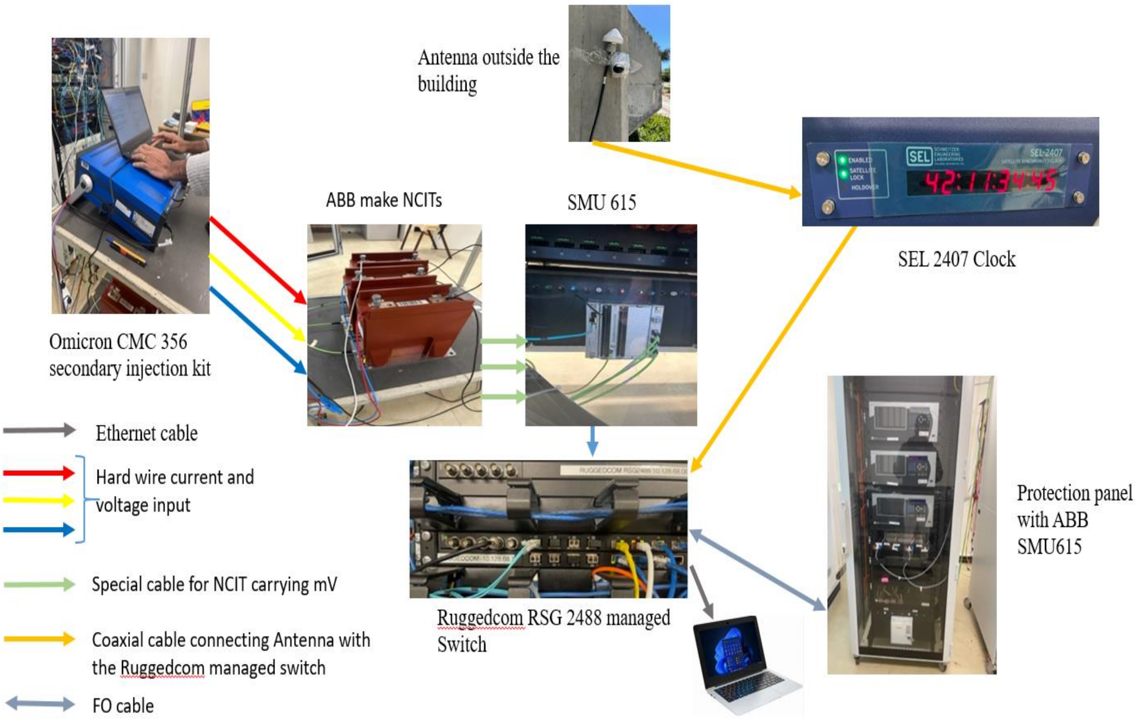
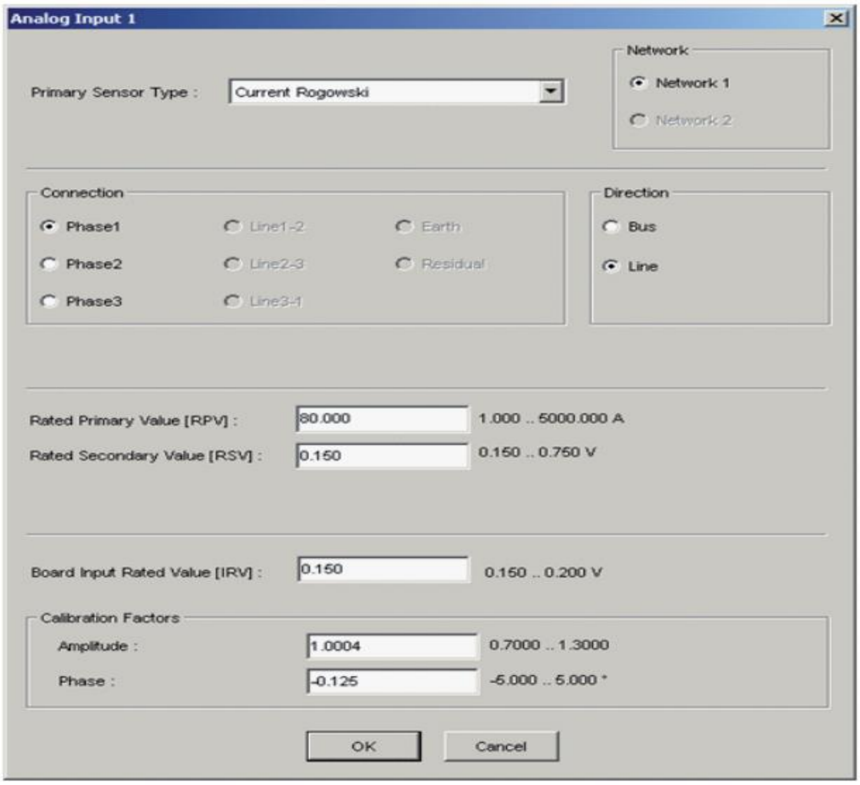

Antenna outside the building
SEL 2407 Clock
ABB make NCITs
SMU 615
Omicron CMC 356 secondary injection kit
Ethernet cable
Hard wire current and voltage input
Special cable for NCIT carrying mV
Coaxial cable connecting Antenna with the Ruggedcom managed switch
FO cable
Ruggedcom RSG 2488 managed Switch
Protection panel with ABB SMU615

Fig. 5.11. Connection diagram at SV flow in a Process bus environment.

The amplitude and phase error of this combi-sensor is independent of primary current, and this is achieved by suitably setting up the SMU Logic as shown in Fig. 5.12.



Analog Input 1

Primary Sensor Type : Current Rogowski

Network
● Network 1
○ Network 2

Connection
● Phase1 ○ Line1-2 ○ Earth
○ Phase2 ○ Line2-3 ○ Residual
○ Phase3 ○ Line3-1

Direction
○ Bus
● Line

Rated Primary Value [RPV] : 80.000 1.000 .. 5000.000 A
Rated Secondary Value [RSV] : 0.150 0.150 .. 0.750 V

Board Input Rated Value [IRV] : 0.150 0.150 .. 0.200 V

Calibration Factors
Amplitude : 1.0004 0.7000 .. 1.3000
Phase : -0.125 -5.000 .. 5.000 °

Fig. 5.12. Setting up of SAMU 615.

The setting of ABB makes SMU615 having VLAN and ID is shown in Fig. 5.13 (a) which is carried out using a PM600 software tool. The NCIT available at the Curtin University laboratory have a rated primary current 80A which is scaled to 150 mV, having maximum linearity limit of 4000 A. The correction factor used is about 15 times higher than the conventional ones. PCM600 tool indicates that SAMU600 is online by virtue of the green tick. Other parameter settings such as IP name, VLAN setting, technical key is shown in Fig. 5.13 (b). The calculation and setting up the correction factor scale is an important task prior to testing.

The equation of correction factor is given by

$$RSV = (I_n \text{ x } I_{pr}) * K_f / f_n \qquad (1)$$

Where, RSV = Rated Secondary Value in mV/ Hz

I_n = Rated nominal current

I_{pr} = Rated primary current

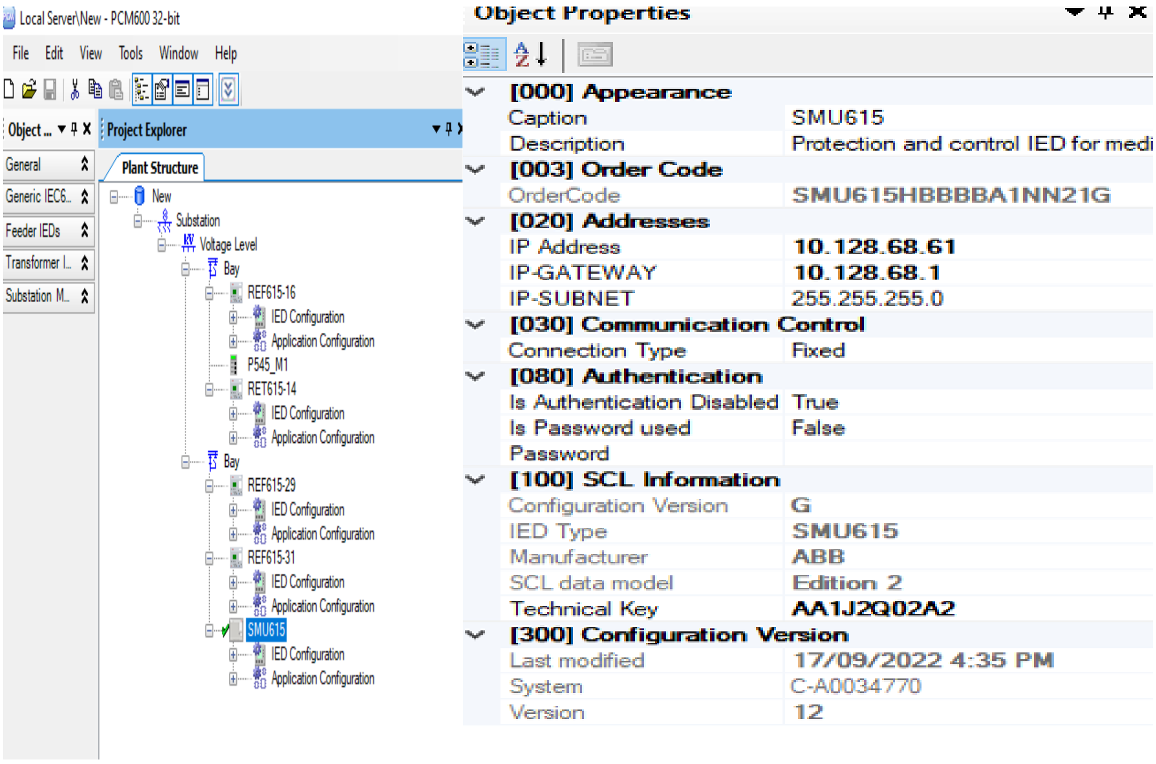
K_f = Correction factor in kV

f_n = Nominal Frequency in Hz

RSV = [(150/80) * 150mV]/50 Hz

= 5.62 mV/Hz

The output of the NCITs i.e. 5.52 mV/Hz were fed into the SMU615 which produced SV routed via Ruggedcom managed switch. Fig. 5.12 exhibits SMU615 detection by ABB tool PCM600 online and its technical key AA1J2Q02A2 and IP address 10.128.68.61 as seen in the network.

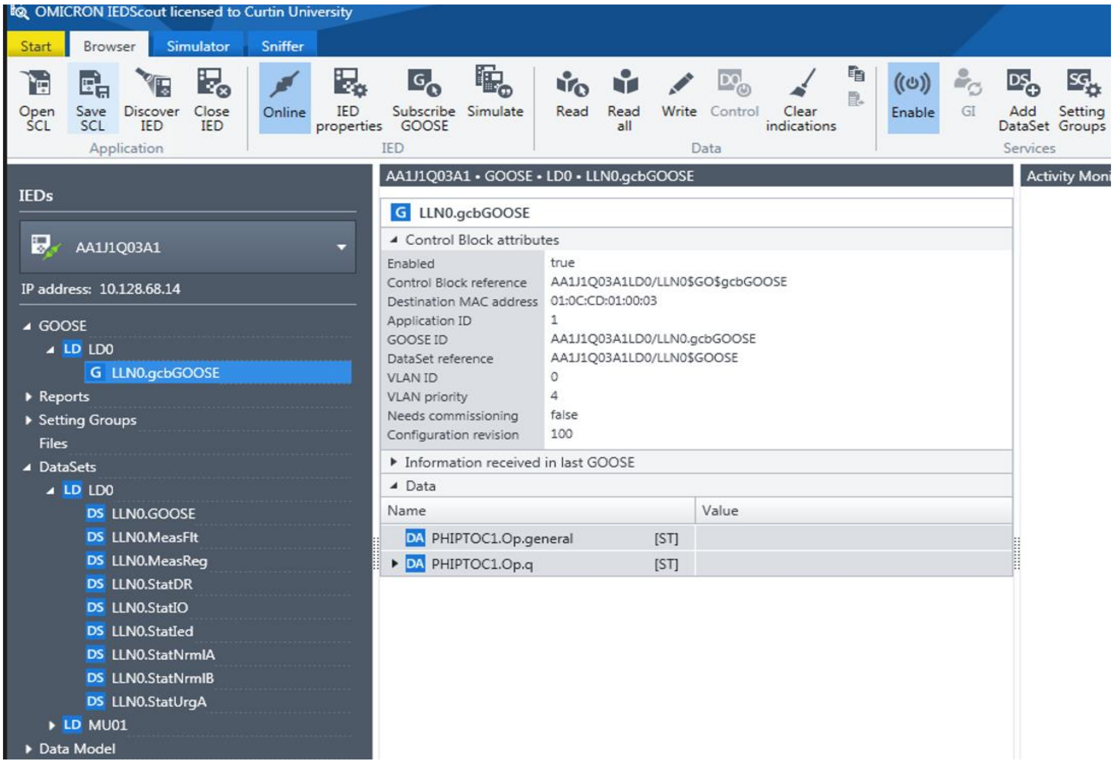


Object Properties

[000] Appearance	
Caption	SMU615
Description	Protection and control IED for medi
[003] Order Code	
OrderCode	SMU615HBBBBA1NN21G
[020] Addresses	
IP Address	10.128.68.61
IP-GATEWAY	10.128.68.1
IP-SUBNET	255.255.255.0
[030] Communication Control	
Connection Type	Fixed
[080] Authentication	
Is Authentication Disabled	True
Is Password used	False
Password	
[100] SCL Information	
Configuration Version	G
IED Type	SMU615
Manufacturer	ABB
SCL data model	Edition 2
Technical Key	AA1J2Q02A2
[300] Configuration Version	
Last modified	17/09/2022 4:35 PM
System	C-A0034770
Version	12

Fig. 5.13. Visibility of SMU 615 online in PCM600 tool with parameter setting.

Fig. 5.14 exhibits the discovery of ABB make RET 615 IED which verifies its online status in the network using Omicron tool IED Scout. All parameters previously including the technical keys have been exhibited in this screenshot.



IP address: 10.128.68.14

AA1J1Q03A1 • GOOSE • LD0 • LLN0.gcbGOOSE

G LLN0.gcbGOOSE

Control Block attributes

Enabled	true
Control Block reference	AA1J1Q03A1LD0/LLN0$GO$gcbGOOSE
Destination MAC address	01:0C:CD:01:00:03
Application ID	1
GOOSE ID	AA1J1Q03A1LD0/LLN0.gcbGOOSE
DataSet reference	AA1J1Q03A1LD0/LLN0$GOOSE
VLAN ID	0
VLAN priority	4
Needs commissioning	false
Configuration revision	100

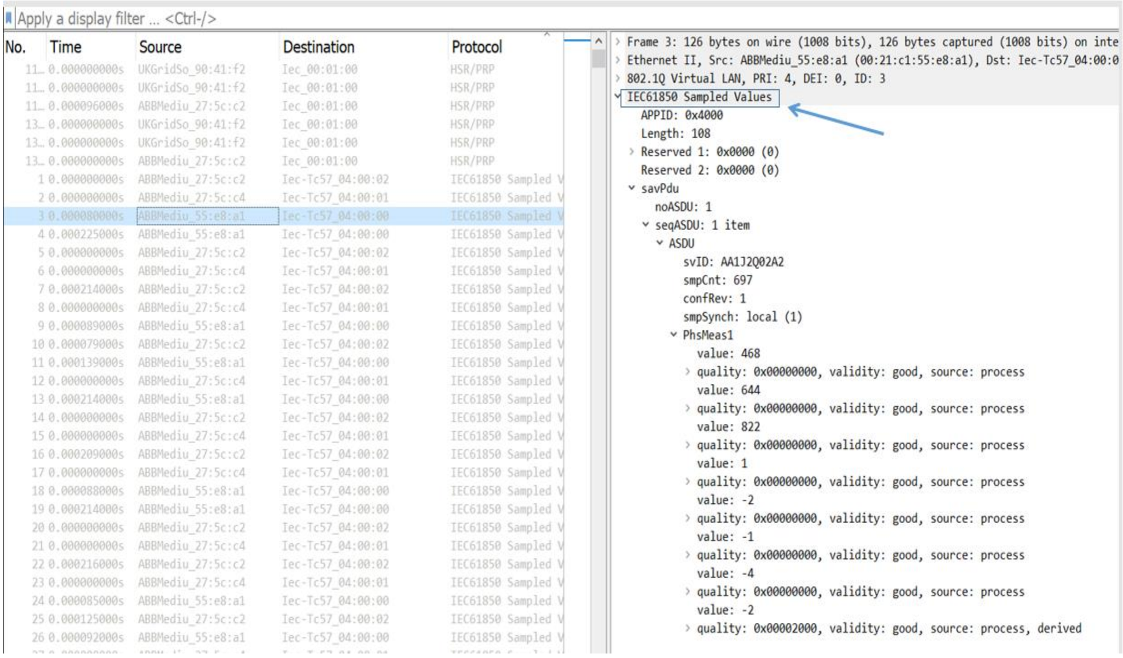
Information received in last GOOSE

Data

Name		Value
DA PHIPTOC1.Op.general	[ST]	
DA PHIPTOC1.Op.q	[ST]	

Fig. 5.14. IED Scout screen shot of discovery of RET615.

Fig. 5.15 exhibits a screen shot of the Wireshark tool of SMU 615 that captures the flow of SV to Ruggedcom MU. The flow of SV stream is better understood observing overall connection diagram in Fig. 5.10.

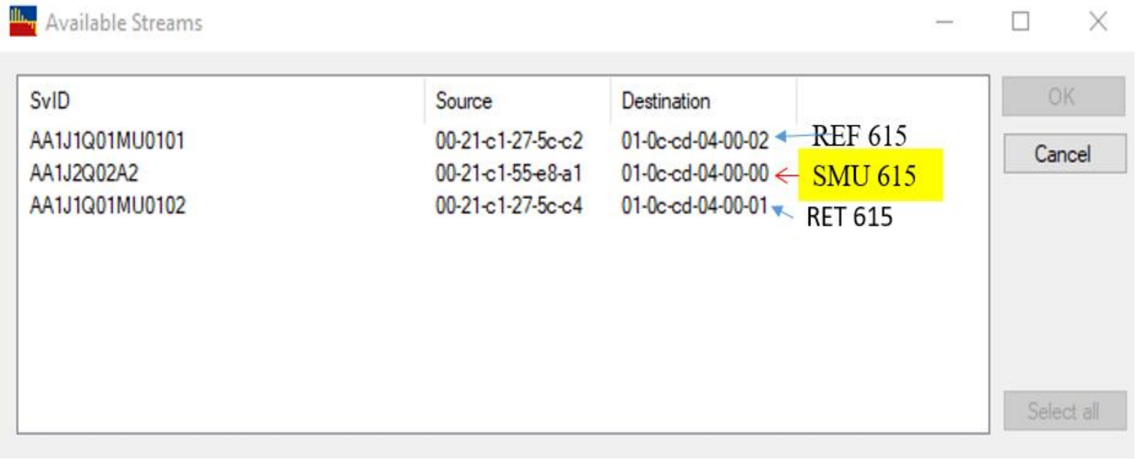

Apply a display filter ... <Ctrl-/>

```
No.   Time          Source               Destination          Protocol
11… 0.000000000s  UKGridSo_90:41:f2    Iec_00:01:00         HSR/PRP
11… 0.000000000s  UKGridSo_90:41:f2    Iec_00:01:00         HSR/PRP
11… 0.000096000s  ABBMediu_27:5c:c2    Iec_00:01:00         HSR/PRP
13… 0.000000000s  UKGridSo_90:41:f2    Iec_00:01:00         HSR/PRP
13… 0.000000000s  UKGridSo_90:41:f2    Iec_00:01:00         HSR/PRP
13… 0.000000000s  ABBMediu_27:5c:c2    Iec_00:01:00         HSR/PRP
  1 0.000000000s  ABBMediu_27:5c:c2    Iec-Tc57_04:00:02    IEC61850 Sampled V
  2 0.000000000s  ABBMediu_27:5c:c4    Iec-Tc57_04:00:01    IEC61850 Sampled V
  3 0.000080000s  ABBMediu_55:e8:a1    Iec-Tc57_04:00:00    IEC61850 Sampled V
  4 0.000225000s  ABBMediu_55:e8:a1    Iec-Tc57_04:00:00    IEC61850 Sampled V
  5 0.000000000s  ABBMediu_27:5c:c2    Iec-Tc57_04:00:02    IEC61850 Sampled V
  6 0.000000000s  ABBMediu_27:5c:c4    Iec-Tc57_04:00:01    IEC61850 Sampled V
  7 0.000214000s  ABBMediu_27:5c:c2    Iec-Tc57_04:00:02    IEC61850 Sampled V
  8 0.000000000s  ABBMediu_27:5c:c4    Iec-Tc57_04:00:01    IEC61850 Sampled V
  9 0.000089000s  ABBMediu_55:e8:a1    Iec-Tc57_04:00:00    IEC61850 Sampled V
 10 0.000079000s  ABBMediu_27:5c:c2    Iec-Tc57_04:00:02    IEC61850 Sampled V
 11 0.000139000s  ABBMediu_55:e8:a1    Iec-Tc57_04:00:00    IEC61850 Sampled V
 12 0.000000000s  ABBMediu_27:5c:c4    Iec-Tc57_04:00:01    IEC61850 Sampled V
 13 0.000214000s  ABBMediu_55:e8:a1    Iec-Tc57_04:00:00    IEC61850 Sampled V
 14 0.000000000s  ABBMediu_27:5c:c2    Iec-Tc57_04:00:02    IEC61850 Sampled V
 15 0.000000000s  ABBMediu_27:5c:c4    Iec-Tc57_04:00:01    IEC61850 Sampled V
 16 0.000209000s  ABBMediu_27:5c:c2    Iec-Tc57_04:00:02    IEC61850 Sampled V
 17 0.000000000s  ABBMediu_27:5c:c4    Iec-Tc57_04:00:01    IEC61850 Sampled V
 18 0.000088000s  ABBMediu_55:e8:a1    Iec-Tc57_04:00:00    IEC61850 Sampled V
 19 0.000214000s  ABBMediu_55:e8:a1    Iec-Tc57_04:00:00    IEC61850 Sampled V
 20 0.000000000s  ABBMediu_27:5c:c2    Iec-Tc57_04:00:02    IEC61850 Sampled V
 21 0.000000000s  ABBMediu_27:5c:c4    Iec-Tc57_04:00:01    IEC61850 Sampled V
 22 0.000216000s  ABBMediu_27:5c:c2    Iec-Tc57_04:00:02    IEC61850 Sampled V
 23 0.000000000s  ABBMediu_27:5c:c4    Iec-Tc57_04:00:01    IEC61850 Sampled V
 24 0.000085000s  ABBMediu_55:e8:a1    Iec-Tc57_04:00:00    IEC61850 Sampled V
 25 0.000125000s  ABBMediu_27:5c:c2    Iec-Tc57_04:00:02    IEC61850 Sampled V
 26 0.000092000s  ABBMediu_55:e8:a1    Iec-Tc57_04:00:00    IEC61850 Sampled V
```

```
> Frame 3: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits) on inte
> Ethernet II, Src: ABBMediu_55:e8:a1 (00:21:c1:55:e8:a1), Dst: Iec-Tc57_04:00:0
> 802.1Q Virtual LAN, PRI: 4, DEI: 0, ID: 3
v IEC61850 Sampled Values
    APPID: 0x4000
    Length: 108
  > Reserved 1: 0x0000 (0)
    Reserved 2: 0x0000 (0)
  v savPdu
      noASDU: 1
    v seqASDU: 1 item
      v ASDU
          svID: AA1J2Q02A2
          smpCnt: 697
          confRev: 1
          smpSynch: local (1)
        v PhsMeas1
            value: 468
          > quality: 0x00000000, validity: good, source: process
            value: 644
          > quality: 0x00000000, validity: good, source: process
            value: 822
          > quality: 0x00000000, validity: good, source: process
            value: 1
          > quality: 0x00000000, validity: good, source: process
            value: -2
          > quality: 0x00000000, validity: good, source: process
            value: -1
          > quality: 0x00000000, validity: good, source: process
            value: -4
          > quality: 0x00000000, validity: good, source: process
            value: -2
          > quality: 0x00002000, validity: good, source: process, derived
```

Fig. 5.15. Wireshark capture of SV burst out of SMV 615 in the network.

Fig. 5.16 is a screenshot of an Omicron tool SV Scout which exhibits the three IEDs and its technical key names, source, and Media Access Control (MAC) tags. This is an important set-up of parameters pointing to identify the source. “Technical key” helps the user to allow flow of SV to its destination and subscribing IEDs in a SAS network. Without the technical key the SV wouldn’t reach its destination. In this screenshot SV key ID AA1J2Q02A2 is reaching SMU615 as highlighted.



SvID	Source	Destination
AA1J1Q01MU0101	00-21-c1-27-5c-c2	01-0c-cd-04-00-02
AA1J2Q02A2	00-21-c1-55-e8-a1	01-0c-cd-04-00-00
AA1J1Q01MU0102	00-21-c1-27-5c-c4	01-0c-cd-04-00-01

Fig. 5.16. Identification of technical key and its flow in a SAS network.

Fig. 5.17 and Fig. 5.18 exhibit the setup of a 132-kV NCIT in the laboratory. Secondary injection was carried with reduced current from a safety perspective and the output was scaled up for analysis with CIT. Faults were simulated with the Omicron secondary injection kit in the circuit. The maximum short circuit withstand capability of this class 5P HV NCIT was 63-kA for 1 sec. and DC offsets were recorded for comparison with CIT.

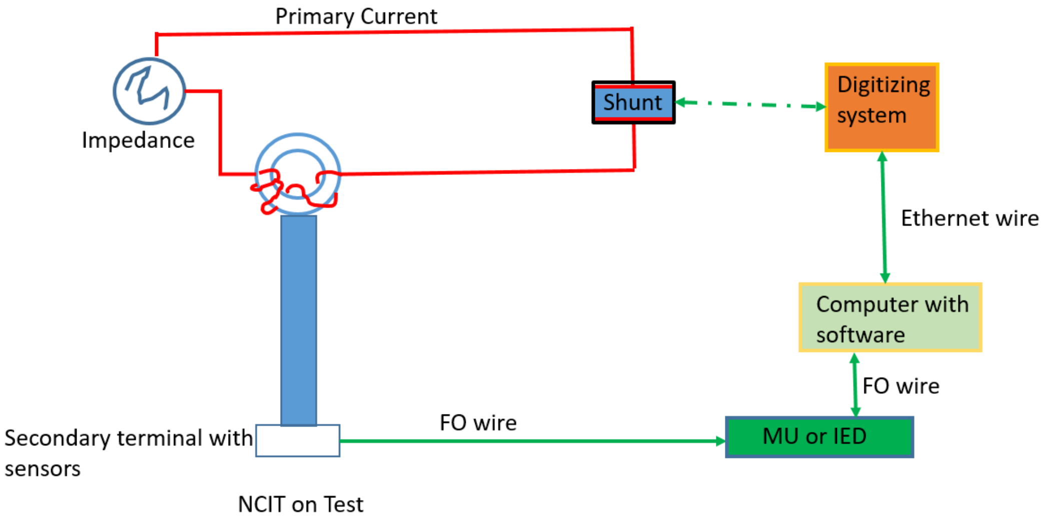


Fig. 5.17. Equipment set-up.

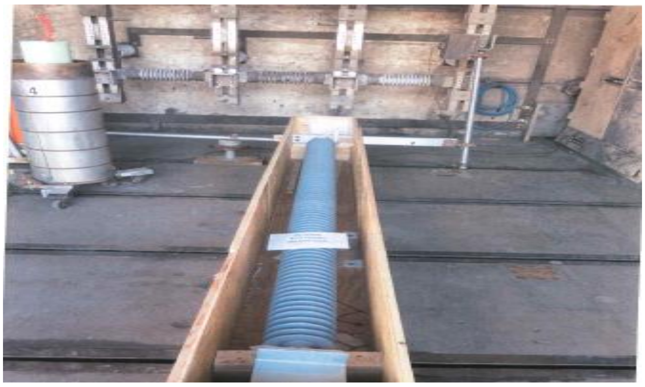


Fig. 5.18. 132-kV NCIT set up for experiment.

The HV Rogoswiki sensor wound over the primary bar is shown in Fig. 5.18 ready for test at the laboratory in a safe area.

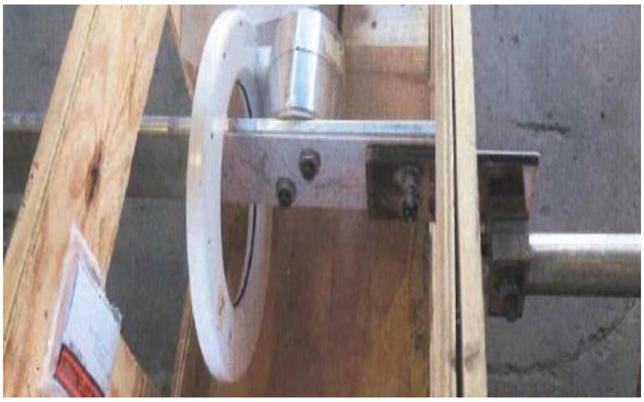


Fig. 5.19. Primary bar of a 132-kV NCIT head.

Fig. 5.20 exhibits a schematic diagram of the test set-up involving HV NCIT shown in Fig. 5.17. Between the source generator and the optical current transducer is positioned a source impedance named X_S. The test involved short time and peak withstand current test and, observing the result, the composite errors were found to be 1.39% while peak error was determined to 1.79%. The tests were carried out with HV NCIT in horizontal position.

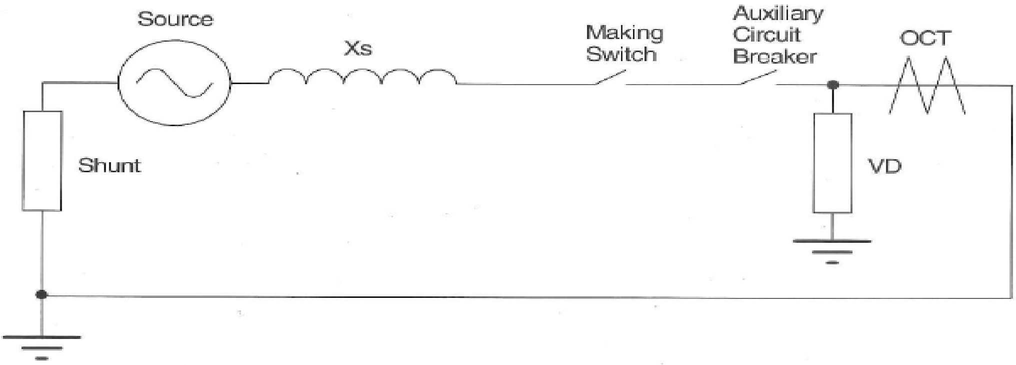


Fig. 5.20. NCIT test illustration with an equivalent diagram.

The single-phase fault condition and DC offset of the NCIT on test were plotted as shown in Fig. 5.21 and Fig. 5.22 respectively. Comparative study of fault response and DC offset favour its future application of HV NCIT in HV substation switchyard as its parameters are well within the tolerance limit as stipulated in IEC 60044-8 [31].

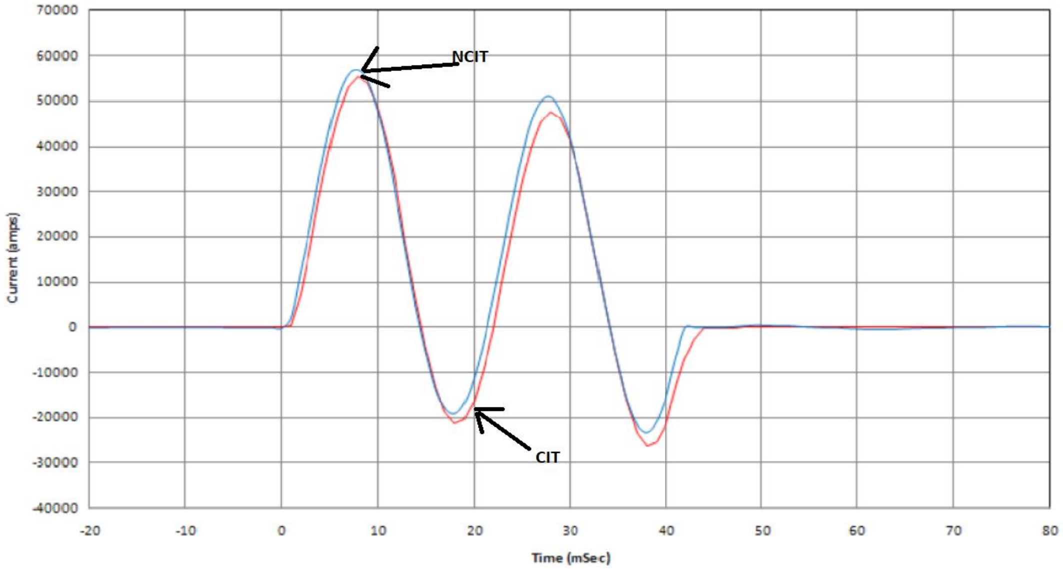


Fig. 5.21. Comparison of Single-Phase Fault Condition.

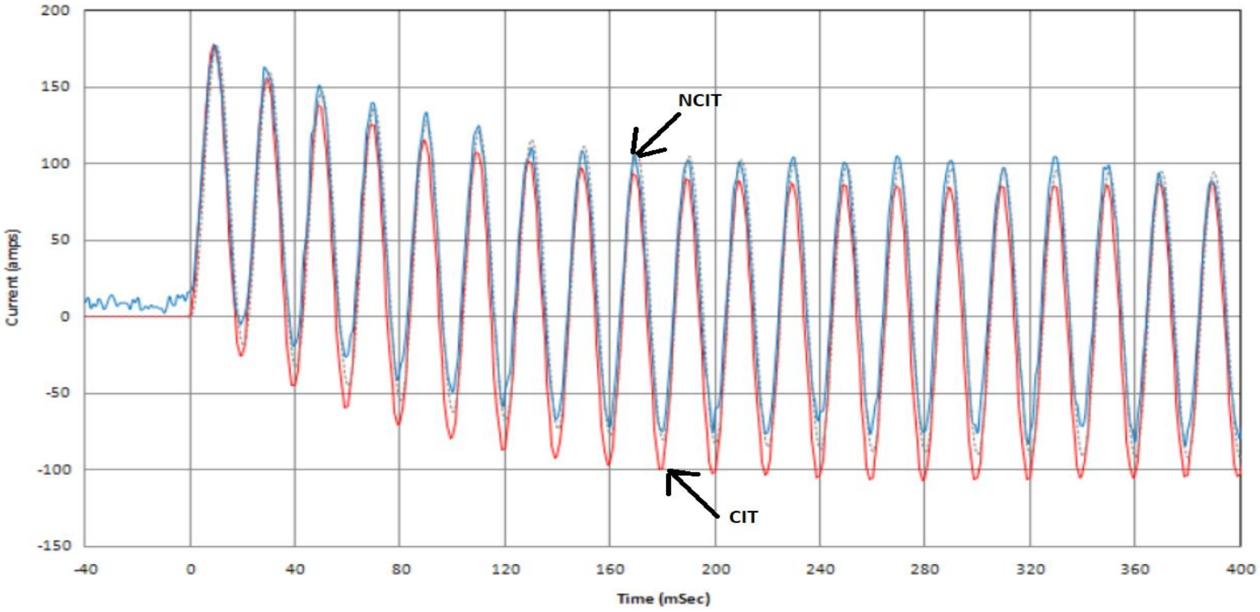


Fig. 5.22. Comparison of DC offset.

In the final test on frequency response of this HV NCIT it was observed that the delay time of SV streams was streaming at100-μs which is well within the stipulated Utility Communication Architecture (UCA) guideline as shown in Fig. 5.23. The experiment was carried out with frequencies from 48 hz to 51 Hz and 57 hz to 61 hz.

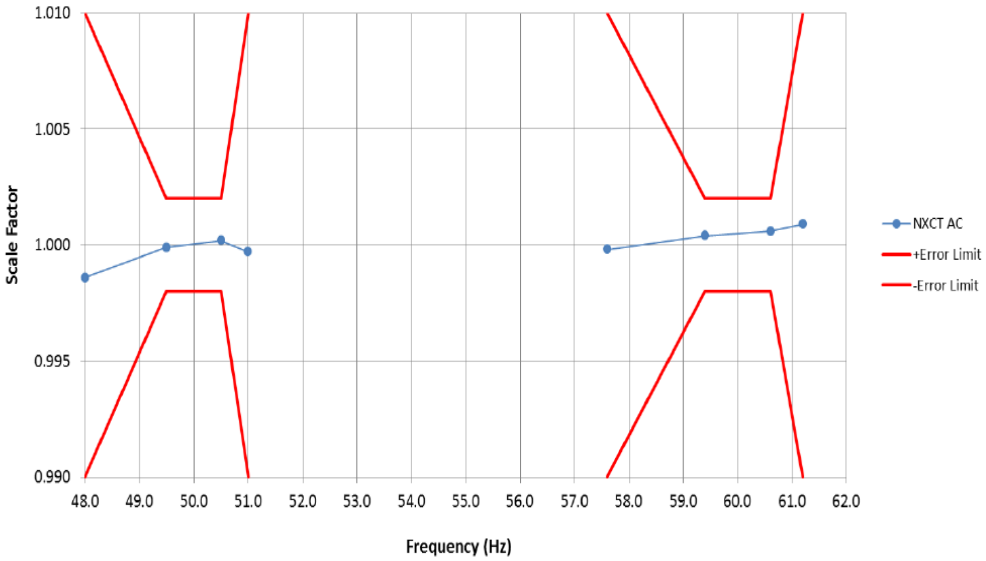


Fig. 5.23. Frequency response of a 132-kV NCIT.

5.4 OPNET SIMULATION IN A LABORATORY SET-UP

In this experiment an OPNET Modeller was used which modelled all network nodes such as switches, MU and IED. The nodes were connected with 100 base T wires obtained from OPNET pallet or library as shown in Fig. 5.24. The editors that configure a network and run the simulation are categorised as parameter, process, and project editors.

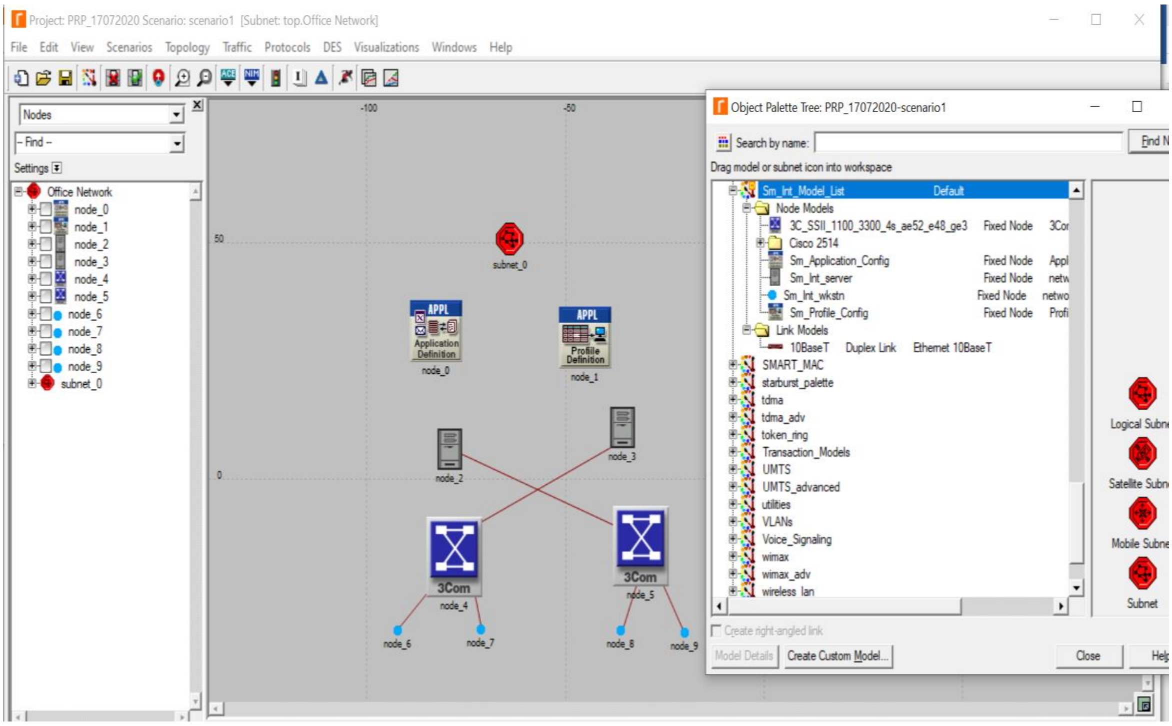


Fig. 5.24. Object pallet library having different nodes i.e., switches, MU and IEDs.

Parameter editors have MAC profile of the device, address of the port where frame shall arrive, packet size and timestamping of the frame arrival. In the process editor, program logic and different protocols are set at the onset of the project. Fig. 5.25 shows a typical project editor within star topology having various nodes and branches. This editor is built on C++ language with finite state machine and state transition diagrams (STD). Project editors allow an entire network to build up from scratch using object pallet. The algorithms of the simulated models are kept on the project profile as it conducts number of iterations in the background periodically [32].

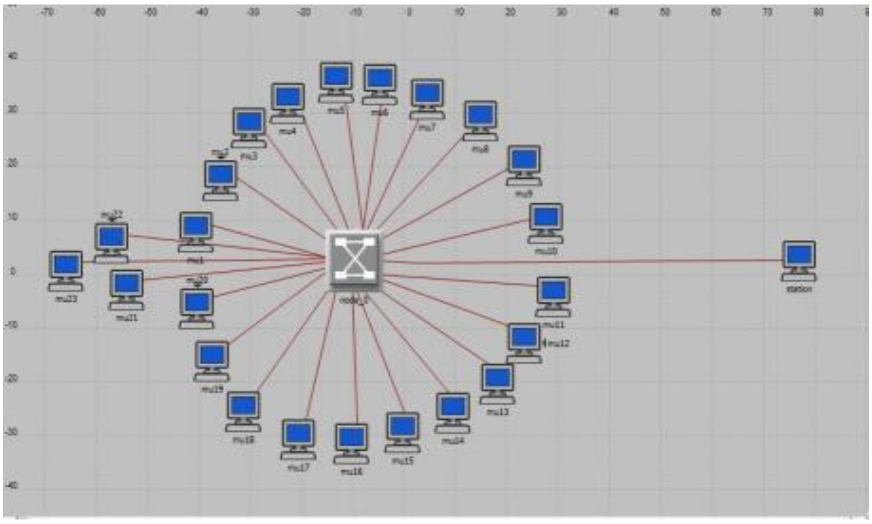


Fig. 5.25. Project editor with star topology.

Fig. 5. 26 shows OPNET simulator in which raw data source of analogue values use a bursty gen simulator run over an Ethernet network. Bursty gen defines packet format, rates, and types of time. The sink module calculates the statistical data and transfer time. The eth_mac_intf and mac modules contain algorithms and OPNET simulator does all the processing leveraging on these files. Hub_rx0 and hub_tx0 represent point-to-point receiving and transmitting packets replicating IEDs. The switches in this OPNET model follow the guidelines outlined in the IEEE 802.1Q protocol [33].

At the Curtin University laboratory, simulation of NCIT was carried out by building the project editor on an OPNET simulator and taking into account the SV and GOOSE flow from field devices to IED on an Ethernet platform as shown from a screen shot in Fig. 5.26. The evaluation of ETE and Average delay gave a good indication of the efficiencies of a digital substation network and operation of IEDs in the network.

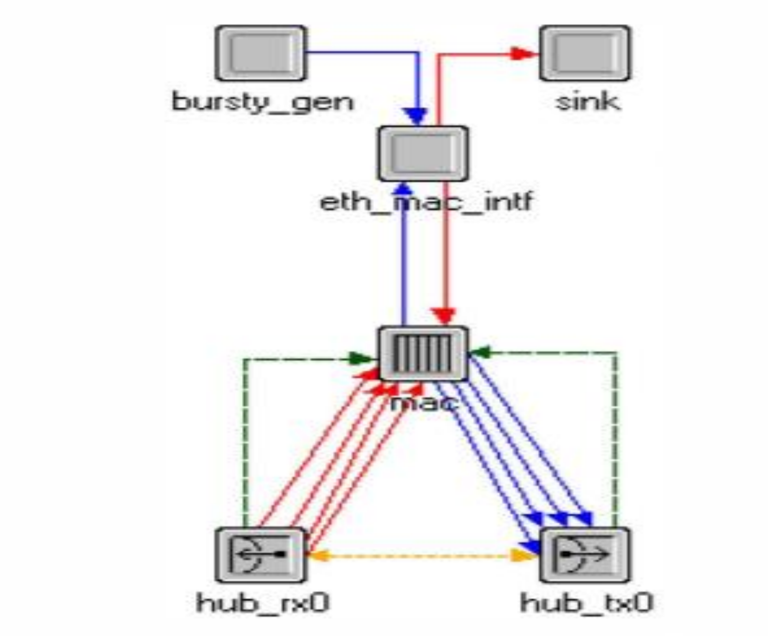


Fig. 5.26. OPNET model of the packet flow in 100baseT.

5.5 OPNET SIMULATION USING NCIT AND IEDS IN A LABORATORY SET-UP

Single line diagram (SLD) is the backbone of any substation conceptualization. SLD gives the key concept of the voltage level and the key assets of the substation. Below is the SLD of a 132-kV switchyard with two-line incomers.

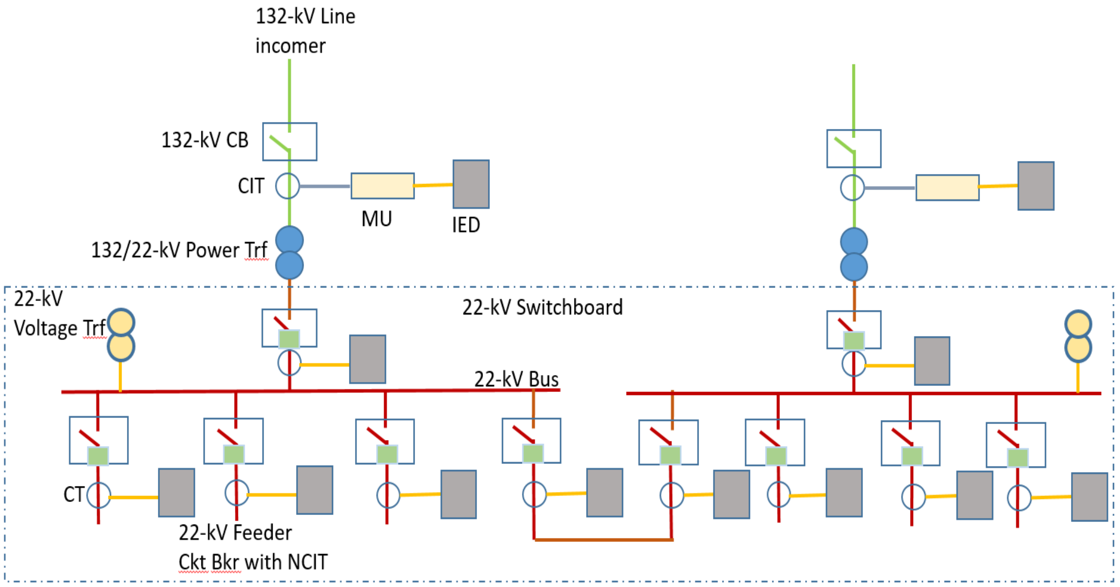


Fig. 5.27. SLD of a 132/22-kV zone substation of a utility [34].

Fig. 5.27 is a SLD of a HV substation comprising of two-line incomers at 132-kV, six feeders and two bus ties at 22-kV.

NCITs are kept in the 132-kVswitchyard as well as within the 22-kV switchboard. These devices send SV signal via MU to IEDs. In this simulation, assumption is made such that their field CITs are at 132-kV, switchboard NCITs are at 22-kV and GOOSE messages open or close the HV CBs as shown in SLD Fig. 5.25. Understanding the average delay of SV and GOOSE frames arrival at the nodes would give a better perspective of the SAS reliability. Table 5.6 provides an overview of the number of equipment in this 132-kV substation network for simulation.

Table 5.6. IED Equipment for Simulation.

Bay Name	NCIT	Incomer IEDs	Feeder IEDs	Total Equipment
132kV incomer	2 sets of CITs	2	2	6
Power Trf.	-	-	-	-
22kV incomer	2	2	-	4
22kV Feeder	6	3	-	9
Bus section	-		2	2
				21

5.6 SIMULATION USING SMART DEVICES

This simulation set-up was carried out using the project editor and with an assumption that the overall speed of the network is 100 base T as shown in Fig. 5.28. The program was run with an assumption that SV and GOOSE messages were being broadcast and subscribed by IED passing via managed switch and the origin of SV were NCITs.

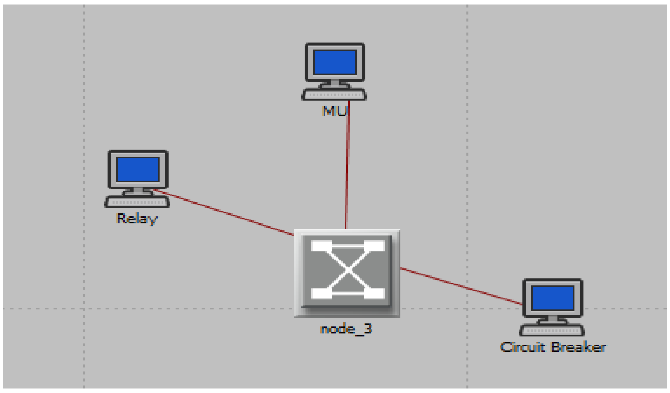


Fig. 5.28. OPNET model of the section of the network exhibiting 100 base T model network.

Fig. 5.29 shows a node model in OPNET which is similar to a physical model in the substation. Most of the mal-operation detection take place at this node as the smart algorithm in the node of IED or VLAN security of the switch is able to determine the identity of a GOOSE or SV frame. The reason for choosing 100 base T network for simulation is attributed to industry's practice of choosing this speed as this is the optimal speed of a FO or Ethernet network to operate.

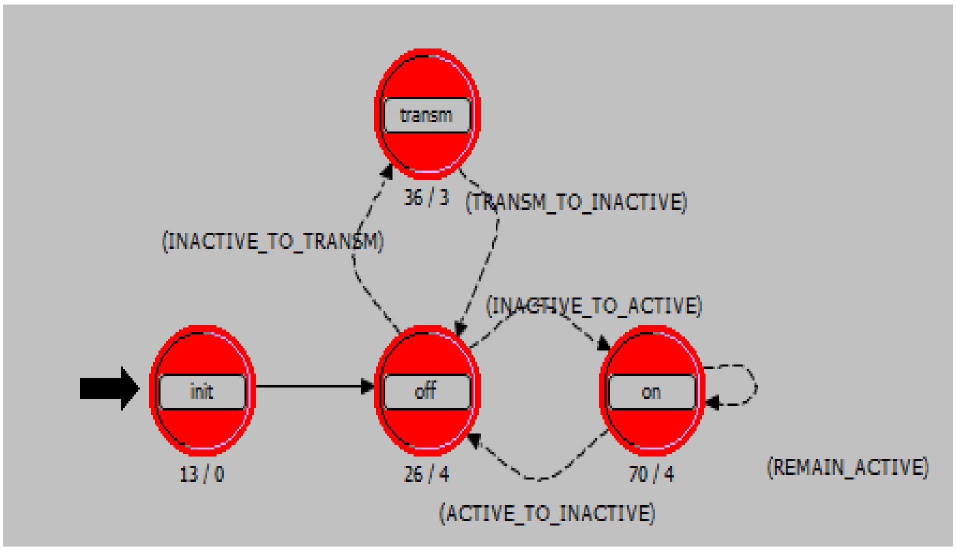


Fig. 5.29. Node model in an OPNET.

5.7 OPNET SIMULATION RESULTS AND DISCUSSION

Digital substations are still in its early stages of deployment although it has been the focus of attention since 2002. The confidence to engage with digital substation network depends upon the Average and ETE delays of SV and GOOSE frames to arrive at the nodes.

Fig. 5.30 exhibits an Ethernet delay time of GOOSE versus SV frame circulating in the network. In the characteristic populated in Fig 5.30 it is observed that the GOOSE frames have an erratic pattern of reaching the node while SV frames maintain steady flow to reach their destination. The simulation was carried at 400 kbps with the assumption that it was peak traffic, and all frames reached the destination as stipulated in IEC 61850-5 related to latency, delay, and queuing of frames at the node [35].

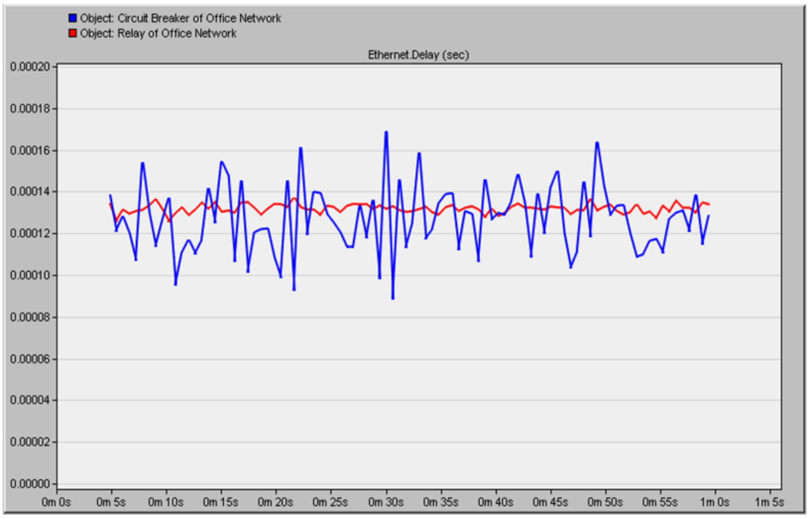


Fig. 5.30. Delay of SV and GOOSE frames arrival at nodes.

The parameters OPNET simulation were set in the project editor as shown in Table 5.7 and narrated previously in Fig. 5.29. It is inferred that the GOOSE frames took much longer time to reach the nodes as opposed to SV frames. Also, the Process bus method of protection based on IEC 61850-9-2-LE is much faster than wired relay or GOOSE based protection. Experimental results and simulation at Curtin University laboratory exhibit that digital protection IED could operate reliably with a gain of 4 ms advantage over conventional relay as shown in Fig. 5.29.

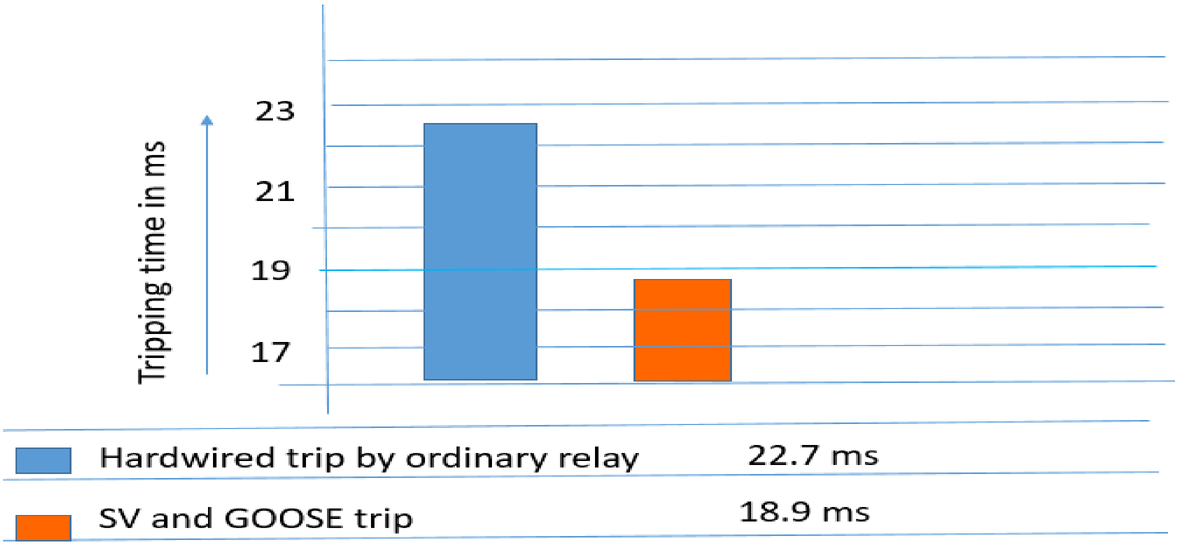


Fig. 5.31. Advantage of tripping of a digital IED over a conventional relay.

The project editor of OPNET is set with the parameters outlined in Table 5.7. The Average speed and ETE delays of frame arrival at various nodes give an overall idea of the protection to operate.

Table 5.7. List of Parameters Used in OPNET Simulation.

Tasks	2,599,479
Speed on an average (events/sec)	2,5933,49
elapsed time (ms)	1
Simulated for (Hr)	1
Log of Discrete Event Simulation	2 entries
Speed of LAN communication (Mbps)	75
Burst or Frame speed (Kbps)	400
Loss of frames (per sec)	3
Rate of sampling (Hz)	4800

Table 5.8 provides the simulation results of delay occurring of SV and GOOSE as they pass via various nodes with a LAN speed of 100 Mbps and sampling rate of 4900 Samples/s.

Table 5.8. SV and GOOSE Message ETE Delay in OPNET Simulation.

Speed of the network (Mbps)	Rate of sampling (Sample/sec)	End to End Delay of SV frames (µs)		End to End delay of GOOSE frames (µs)	
		Ave.	Max	Ave	Max
100	4800	133	149	175	193

End-to-End delay of SV and GOSSE frames demonstrates that Process bus topology is more suited for the protection of substation equipment and that SV packets pass through the traffic due to its priority tagging, although there have been losses on the way to its destination. This simulation undertaken leveraging on IEC 61850-9-2 guidance confirms that the frames arrive within 4 µs tolerance.

Also, the combi-sensors i.e., NCITs used at Curtin laboratory performance was superior from protection and measurement points of view. However, these sensors need to be carefully handled if subjected to harsh environmental condition. They could erratically behave due to settlement of dust and foreign particle on them. The accuracy and errors are much superior to CITs as they can operate from -4 ºC to 50 ºC. Application of the correction factor and suitable information into SMU 615 needs be done. The special cables from ABB make sensors adapt well with SAMU 615 which is taken to a managed switch.

5.8 CHAPTER SUMMARY

Although Process bus topology has been in existence for a decade, not many substations are deploying this topology. The lack of knowledge and understanding of the digital devices could be one of the key reasons. Compounding these issues are nonexistence of sound understanding of the data packet flow of SV and GOOSE in the network, erratic behaviours during peak traffic and data clogging. These limitations need to be fully understood through experimental validation and research which has been the highlight of this chapter, by simulating on desktop and following it up with practical tests on HV NCITs as applicable to a utility substation.

Experimental results heavily favour NCITs and recommend its deployment due to superiority over the based on key performance indices, such as Average and ETE delay, DC offset and frequency response of the apparatus. It is envisaged that NCIT shall herald a new paradigm in SAS due to lack of ferromagnetic material and reduced copper wires in the circuit. It probably shall become a game changing retrofit in the protection world.

5.9 REFERENCES

[1] D. M. Robalino and I. Güner, "Investigation of EHV Current Transformer Failure by Dielectric Frequency Response Technique," *2020 IEEE Electrical Insulation Conference (EIC)*, Knoxville, TN, USA, 2020, pp. 72-75, doi: 10.1109/EIC47619.2020.9158762.

[2] D. Burgund and S. Nikolovski, "Comparison of Functionality of Non-Conventional Instrument Transformers and Conventional Current Transformers in Distribution Networks," *2022 International Conference on Smart Systems and Technologies (SST)*, Osijek, Croatia, 2022, pp. 55-60, doi: 10.1109/SST55530.2022.9954785.

[4] G. Y. Chen and T. P. Newson, "Detection of fibre-optic current sensors based on faraday effect," The IET Journals & Magazines, vol. 50, Issue 8, 2014.

[5] Th. Buhagiar, J-P. Cayuela, A. Procopiou, S. Richards: Poste Intelligent-the Next Generation Smart Substation for the French Power Grid. PS3-305 – CIGRE SC B5 Colloquium September 2015 Nanjing, China

[6] T. S. Sidhu and Y. Yin, "Modelling and simulation performance evaluation of IEC 61850 based substation communication system", *IEEE Trans. on Power Del.,* vol. 22, no. 3, 2007.

[7] IEC 61850-9-2 2004, Communication Networks and Systems in Substations – Part 9-2: Specific Communication System mapping (SCSM) – Sampled Values Over ISO/IEC 802-3, First Edition, May 2005.

[8] S. Kumar, N. Das, S. Islam and A. Abu-Siada, " A Fast and Reliable Blocked Bus Bar Protection Scheme Leveraging on Sampled Value and GOOSE Protection based on IEC 61850," *2021 30th Australasian Universities Power Engineering Conference (AUPEC),* Perth, Australia 2021, pp. 1-6978-1-6654-3451-5/21

[9] R. Amoah, S. Camtepe and E. Foo, "Securing DNP3 Broadcast Communications in SCADA Systems*," in IEEE Transactions on Industrial Informatics, vol. 12, no. 4, pp. 1474-1485,* Aug. 2016, doi: 10.1109/TII.2016.2587883

[10] IEC 61850-5: Communication networks and systems for power utility automation - Part 5: Communication requirements for functions and device models

[11] M. G. Kanabar and T. S. Sidhu, “Performance of IEC 61850-9-2 Process bus and Corrective measure of digital relaying.” IEEE Trans. on Power Del., vol. 26, no. 2, 2007.

[12] P. Schaub, J. Haywood, D. Ingram, A. Kenwrick, and G. Dusha, “Test and Evaluation of Non-Conventional Instrument Transformers and Sampled Value Process bus on Powerlink’s Transmission network*”,* Cigre Panel B5, SEAPAC 2011, Sydney, Australia.

[13] UCA “Implementation guideline for digital interface to instrument transformer using IEC 61850-9-2”, *UCA International User Group*, Raleigh, NC, USA.

[14] J. Schmid and M. Schumarcher, “IEC 61850 Merging Unit for the universal connection of conventional and Non-Conventional Instrument Transformers,” Cigre, AS-306, 2008.

[15] K. Liu, X. Dong, and Z. Bo, “Current differential protection based on non-conventional instrument transformer and IEC 61850.” in proc. of the 43rd Universities Power Engineering Conference 2008 (UPEC 2008), 1~4 September 2008, Padova, Italy.

[16] J. Schmid and M. Schumarcher, “IEC 61850 Merging Unit for the universal connection of conventional and Non-Conventional Instrument Transformers,” Cigre, AS-306, 2008.

[18] ALSTOM cost comparison spreadsheet, Private Communications/ Consultations with Engineers, 2015.

[19] N. Paviya, A. Varghese, M. Boucherit, P. Newman, and P. Diemer, “IEC 61850 Process bus application in Energinet Denmark,” in proc. of the 12th IET International Conference Developments in Power System Protection (DPSP 2014), Copenhagen, Denmark, 2014.

[20] IEC 61850-9-2 LE, Implementation Guideline for Digital Interface to Instrument transformers Using IEC 61850-9-2, UCA International Users Group.

[21] S. Kumar, N. Das, S. Islam and A. Abu-Siada, "Toward a Substation Automation System Based on IEC," *2021*. Electronics 2021, 10, 310. https://doi.org/10.3390/electronics 10030310

[22] IEC 61850-9-2: Specific communication service mapping (SCSM) - Sampled values over ISO/IEC 8802-3

[23] K. Hinkley and D. Batger, "TransGrid's journey to a full digital substation", SEAPAC 17-APB5, 14-15 September, Melbourne, Australia

[24] J. Schmid and M. Schumarcher, "IEC 61850 Merging Unit for the universal connection of conventional and Non-Conventional Instrument Transformers," Cigre, AS-306, 2008.

[25] N. Das. W. Ma, and S. Islam, "Comparison study of various factors affecting end to end delay in IEC 61850 substation communication using OPNET", in proc. of the Australasian Power Engineering Conferences 2012 (AUPEC 2012), Bali, Indonesia, 26-29 Sept. 2012.

[26] D. M. E. Ingram, P. Schaub, R. R. Taylor, and D. A. Campbell, "Performance analysis of IEC 61850 Sampled Value process bus networks," IEEE Trans. on Industrial Informatics, vol. 9, issue No. 3, 2013.

[27] L. Li, D. Zhang and Y.Dong, "Time synchronization technology for the smart substations,"*2011 International Conference on Advanced Power System Automation and Protection,* Beijing, China, 2011, pp. 2283-2285, doi: 10.1109/APAP.2011.6180808.

[28] C. A. Outra, S. L. Zimath, H. Rachade and L. B. de Oliveira, "Substation time synchronization in today and future architectures," *12th IET International Conference on Developments in Power System Protection (DPSP 2014),* Copenhagen, Denmark, 2014, pp. 1-6, doi: 10.1049/cp.2014.0082.

[29] D. M. E. Ingram, P. Schaub, D. A. Campbell and R. R. Taylor, "Evaluation of Precision Time synchronisation methods for substation applications," *2012 IEEE International Symposium on Precision Clock Synchronization for Measurement, Control and Communication Proceedings, San* Francisco, CA, USA, 2012, pp. 1-6, doi: 10.1109/ISPCS.2012.6336630.

[30] M. Kanabar, "Investigation performance and reliability of process bus networks for digital protective relaying," The University of Western Ontario, The school of graduate and postdoctoral studies, PhD thesis, 2007.

[31] IEC 60044-8:2002 - Instrument transformers - Part 8: Electronic current transformers.

[32] M. Kaczmarek, "Accuracy of current transformer with current errors at harmonics equal to the limiting values defined in IEC 60044-8 standard for transformation of distorted primary current," *2015 Modern Electric Power Systems (MEPS),* Wroclaw, Poland, 2015, pp. 1-4, doi: 10.1109/MEPS.2015.7477205.

[33] OPNET Modeler–OPNET Technologies, [Online]. Available in the weblink: http://www.opnet.com

[34] IEEE 802.1 Q Networking standard that supports virtual local area networking (VLANs) on an IEEE 802.3 Ethernet network.

[35] D. M. E. Ingram; P. Schaub, R. R. Taylor, and D. A. Campbell, “System-level tests of Transformer differential protection using an IEC 61850 Process bus,” IEEE Trans. on Power Del., vol. 29, issue No. 3, 2014

[35] S. Kumar, N. Das, S. Islam and A. Abu-Siada, "Toward a Substation Automation System Based on IEC," *2021*. Electronics 2021, 10, 310. https://doi.org/10.3390/electronics 10030310

CHAPTER 6:

PERFORMANCE TESTING OF MULTIVENDOR DIGITAL PROTECTION SCHEMES IN A LABORATORY ENVIRONMENT

6.1 INTRODUCTION

Digital SAS is gradually gaining popularity due to ease of maintenance and quick diagnostics. More and more utilities and industries are focusing their attention on digital protocols and vendors are ensuring that their devices communicate with other manufacturers' devices thus minimising interoperability issues in an SAS network [1]. The smart devices and information technology layers within these smart devices have connotations similar to "*html*" when information technology was making wave in in early 1990s. However, digital SAS has a few issues with latencies, data corruption, traffic jamming and interoperability which issues could be addressed better at the laboratory environment [2]. A practical Blocked Busbar Protection (BBP) scheme has been tested and, in this chapter, the results validated BBP from a protection reliability perspective. Practical testing was performed at the Curtin University IEC61850 laboratory, Perth, Australia in a mining process plant that could use digital SAS. It was observed that this testing and validation could herald a new paradigm in protection using smart IED and peripherals connected using Ethernet or FO wires.

6.2 BACKGROUND OF DIGITAL SAS

The main requirement of protection schemes is to isolate the fault in the fastest possible time, preventing catastrophic burnout, a catastrophic failure of power equipment. Researchers are constantly working towards making diagnostics easy by continuously monitoring the network and this could be achieved by the IEC 61850 protocol. However due to the proprietary features of IEC 61850 compatible devices, it is imperative to test the protection system prior to deployment [3]. A number of experimental testings to validate the results were conducted in a laboratory environment, to test the performance of managed switches, IEDs, Red Boxes, and other secondary system peripherals to prove the reliability of the SAS system. There are multiple advantages in using IES 61850 protocol such as minimisation of copper wires in te secondary, reduced cubicle size of the protection panel, smaller trenches and continuous condition monitoring of the network for GOOSE and SV frames, and ease of detection disturbances [4]. Application of smart CBs has led to ease of interlocking and blocking schemes which would be more complex to achieve in a more conventional method than with GOOSE and SV frames, which replicate almost all the protection concept that could be achieved using copper wires such as Bus bar protection [5]. Transformer differential protection, Line differential protection, Feeder protection, Generator protection etc. Table 6.1 provides a comparative analysis between digital versus conventional methods of protection.

Table 6.1. Digital Versus conventional Bus Bar Protection [6].

Conventional	Digital
Interposing relays could be slow acting and may introduce delays in tripping the relays	SV and GOOSE frames are much faster to act over a FO network than conventional protection
High chances of CT opening its secondary terminals and saturation could take place	Fast data communication through GOOSE messages with minimal chances of NCIT affected by saturation due to sensor technology
More wires at the terminals of instrument transformers	One Ethernet or FO wire to IED is unlike three wires from CT to conventional protection relays

A Blocked Bus Bar (BBP) has been tested and results validated, reported in this chapter, and provided with the effectiveness of a digital protection system that is also easy to implement. The laboratory test used a number of multivendor equipment, and the reliability of protection was validated for an SAS network. The scheme tested faults occurring within and outside the fault zone as well as the effect of discontinuity of wire. Busbars are of critical importance in an HV switchboard, and its protection depends upon its service area pertaining to a utility or industry. In a utilities set-up, a differential bus bar protection is a must to have but, in a mining, set up it suffices to have a BBP in its simplest form [7].

In Fig. 6.1, SLD a single busbar with three outgoing feeders and one incomer is shown. In the three fault scenarios, the test validated the superiority in reliability of the digital SAS over the conventional one. The Inverse Definite Multiple Time (IDMT) and earth element of the feeder relay usually acts and latches the conventional relay. It prevents incomer relay from acting instantaneously as the logic ensures it acts only and after a delay; should the feeder relay not respond; it allows the incomer relay to act [8]. The experiment conducted at Curtin University used GOOSE and SV to trip command to a HV CB while blocking incomer IED and delayed it to act as back up after 10 milliseconds. A MU that streams SV packets from field equipment interfaces with IEDs broadcasts different signals depending upon the condition of the network.

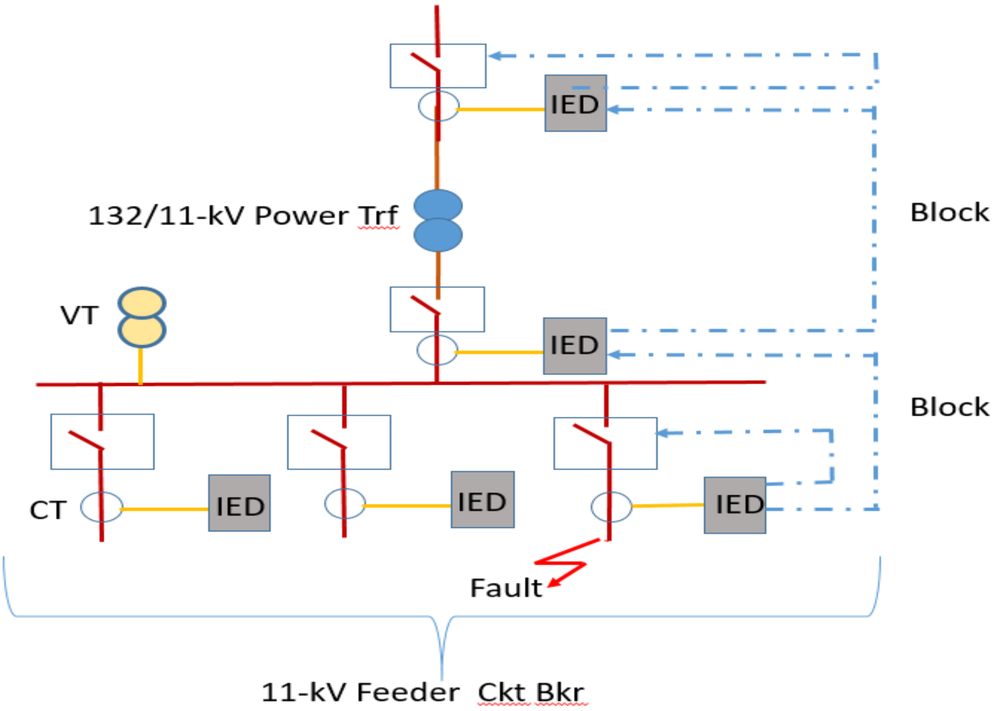


Fig. 6.1. Blocked feature of a typical Bus bar [9].

Station and Process bus topology have been elaborated in Chapter 2. GOOSE messages have been deployed to trip CB at many utilities substation e.g., Western Power in Perth, Australia. At Process bus level switchyard equipment such as isolator, CT, VT, Power Transformer and CB are monitored using SV. The production of SV occurs when MU are kept in the switchyard. In a Process bus topology, MU devices are usually located near to the primary plants either in the switchyard or within the switchboard. While Station bus prefers horizontal communication Process bus controls and commands CB using vertical communication in an SAS network [10]. GOOSE and SV packets are utilised for control and command and provide CB status to local and remote-control rooms. Smart substation equipment continuously monitors the GOOSE and SV packets circulating in the network. An alert at the nodes for malformed packets is detected with a number of software tool available. There is a high bandwidth requirement for bursts of SV and GOOSE messages to circulate along with time synchronisation for validation of certain protection schemes like distance protection of two WAN substation. The rate at which SV circulation occurs at 80 samples per cycle having 5-6 Mb per stream of data are exhibited in Fig. 6.2 produced by a MU [11]. These SV travel much faster than conventional current and voltage as they travel over FO wires.

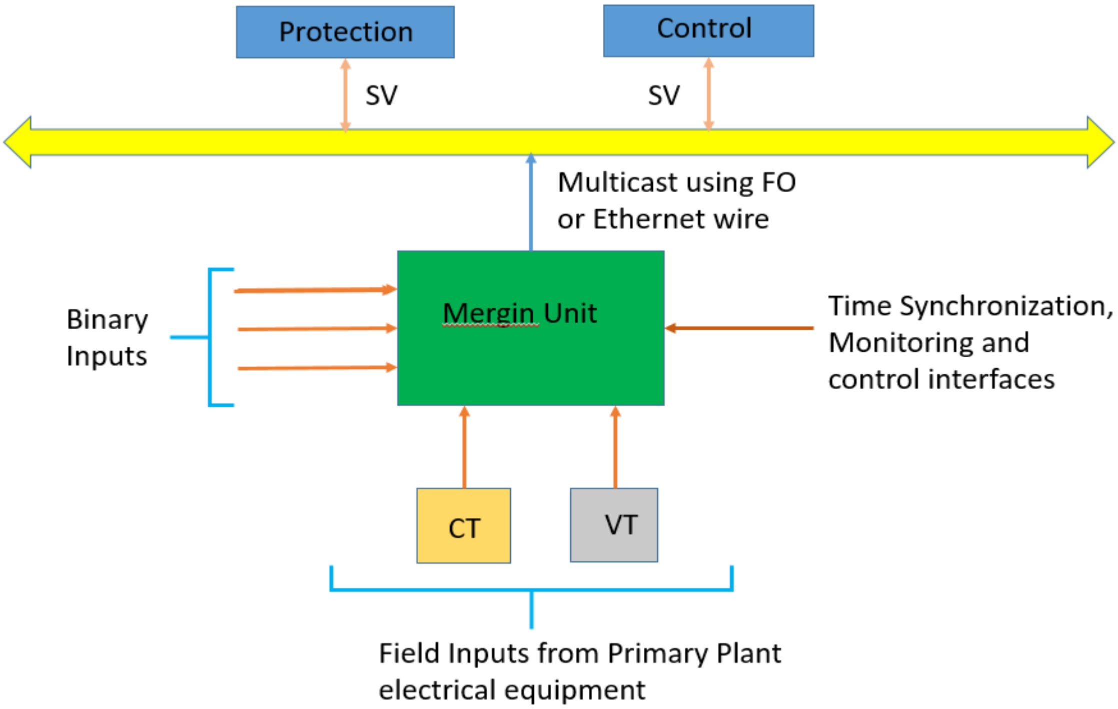

Protection
Control
SV
SV
Multicast using FO or Ethernet wire
Binary Inputs
Mergin Unit
Time Synchronization, Monitoring and control interfaces
CT
VT
Field Inputs from Primary Plant electrical equipment

Fig. 6.2. Production of SV from a MU at the field [12].

GOOSE, SV, and Manufacturing Machine Specification (MMS) frames circulating in network perform important tasks for automation. MMS and GOOSE perform horizontal communication while SV and R-GOOSE do vertical communication and carry frames over a long distance for substation automation [12]. While it is alright to have digital topologies in Station or Process bus, what principally guides the end user is its reliability to trip the CB during a fault using GOOSE or SV. An unwanted traffic jam and an excessive burst of SV or GOOSE stream could have an adverse impact on the network protection. Hence it is important to have VLAN filters to allow specific frames to pass through. In the given experiment a tree topology was considered to provide for expandability of the network in future [13].

Table 6.2. Features of Data Packets Circulating within a Digital Substation [14].

Type of messages	IEC standard applied	Typical application	Media of circulation	Final reaching point
GOOSE	IEC 61850-8	CB open, close available and status	Ethernet, Multicast	IEDs in station and process buses
SV	IEC 61850-9-2	Time synchronised and rapid burst at regular interval	Ethernet Multicast	Between Process and Station bus
MMS	IEC 61850-8	used in conventional substation for supervisory control and data acquisition (SCADA)	TCP/IP unicast	Station and Process buses

In Chapter 2, tree topologies advantages have been discussed at length. The experiment at Curtin University with multi-vendor equipment in tree topology had the following consideration as shown in Table 6.3.

Table 6.3. Importance of Tree Topology in BBP Scheme [15].

Consideration	Expandability of the network
Fault Tolerance	More reliable than bus or ring topology
Availability	Mostly available in the network
Latency	Low compared to bus and ring
Bandwidth	High
Expansion	A key feature
Implementation	Easy to implement with compatible equipment

The following section gives the details of testing and discussion of digital substation protection.

6.3 TESTING AND VALIDATION OF DIGITAL SUBSTATION

6.3.1 Bus Bar Testing

Busbar protection has a few protection challenges that are not often seen during commissioning stages. A typical single busbar system has been illustrated in Fig. 6.3 in the SLD that represents a HV switchboard with one incoming and three outgoing feeders at 11-kV level. The three fault scenarios have been shown which replicates true site condition in the form of bus fault, feeder fault and disconnection or break in FO wiring [16].

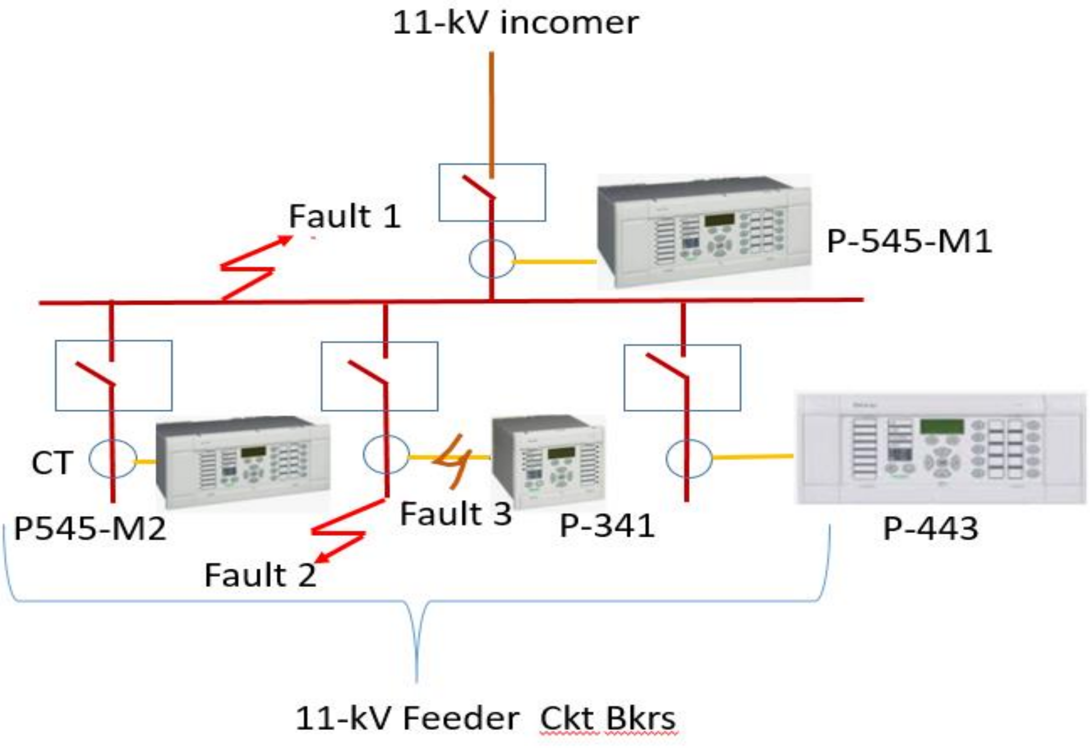


Fig. 6.3. SLD of the IEDs in the Network Experiment.

A number of multivendor equipment have been connected in IEC 61850 protocol in Station and Process bus mode as shown in Table 6.4 but not limited to IEDs, switches, MU etc. A secondary injection kit has been used to inject current into IEDs which is similar to CITs feeding analogue signals to relays. A summary of equipment used and results accrued is given in Table 6.4.

Table 6.4. Use of Multi-vendor Equipment And Software In The Practical Testing.

Hardware	Software	Remarks
Omicron CMC356	Test universe	This secondary test kit is used for injecting current and voltage into IEDs and MU. This kit has the ability to produce directly GOOSE and SV.
Alstom MU	S1 Agile	This device when injected with current and voltage produced SV. This is connected to a managed switch with FO wire.
SEL 2488 Switch	Accelerator	This device is a managed switch which accepts GOOSE and SV using VLAN gate.
Two Schneider IEDs P543-M1 and P-545-F2	Easergy	One of the IED P545-M1 acts as the protection device for the bus bar incomer and the other for feeder. The logic in the IED is set using Easergy software in the IED. These two IEDs subscribe and transmit GOOSE and SV in the experiment.
Alstom P443	S1 Agile	This IED subscribes to GOOSE and acts as a feeder protection in the experiment.
Schneider P341	Easergy	This device subscribes to GOOSE frames and acts as a feeder protection in the experiment.
Laptop	Thinkpad	All software such as IED Scout, SV scout to monitor GOOSE and SV and IED software such as S1 Agile, Easergy, Accelerator etc. have been installed here and it can connect with the switch using an Ethernet wire.
Wireshark	General software	This important software has been installed in the laptop which monitors the flow of SV and GOOSE traffic in the network.
IED Scout	Software by Omicronenergy	This software installed in the laptop which detects all GOOSE compliant IEDs in the network.
SV scout	Software by Omicronenergy	This software installed in the laptop which detects all SV in the network.

All relevant software of the applied devices i.e., IEDs, secondary injection kit, MU used in the experiment are shown in Fig. 6.4.

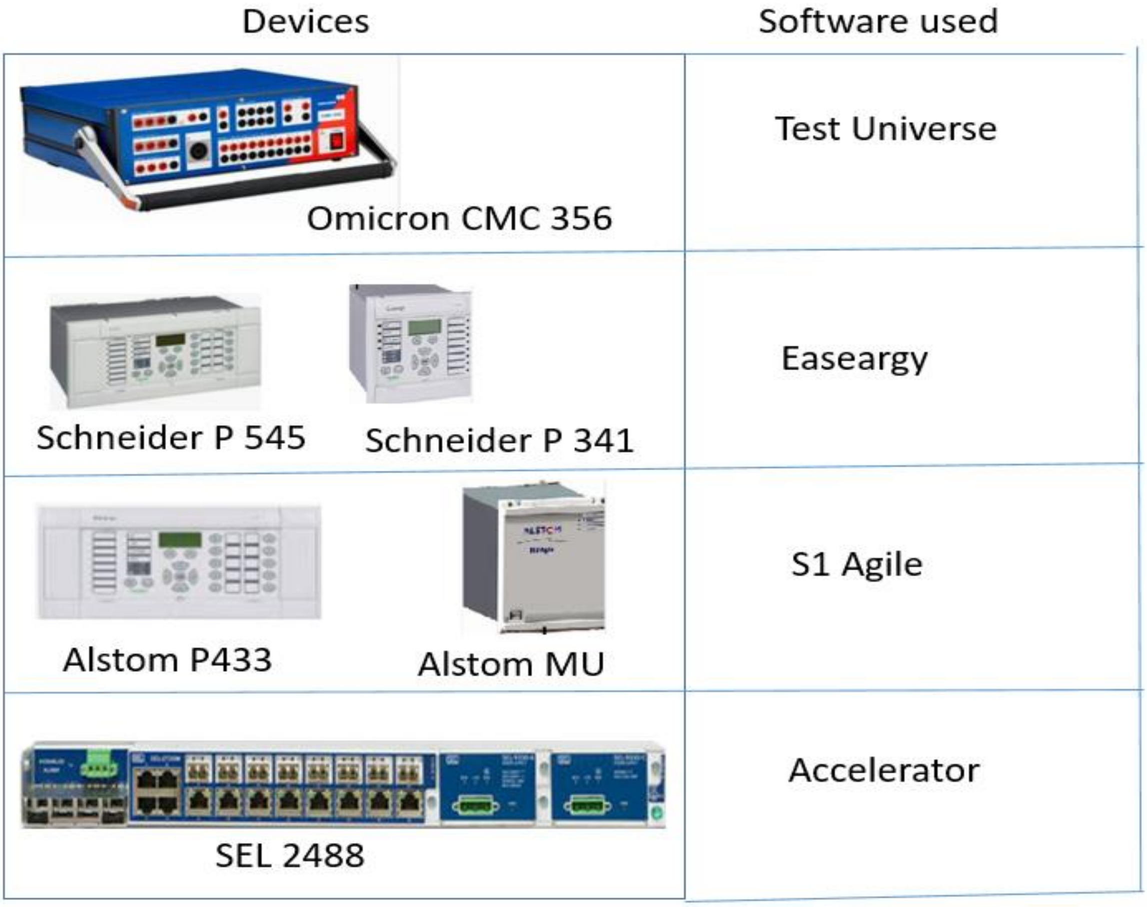


Fig. 6.4. Multi-Vendor Devices Used in the Experiment.

In the experiment three types of fault scenarios, shown in Fig. 6.5, tested the digital protection system using GOOSE and SV. All program logics and VLANs were installed into IEDs, MU and managed switch using relevant software, and using the laptop. All network devices such as IEDs and MU were detected by IED Scout and validated for their presence in the network by GOOSE detection method. Similarly, all SV circulating in the network after performing a secondary injection, were detected by sinusoidal wave pattern. GOOSE and SV flow in the network is further monitored by Wireshark tool. Alstom MU produced SV and circulated it to the targeted IED via a managed switch. These SV frames reach the subscribing Process bus incomer IED i.e., P545-M1 and in the event of a bus bar fault at the incomer, P535-M1 tripped. The program logic of P545-M1 guards against instantaneous trip of feeder IEDs which maintain a delay of 4 ms before all three tripping i.e., F1, F2 and F3 as narrated in the case studies below:

Case 1: F1 is a busbar fault; Case 2: F2 is a feeder fault which enables tripping of its own IED while blocking the incomer IED for a delay of 4 ms; Case 3: Status of F3 due to disconnection of feeder IED.

The connection of IEDs, MU and managed switch is shown in Fig. 6.5.

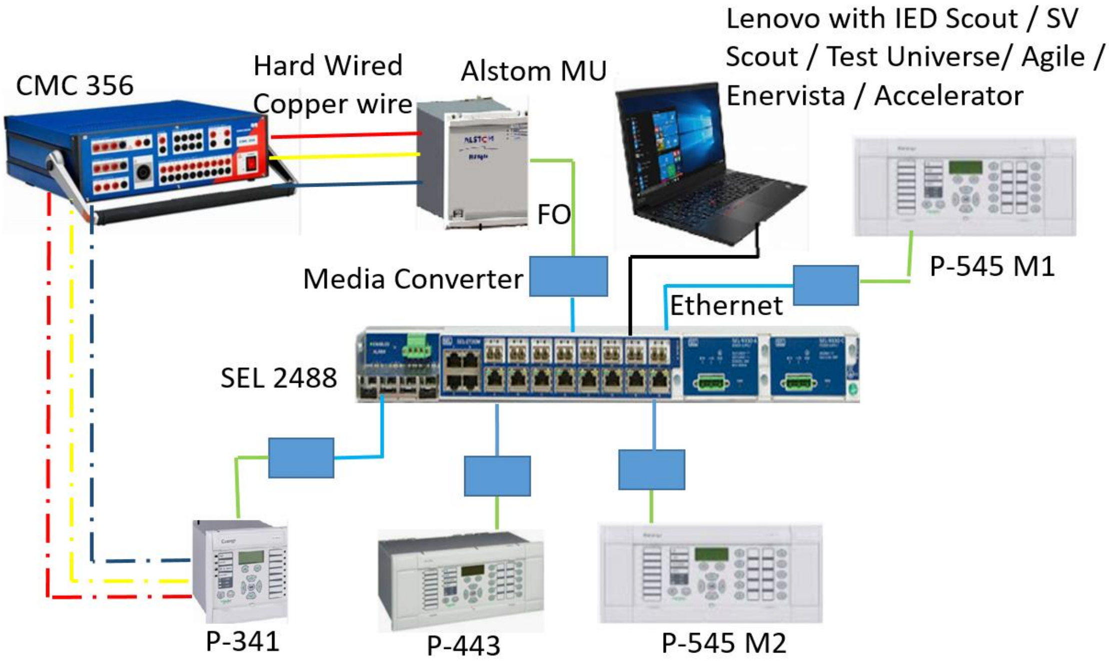
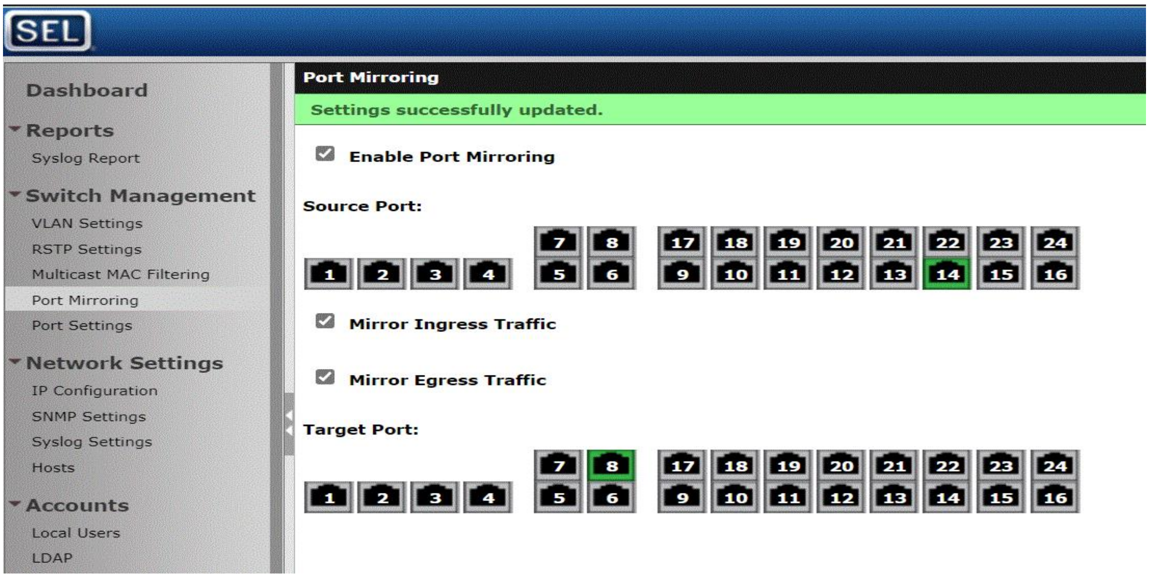


Fig. 6.5. Experimental Set-up to Test BBP Scheme Digitally.

VLAN within SEL switch managed GOOSE and SV traffic. All GOOSE and SV traffic was assigned 2 and 3 for SV respectively, which provided filtering and security to a busy network. This connection was set up to carry out communication with multiple devices of different manufacturers and allowed communication. Fig. 6.6 shows ports of SEL 2456 having its VLAN configured at each port to subscribe and transmit GOOSE and SV frame.



Port Mirroring

Settings successfully updated.

☑ Enable Port Mirroring

Source Port: 14

☑ Mirror Ingress Traffic

☑ Mirror Egress Traffic

Target Port: 8

Fig. 6.6. SEL Ports Connected To Test Kits, IEDs, MU And Laptop For GOOSE and SV Traffic Flow Conditions.

Fig. 6.7 is the logic diagram built within P545-M1 using Easergy tool using AND and OR gate. A delay of 50 ms was given between incomer IED and other feeder IEDs to test for blocking stability. The delay between IEDs and blocking has been described in scenarios 1 and 2.

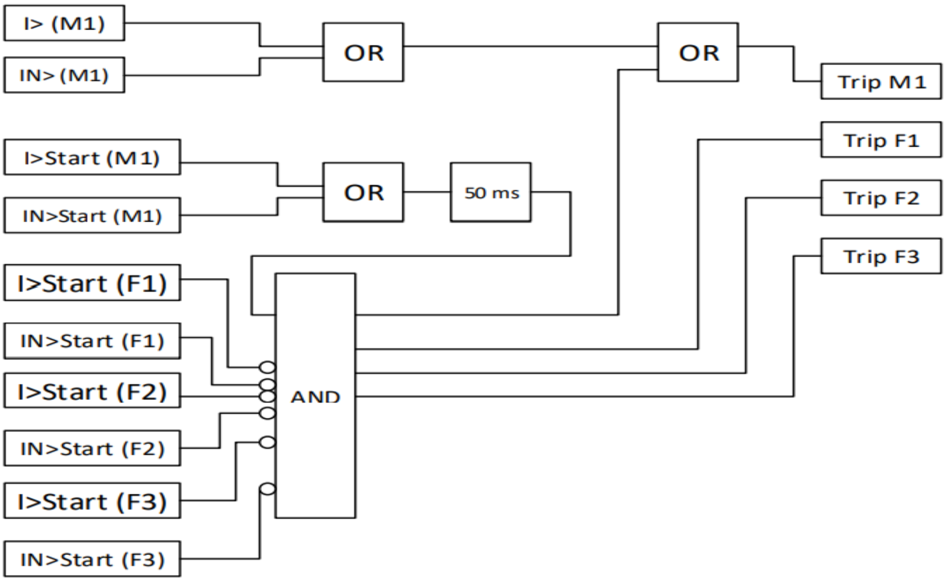


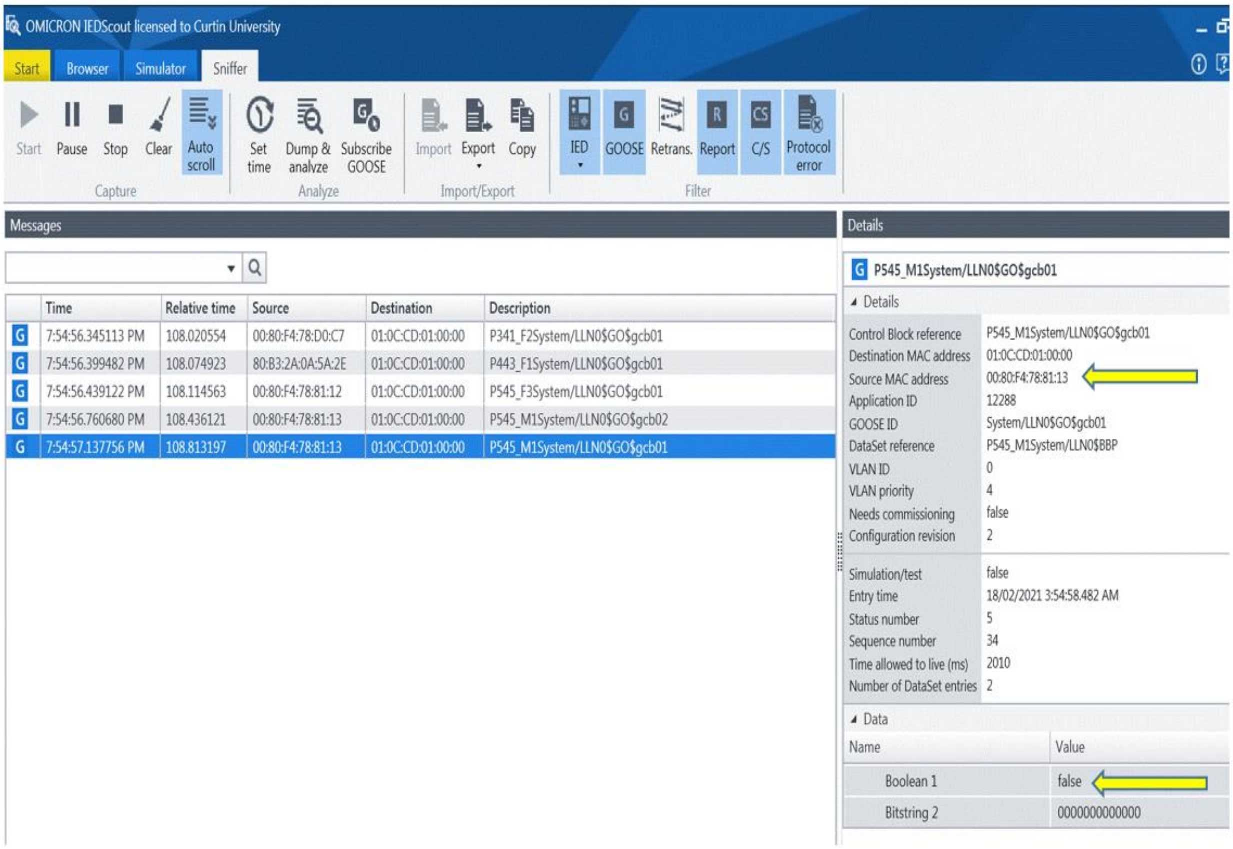
Fig. 6.7. BBP Conceptual Logic Flow Diagram.

Case 1: When there is a Bus fault (Fault F1)

To simulate this test at Curtin University laboratory, Omicron CMC 356 injected current only to incomer IED i.e. P545-M1 for 1.2A while the threshold of the IED was set to 1.1A. No current was injected into the other three feeders and resulted in an instantaneous trip in incomer

IED. Once IED P545-M1 operated its LED turned red from green. Case 1 is a bus fault scenario wherein a dead short in the protected zone of bus needs to be cleared instantly as indicated in Fig. 6.5. The program logic of P-545-M1 IED blocks feeder IEDs from acting instantaneously i.e. P443-F1, P545-M2, and P341-F3 but operates after a delay with an assumption that the main incomer IED didn't operate instantaneously.

Figs. 6.8 and 6.9 are screen shots of IED Scout which indicate the status of this incomer IED before and after the fault on the bus. The input to Alstom MU was given by the secondary injection kit which produced SV frames as shown in Fig. 6.8. These SV fames were subscribed by incomer IED P545-M1 and carried out the trip by turning its LED to red from green. After a delay of 50 milliseconds a trip signal was sent out to the three feeder IEDs i.e. P545-M, P-343 and P443. Also, Fig. 6.8 and Fig. 6.9 show the IED settings such as VLAN priority, MAC source and destination. IED Scout screenshots in Fig. 6.8 and Fig. 6.9 further exhibit the IEDs that have been circulating frames in the network and its status change. Fig. 6.8 is the screenshot of IED scout before the inception of the fault which is at "false" state.



	Time	Relative time	Source	Destination	Description
G	7:54:56.345113 PM	108.020554	00:80:F4:78:D0:C7	01:0C:CD:01:00:00	P341_F2System/LLN0$GO$gcb01
G	7:54:56.399482 PM	108.074923	80:B3:2A:0A:5A:2E	01:0C:CD:01:00:00	P443_F1System/LLN0$GO$gcb01
G	7:54:56.439122 PM	108.114563	00:80:F4:78:81:12	01:0C:CD:01:00:00	P545_F3System/LLN0$GO$gcb01
G	7:54:56.760680 PM	108.436121	00:80:F4:78:81:13	01:0C:CD:01:00:00	P545_M1System/LLN0$GO$gcb02
G	7:54:57.137756 PM	108.813197	00:80:F4:78:81:13	01:0C:CD:01:00:00	P545_M1System/LLN0$GO$gcb01

G P545_M1System/LLN0$GO$gcb01

Details

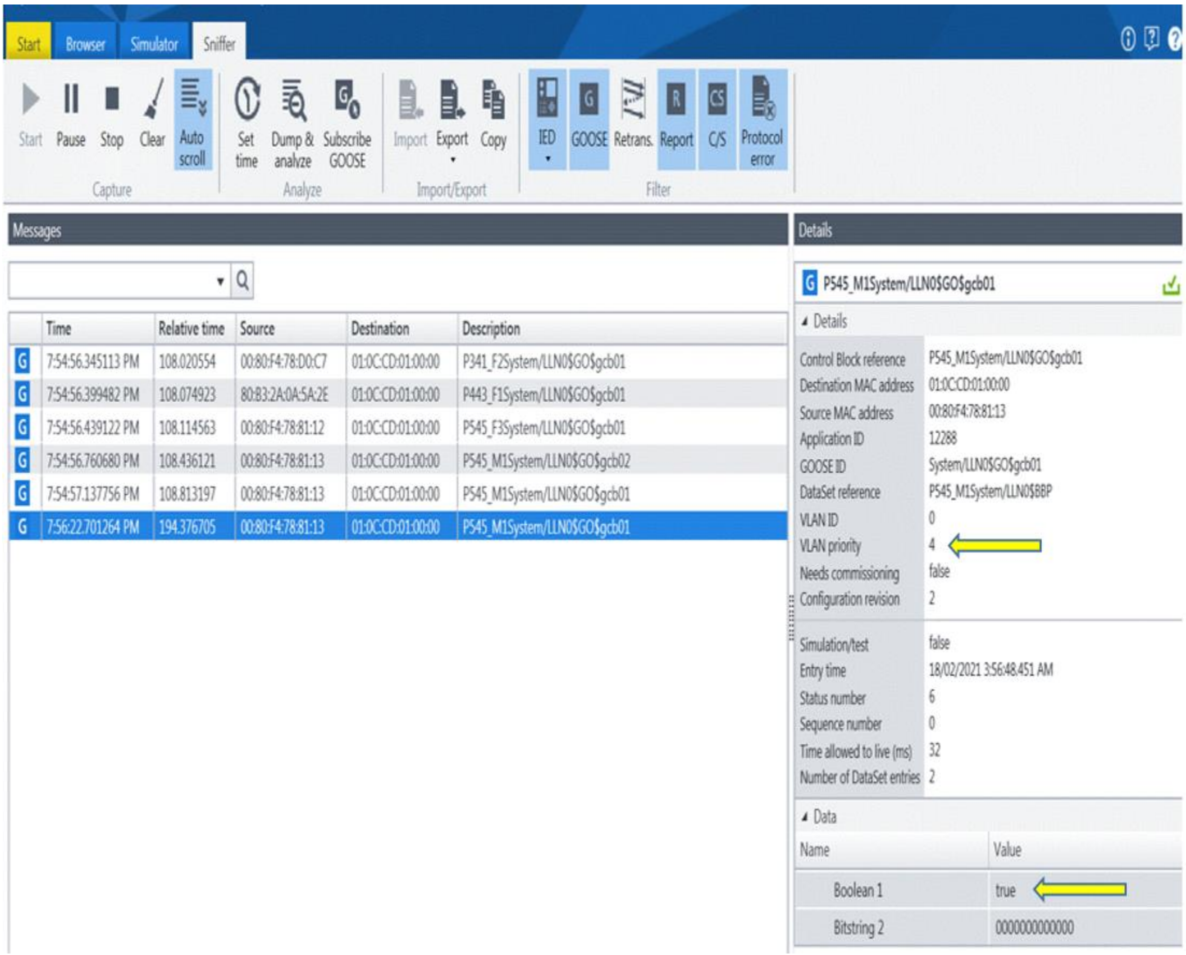
Control Block reference	P545_M1System/LLN0$GO$gcb01
Destination MAC address	01:0C:CD:01:00:00
Source MAC address	00:80:F4:78:81:13
Application ID	12288
GOOSE ID	System/LLN0$GO$gcb01
DataSet reference	P545_M1System/LLN0$BBP
VLAN ID	0
VLAN priority	4
Needs commissioning	false
Configuration revision	2
Simulation/test	false
Entry time	18/02/2021 3:54:58.482 AM
Status number	5
Sequence number	34
Time allowed to live (ms)	2010
Number of DataSet entries	2

Data

Name	Value
Boolean 1	false
Bitstring 2	0000000000000

Fig. 6.8. Status of P-541-M1 Before Inception of the Fault.

Fig. 6.9 exhibits of the status of IED P545-M1 after the bus fault F1 occurs, thus changing its status. The change of status was recorded as “true” as seen in a IED scout tool.



	Time	Relative time	Source	Destination	Description
G	7:54:56.345113 PM	108.020554	00:80:F4:78:D0:C7	01:0C:CD:01:00:00	P341_F2System/LLN0$GO$gcb01
G	7:54:56.399482 PM	108.074923	80:B3:2A:0A:5A:2E	01:0C:CD:01:00:00	P443_F1System/LLN0$GO$gcb01
G	7:54:56.439122 PM	108.114563	00:80:F4:78:81:12	01:0C:CD:01:00:00	P545_F3System/LLN0$GO$gcb01
G	7:54:56.760680 PM	108.436121	00:80:F4:78:81:13	01:0C:CD:01:00:00	P545_M1System/LLN0$GO$gcb02
G	7:54:57.137756 PM	108.813197	00:80:F4:78:81:13	01:0C:CD:01:00:00	P545_M1System/LLN0$GO$gcb01
G	7:56:22.701264 PM	194.376705	00:80:F4:78:81:13	01:0C:CD:01:00:00	P545_M1System/LLN0$GO$gcb01

G P545_M1System/LLN0$GO$gcb01

Details

Control Block reference	P545_M1System/LLN0$GO$gcb01
Destination MAC address	01:0C:CD:01:00:00
Source MAC address	00:80:F4:78:81:13
Application ID	12288
GOOSE ID	System/LLN0$GO$gcb01
DataSet reference	P545_M1System/LLN0$BBP
VLAN ID	0
VLAN priority	4
Needs commissioning	false
Configuration revision	2
Simulation/test	false
Entry time	18/02/2021 3:56:48.451 AM
Status number	6
Sequence number	0
Time allowed to live (ms)	32
Number of DataSet entries	2

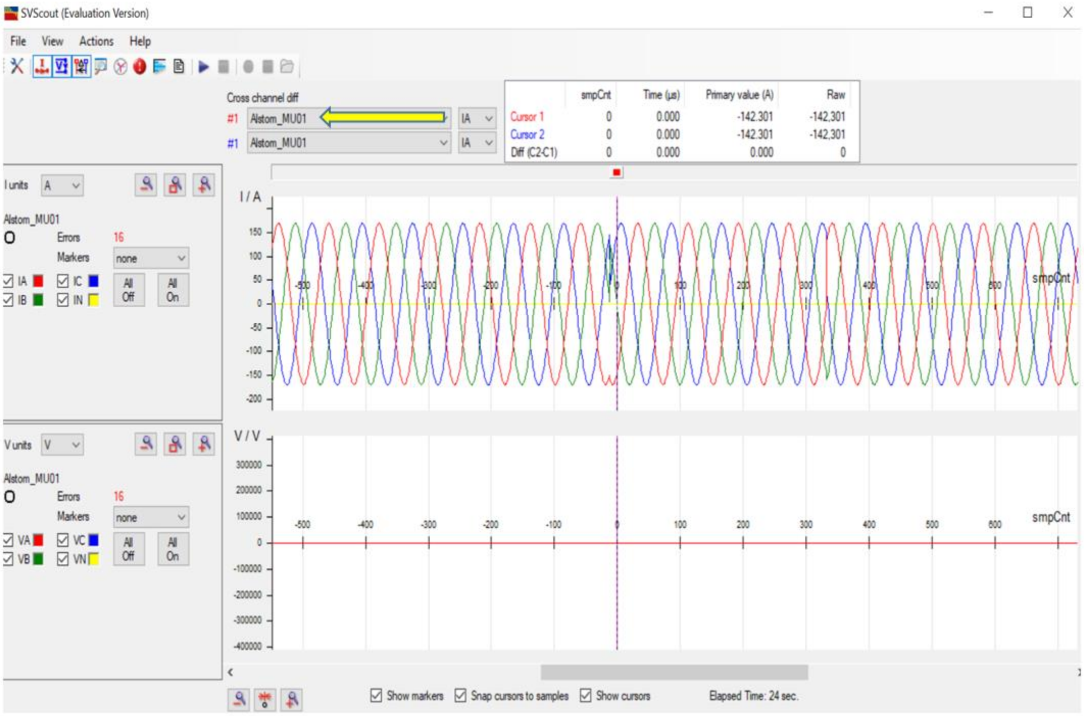
Data

Name	Value
Boolean 1	true
Bitstring 2	0000000000000

Fig. 6.9. Fault Injected into P545-M1 Exhibiting the Instantaneous Trip Condition.

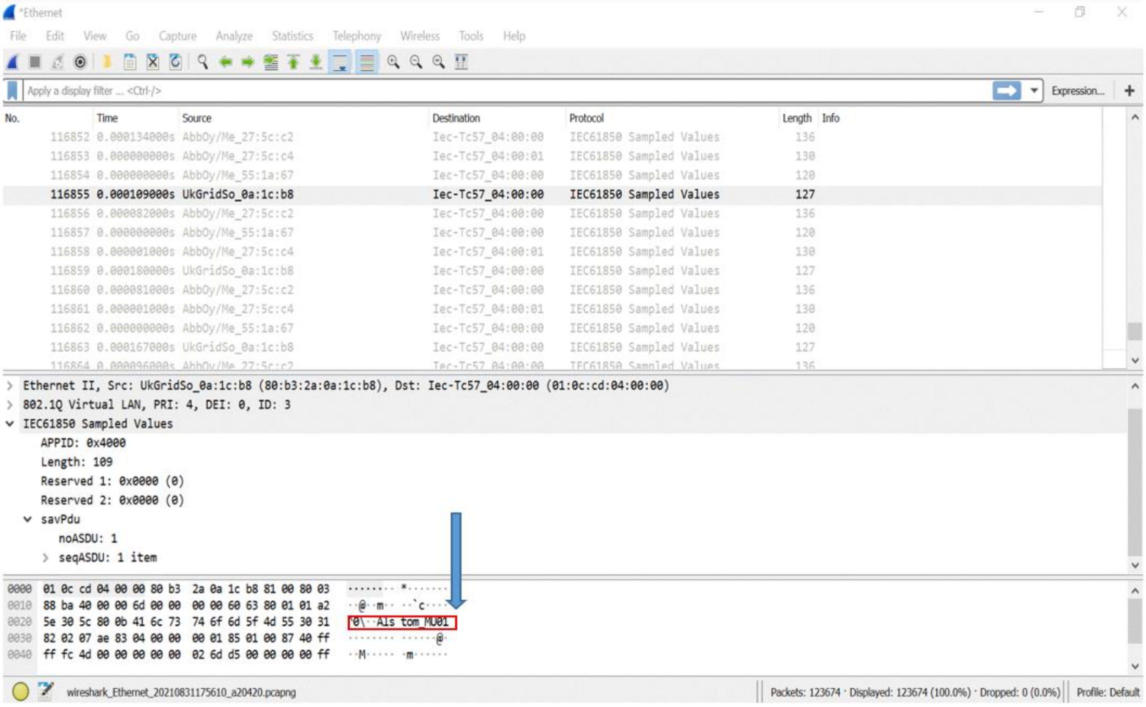
Case 1 represents the reliable operation of incomer IED and associated feeder IEDs for bus fault F1.

Fig. 6.10 and Fig. 6.11 exhibits the SV stream when there is a three-phase current from secondary injection kit to the MU. The screen shot also exhibits Alstom MU technical key in SV Scout and Wireshark tool respectively.



	smpCnt	Time (µs)	Primary value (A)	Raw
Cursor 1	0	0.000	-142.301	-142,301
Cursor 2	0	0.000	-142.301	-142,301
Diff (C2-C1)	0	0.000	0.000	0

Fig. 6.10. SV Streams Out of ALSTOM MU.

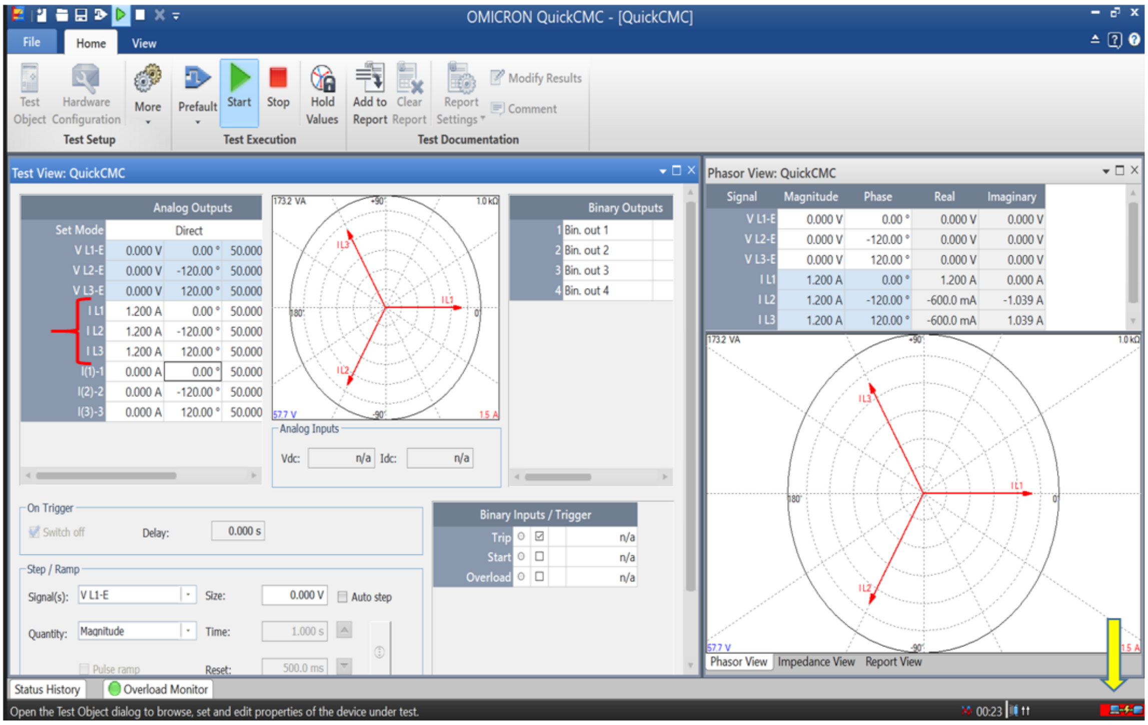

*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...

```
No.       Time         Source              Destination          Protocol                  Length  Info
  116852 0.000134000s AbbOy/Me_27:5c:c2   Iec-Tc57_04:00:00    IEC61850 Sampled Values   136
  116853 0.000000000s AbbOy/Me_27:5c:c4   Iec-Tc57_04:00:01    IEC61850 Sampled Values   130
  116854 0.000000000s AbbOy/Me_55:1a:67   Iec-Tc57_04:00:00    IEC61850 Sampled Values   120
  116855 0.000109000s UkGridSo_0a:1c:b8   Iec-Tc57_04:00:00    IEC61850 Sampled Values   127
  116856 0.000082000s AbbOy/Me_27:5c:c2   Iec-Tc57_04:00:00    IEC61850 Sampled Values   136
  116857 0.000000000s AbbOy/Me_55:1a:67   Iec-Tc57_04:00:00    IEC61850 Sampled Values   120
  116858 0.000001000s AbbOy/Me_27:5c:c4   Iec-Tc57_04:00:01    IEC61850 Sampled Values   130
  116859 0.000180000s UkGridSo_0a:1c:b8   Iec-Tc57_04:00:00    IEC61850 Sampled Values   127
  116860 0.000081000s AbbOy/Me_27:5c:c2   Iec-Tc57_04:00:00    IEC61850 Sampled Values   136
  116861 0.000001000s AbbOy/Me_27:5c:c4   Iec-Tc57_04:00:01    IEC61850 Sampled Values   130
  116862 0.000000000s AbbOy/Me_55:1a:67   Iec-Tc57_04:00:00    IEC61850 Sampled Values   120
  116863 0.000167000s UkGridSo_0a:1c:b8   Iec-Tc57_04:00:00    IEC61850 Sampled Values   127
  116864 0.000096000s AbbOy/Me_27:5c:c2   Iec-Tc57_04:00:00    IEC61850 Sampled Values   136

> Ethernet II, Src: UkGridSo_0a:1c:b8 (80:b3:2a:0a:1c:b8), Dst: Iec-Tc57_04:00:00 (01:0c:cd:04:00:00)
> 802.1Q Virtual LAN, PRI: 4, DEI: 0, ID: 3
v IEC61850 Sampled Values
    APPID: 0x4000
    Length: 109
    Reserved 1: 0x0000 (0)
    Reserved 2: 0x0000 (0)
  v savPdu
      noASDU: 1
    > seqASDU: 1 item

0000  01 0c cd 04 00 00 80 b3  2a 0a 1c b8 81 00 80 03   ········ *·······
0010  88 ba 40 00 00 6d 00 00  00 00 60 63 80 01 01 a2   ··@··m·· ··`c····
0020  5e 30 5c 80 0b 41 6c 73  74 6f 6d 5f 4d 55 30 31   ^0\··Als tom_MU01
0030  82 02 07 ae 83 04 00 00  00 01 85 01 00 87 40 ff   ········ ······@·
0040  ff fc 4d 00 00 00 00 00  02 6d d5 00 00 00 00 ff   ··M····· ·m······
```

wireshark_Ethernet_20210831175610_a20420.pcapng | Packets: 123674 · Displayed: 123674 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

Fig. 6.11. Wireshark Tool Exhibiting the SV Frame Flow Into P545-M1 Via Alstom MU.

Fig. 6.12 exhibits the injection carried out using the Test universe tool by CMC 356 tripping the P545-M1 at 1.2 A crossing the threshold at 1.1. The yellow arrow in the Fig 6.12 exhibits the linkage of the test equipment with the experiment.



Test View: QuickCMC

Analog Outputs			
Set Mode	Direct		
V L1-E	0.000 V	0.00 °	50.000
V L2-E	0.000 V	-120.00 °	50.000
V L3-E	0.000 V	120.00 °	50.000
I L1	1.200 A	0.00 °	50.000
I L2	1.200 A	-120.00 °	50.000
I L3	1.200 A	120.00 °	50.000
I(1)-1	0.000 A	0.00 °	50.000
I(2)-2	0.000 A	-120.00 °	50.000
I(3)-3	0.000 A	120.00 °	50.000

Binary Outputs	
1	Bin. out 1
2	Bin. out 2
3	Bin. out 3
4	Bin. out 4

Analog Inputs

Vdc: n/a Idc: n/a

On Trigger

☑ Switch off Delay: 0.000 s

Step / Ramp

Signal(s): V L1-E Size: 0.000 V □ Auto step

Quantity: Magnitude Time: 1.000 s

□ Pulse ramp Reset: 500.0 ms

Binary Inputs / Trigger			
Trip	○	☑	n/a
Start	○	□	n/a
Overload	○	□	n/a

Phasor View: QuickCMC

Signal	Magnitude	Phase	Real	Imaginary
V L1-E	0.000 V	0.00 °	0.000 V	0.000 V
V L2-E	0.000 V	-120.00 °	0.000 V	0.000 V
V L3-E	0.000 V	120.00 °	0.000 V	0.000 V
I L1	1.200 A	0.00 °	1.200 A	0.000 A
I L2	1.200 A	-120.00 °	-600.0 mA	-1.039 A
I L3	1.200 A	120.00 °	-600.0 mA	1.039 A

Open the Test Object dialog to browse, set and edit properties of the device under test.

Fig. 6.12. Injection Using CMC-356 Into ALSTOM MU.

Fig. 6.13 exhibits the sequence of events in a logic diagram during a fault event in the bus section of an HV switchboard that leads to the operation of incomer IED P-545M1. It also shows the status of three feeder IEDs at the inception of fault. The delay of 4 ms is kept deliberately between incomer IED and feeder IED to provide backup protection by the feeder IEDs plus 50 ms of circuit breaker opening time to isolate itself from the fault.

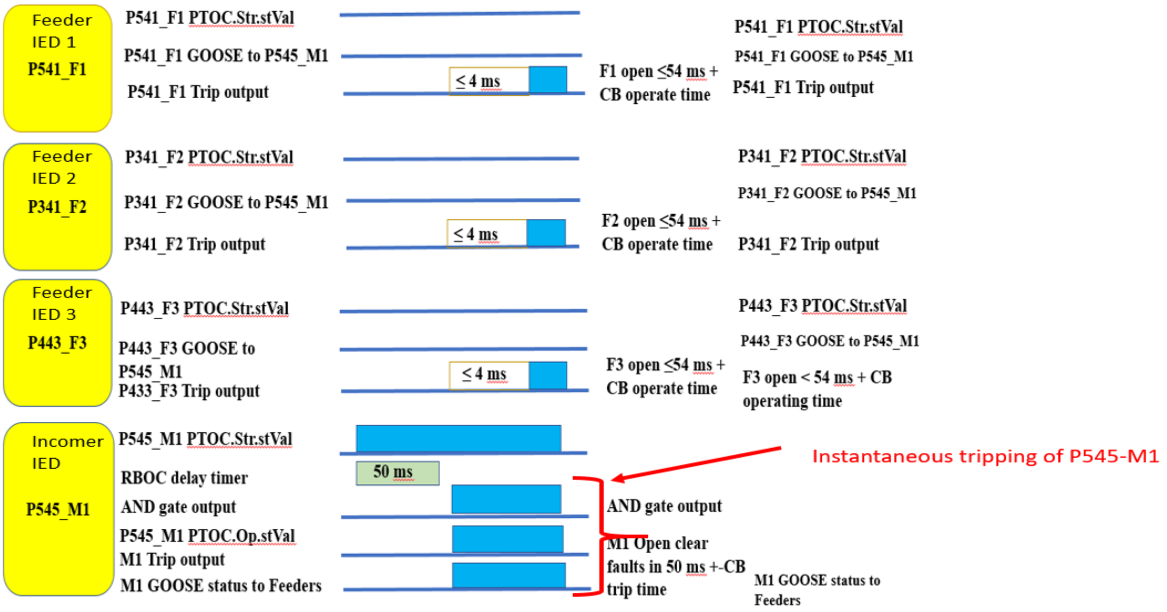
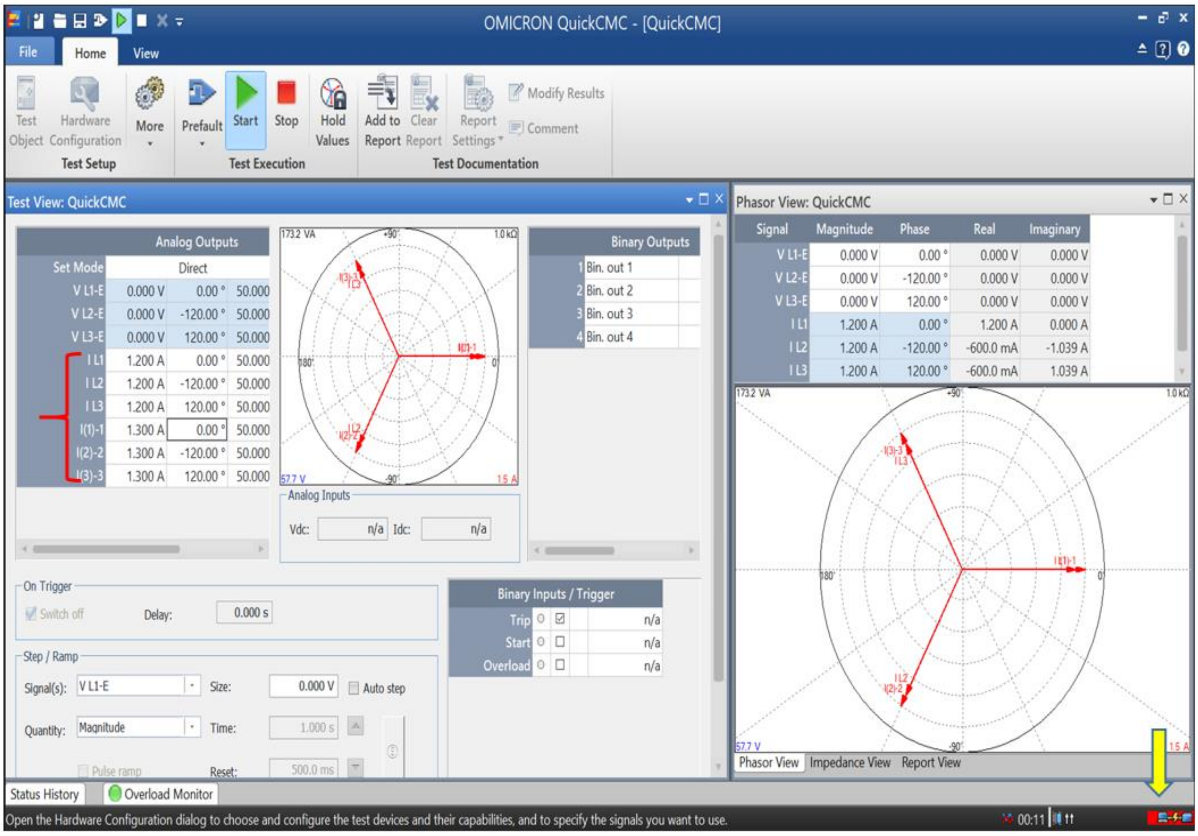


Fig. 6.13. Case 1: Status of Incomer and Feeder IED at the Inception of Fault.

Case 2: When there is an external feeder fault (Fault F2)

A simulation of a feeder fault was carried out on the feeder protected by IED P341 using CMC-356 secondary injection. In this case 2 scenario, a fault in feeder protected by P341 activated its trip element while blocking the incomer IED P545-M1. Although both IEDs i.e., feeder and incomer started operating at the same time, but the logic of P341 guarded P-545-M1 from operating instantaneously. The outgoing feeder protection IED P341-F2 blocked the incomer IED for 8 ms before allowing P545-M1 to trip; similar to having a backup protection.

Using the laptop equipped with a Test universe tool from Omicron CMC 356, a fault was injected at 1.3A at incomer IED P545-M1 and 1.2A feeder IED P341-F2 at the same time using secondary injection kit's two channels as shown in Fig. 6.14. Upon exceeding the nominal current of the IED i.e., 1.1 A, the start element of the feeder IED P341-M1 operated. The program logic of IEDs was set such that P341-M1 operated instantaneously and P541-M1 operated after a 4 ms delay. These logic gateways were programmed using Schneider's Easergy tool.



Analog Outputs			
Set Mode	Direct		
V L1-E	0.000 V	0.00 °	50.000
V L2-E	0.000 V	-120.00 °	50.000
V L3-E	0.000 V	120.00 °	50.000
I L1	1.200 A	0.00 °	50.000
I L2	1.200 A	-120.00 °	50.000
I L3	1.200 A	120.00 °	50.000
I(1)-1	1.300 A	0.00 °	50.000
I(2)-2	1.300 A	-120.00 °	50.000
I(3)-3	1.300 A	120.00 °	50.000

Binary Outputs	
1	Bin. out 1
2	Bin. out 2
3	Bin. out 3
4	Bin. out 4

Analog Inputs

Vdc: n/a Idc: n/a

On Trigger

☑ Switch off Delay: 0.000 s

Binary Inputs / Trigger			
Trip	○	☑	n/a
Start	○	□	n/a
Overload	○	□	n/a

Step / Ramp

Signal(s): V L1-E Size: 0.000 V □ Auto step

Quantity: Magnitude Time: 1.000 s

□ Pulse ramp Reset: 500.0 ms

Signal	Magnitude	Phase	Real	Imaginary
V L1-E	0.000 V	0.00 °	0.000 V	0.000 V
V L2-E	0.000 V	-120.00 °	0.000 V	0.000 V
V L3-E	0.000 V	120.00 °	0.000 V	0.000 V
I L1	1.200 A	0.00 °	1.200 A	0.000 A
I L2	1.200 A	-120.00 °	-600.0 mA	-1.039 A
I L3	1.200 A	120.00 °	-600.0 mA	1.039 A

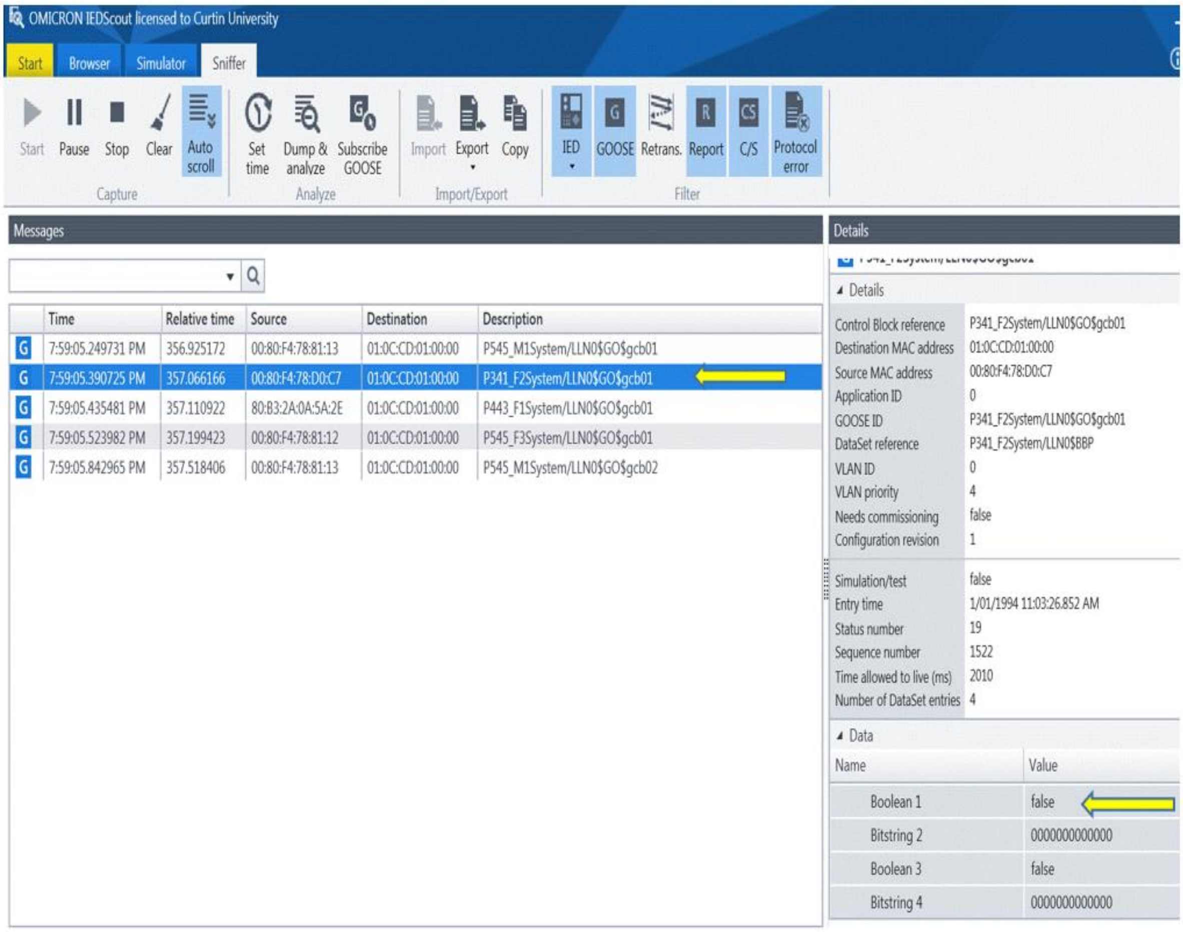
Status History

Overload Monitor

Open the Hardware Configuration dialog to choose and configure the test devices and their capabilities, and to specify the signals you want to use.

Fig. 6.14. Injection of Fault Current into IEDs P341 and P545-M1 using Omicronenergy Test Universe Tool and CMC-356.

The logic allowed a delay of 4 ms for P545-M1 having standard inverse characteristics. Once the blocked incomer IED tripped, i.e., P545-M1, it also took out from the circuit the other two feeder IEDs, i.e., P443 and P543-M2 instantaneously. These conditions have been exhibited indicating the use of GOOSE messages captured by using IED scout tool. The status of the IED P341 before and after the inception fault F2 is shown in Fig. 6.15 and Fig. 6.16. The discovery of other incoming and feeder IEDs in the network was determined by IED Scout, as seen in the screen shots. The status being "False" indicates pre-fault status and "True" indicates the fault has occurred and the IED has tripped on fault.



	Time	Relative time	Source	Destination	Description
G	7:59:05.249731 PM	356.925172	00:80:F4:78:81:13	01:0C:CD:01:00:00	P545_M1System/LLN0$GO$gcb01
G	7:59:05.390725 PM	357.066166	00:80:F4:78:D0:C7	01:0C:CD:01:00:00	P341_F2System/LLN0$GO$gcb01
G	7:59:05.435481 PM	357.110922	80:B3:2A:0A:5A:2E	01:0C:CD:01:00:00	P443_F1System/LLN0$GO$gcb01
G	7:59:05.523982 PM	357.199423	00:80:F4:78:81:12	01:0C:CD:01:00:00	P545_F3System/LLN0$GO$gcb01
G	7:59:05.842965 PM	357.518406	00:80:F4:78:81:13	01:0C:CD:01:00:00	P545_M1System/LLN0$GO$gcb02

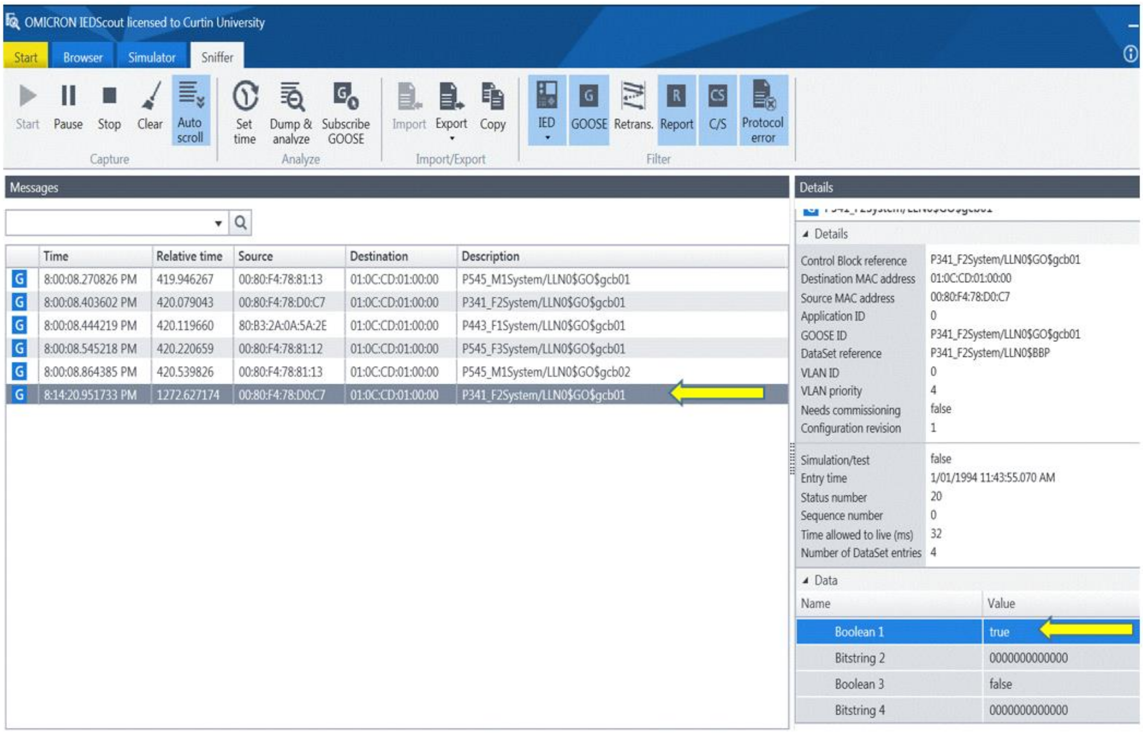
Details

Control Block reference	P341_F2System/LLN0$GO$gcb01
Destination MAC address	01:0C:CD:01:00:00
Source MAC address	00:80:F4:78:D0:C7
Application ID	0
GOOSE ID	P341_F2System/LLN0$GO$gcb01
DataSet reference	P341_F2System/LLN0$BBP
VLAN ID	0
VLAN priority	4
Needs commissioning	false
Configuration revision	1
Simulation/test	false
Entry time	1/01/1994 11:03:26.852 AM
Status number	19
Sequence number	1522
Time allowed to live (ms)	2010
Number of DataSet entries	4

Data

Name	Value
Boolean 1	false
Bitstring 2	0000000000000
Boolean 3	false
Bitstring 4	0000000000000

Fig. 6.15. Status of the IED P341 Prior to the Occurrence of the Fault.



	Time	Relative time	Source	Destination	Description
G	8:00:08.270826 PM	419.946267	00:80:F4:78:81:13	01:0C:CD:01:00:00	P545_M1System/LLN0$GO$gcb01
G	8:00:08.403602 PM	420.079043	00:80:F4:78:D0:C7	01:0C:CD:01:00:00	P341_F2System/LLN0$GO$gcb01
G	8:00:08.444219 PM	420.119660	80:B3:2A:0A:5A:2E	01:0C:CD:01:00:00	P443_F1System/LLN0$GO$gcb01
G	8:00:08.545218 PM	420.220659	00:80:F4:78:81:12	01:0C:CD:01:00:00	P545_F3System/LLN0$GO$gcb01
G	8:00:08.864385 PM	420.539826	00:80:F4:78:81:13	01:0C:CD:01:00:00	P545_M1System/LLN0$GO$gcb02
G	8:14:20.951733 PM	1272.627174	00:80:F4:78:D0:C7	01:0C:CD:01:00:00	P341_F2System/LLN0$GO$gcb01

Details

Control Block reference	P341_F2System/LLN0$GO$gcb01
Destination MAC address	01:0C:CD:01:00:00
Source MAC address	00:80:F4:78:D0:C7
Application ID	0
GOOSE ID	P341_F2System/LLN0$GO$gcb01
DataSet reference	P341_F2System/LLN0$BBP
VLAN ID	0
VLAN priority	4
Needs commissioning	false
Configuration revision	1
Simulation/test	false
Entry time	1/01/1994 11:43:55.070 AM
Status number	20
Sequence number	0
Time allowed to live (ms)	32
Number of DataSet entries	4

Data

Name	Value
Boolean 1	true
Bitstring 2	0000000000000
Boolean 3	false
Bitstring 4	0000000000000

Fig. 6.16. Status Of P341 For Case 2 Scenario When the Nominal Threshold Value Is Exceeded.

The logic inbuilt in P341 is shown in Fig. 6.17 including blocking of P545-M1 when P341 trip element is getting latched as well as the status of other feeder IEDs. This was configured using Schneider's Easergy tool and uploaded to IED P341.

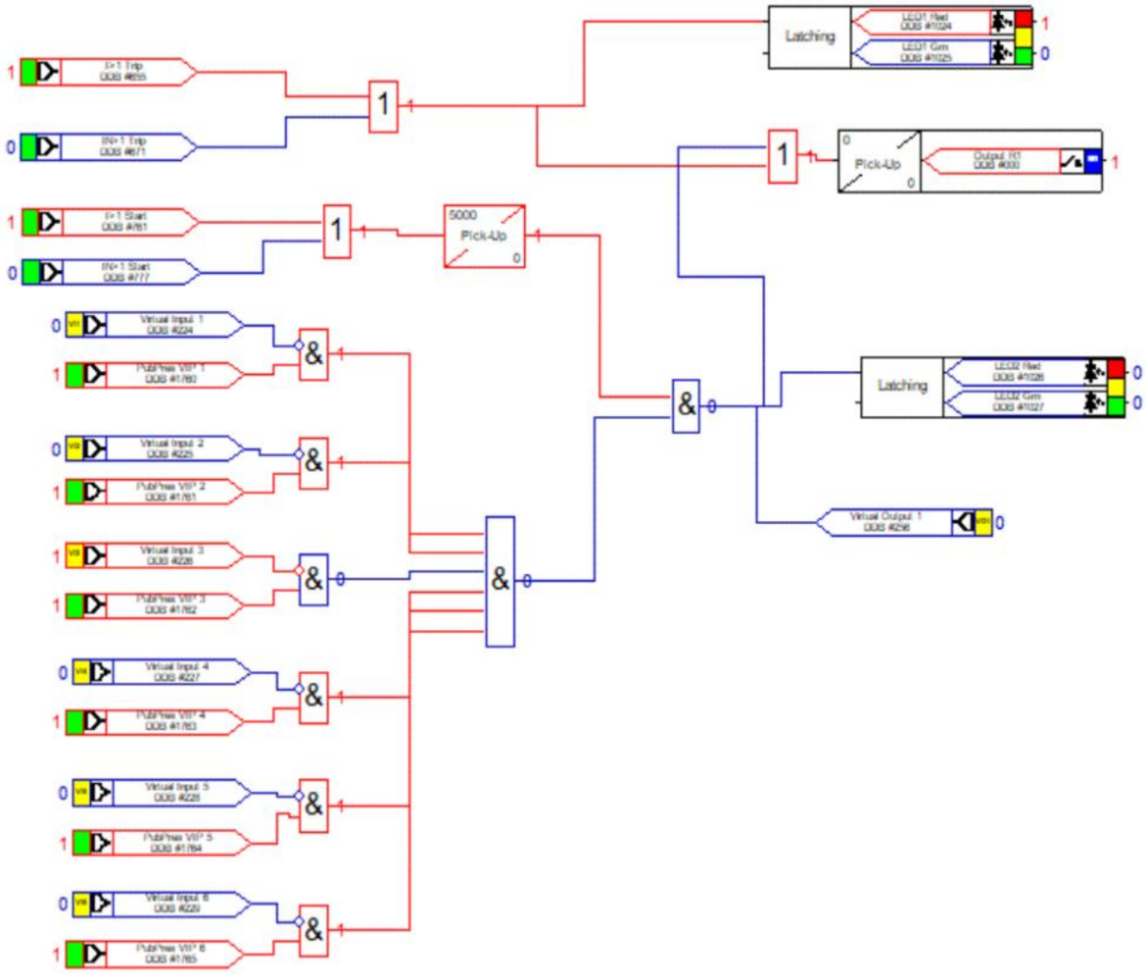


Fig. 6.17. Easergy Tool To Build A Block Logic In P341 And P545-M1.

It is observed that there are sometimes when the protection scheme enumerated above could have a risk due to disconnection of the FO wire or failure of any of the LAN switches or mal-operation of MU or IED from SAS network. This can be negated by inserting RSTP compatible IEDs for self-healing and these IEDs could provide redundancy to the SAS network by Ethernet or FO connection. The healing process and restoration could be achieved by a reverse block overcurrent protection (RBOC) scheme in the busbar with a logic programmed with its file uploaded into the IED as shown in Fig. 6.18.

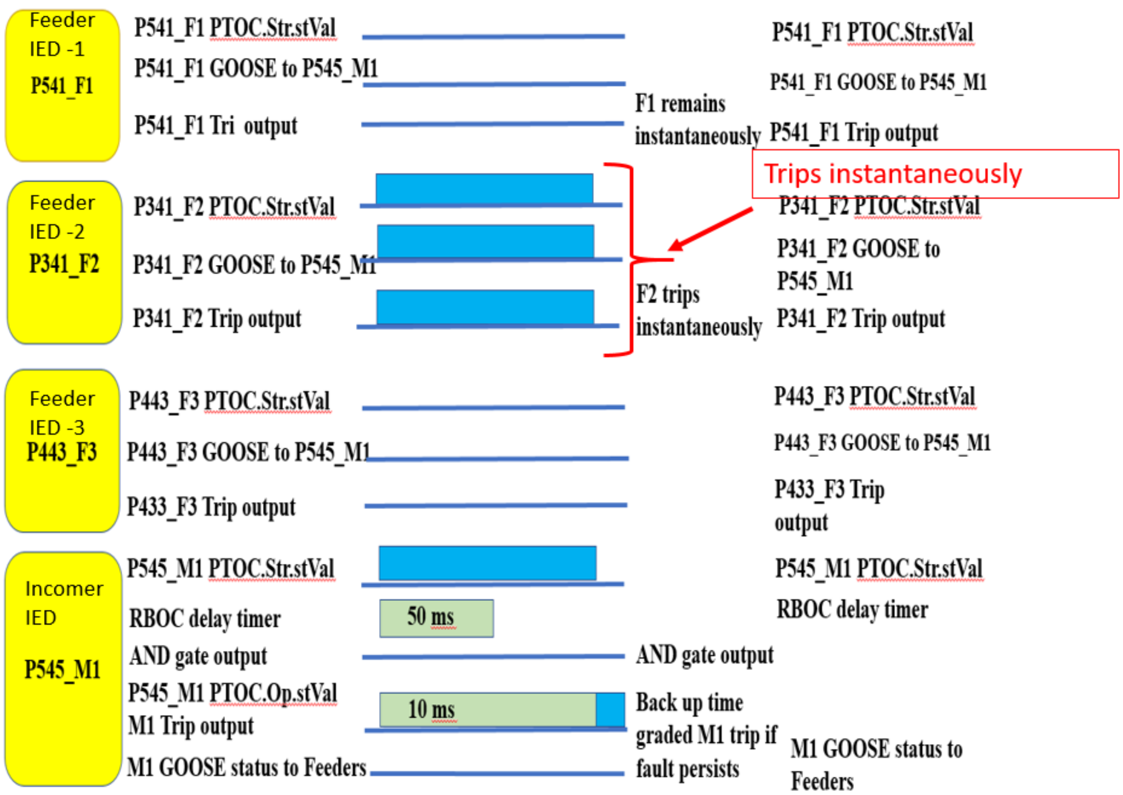


Fig. 6.18. Sequence Of Events Following Operation of P 341-F2 Start Element For A Feeder Fault (Scenario 2).

An SV and GOOSE based protection, based on IEC 62439-3 as enumerated in chapter 4, is preferred as redundancy in the SAS topology could be achieved along with digital protection. Hybrid topology involving PRP-HSR and RSTP networks could provide better redundancy and reliability, but this is a work in the future and not in the scope of this research.

Case 3: External feeder fault condition

In this case study scenario, where Ethernet or FO wire connecting the IED to switch inadvertently is disconnected or breaks during a maintenance mishandling, it could have detrimental effect on the protection scheme and associated primary plants. In such a case, it is desirable that the IED affected remains stable and selfheals. The logic built within the IED P341 guards against discontinuation or link failure and prevents spurious tripping due to an unwanted condition. Fig. 6.20 shown in a previous section has a “publisher present” signal and “ANDed” with blocking signals that prevent IEDs from operate instantaneously as this is not a fault condition in the HV switchboard.

To simulate this scenario, an Ethernet wire was disconnected from the switch and secondary injection was carried out at 1.2A to P545-M1. The IED tripped as the busbar fault was cleared by I>1 element after 10 sec. This proved the reliability in the SAS and stability of the scheme in the event of inadvertent disconnection of Ethernet or FO wires.

6.3.2 Testing of Arc Flash on a HV switchboard using GOOSE

Arc flash is a serious phenomenon that could lead to catastrophic failure of non-Arc Contained HV switchboards causing a safety hazard for the operator. It is imperative from statutory and regulatory perspectives to get such an HV switchboard tested [17].

Conventional relays which coordinate between HV incomer and Feeder IEDs based on inverse definite minimum time (IDMT) characteristics are slower to clear AC and DC arc flash faults as compared to digital IEDs which work on GOOSE based protection. Conventional protection sufferers from having "blind spots" within the bus protection which, having not been protected, leading to switchboard failure. The advantage of the GOOSE method of protection over the conventional method can't be overemphasised are multi-fold, such as reduction in wire, flexibility in communication amongst IEDs, speed of operation. All these could lead to substantial cost savings for the maintenance team [18].

Fig. 6.19 exhibits different zones of protection of an HV switchboard. The concept is similar to conventional protection by overlapping the bus bar, incomer and feeder zones. At Curtin University three scenarios were enacted with scenario 1 – fault occurring at bus – and scenario 2 – fault occurring at the outgoing side on cable and scenario 3 – fault occurring between bus and the feeder HV CB. Omicronenergy's CMC-356 secondary injection has the ability to produce a flash similar to real Arc Flashlight and all the IEDs in use at the laboratory have Overcurrent element, GOOSE based protection worked out well in preventing arc flash occurrence. These GOOSE frames are sensitive in operation and sent status, control and measurement to IEDs that coordinate amongst each other and trip it accordingly. In the program logic of IEDs, GOOSE frames can be blocked during any maintenance operation of the HV CB. This allows flexibility to the operator during protection testing related work [19].

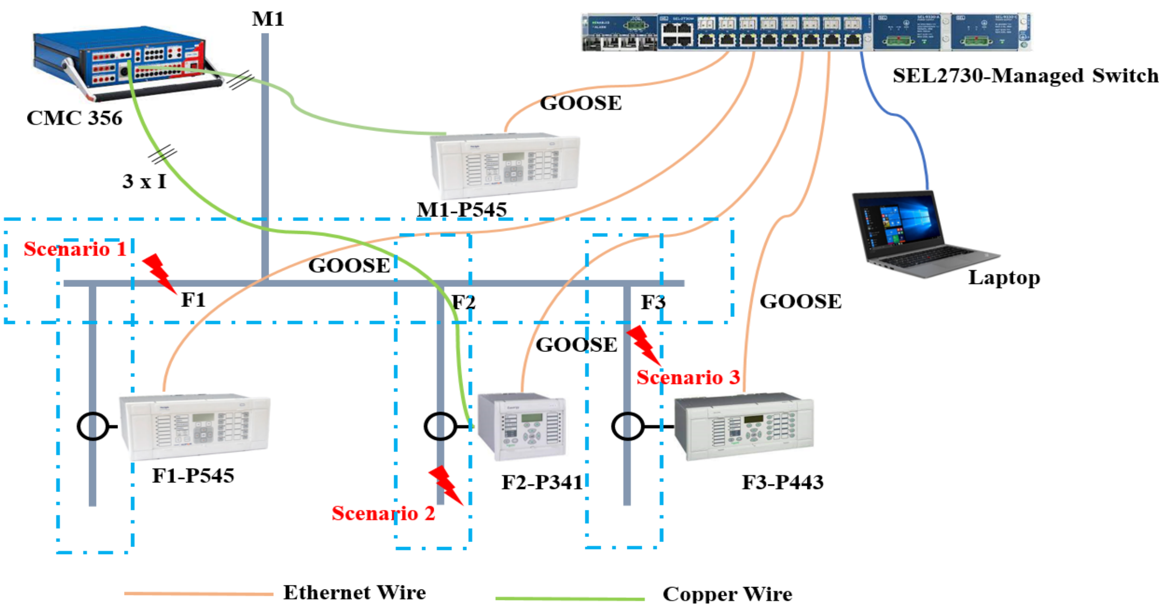


Fig. 6.19. Arc Flash Protection of Incomer and Feeder using IEDs.

Table 6.5. Tabulating the 3 Scenarios of Arc Flash Event.

	Sensors pick up time (ms)	IED pick up time by GOOSE burst (ms)
Scenario 1: Arc Flash at Bus (F1)	0.8	3.3
Scenario 2: Arc Flash at the feeder (F2)	1.3	3.7
Scenario 2: Arc Flash at the feeder (F3)	1.1	3.5

Table 6.5 exhibits that arc flash based IEDs have the ability to operate <5 ms and this is huge improvement as opposed to conventional arc fault relays which operate in 10 ms or more (plus the CB opening time of 50 ms).

6.4 RESULTS AND DISCUSSION

Simulation using GOOSE and SV methodology of tripping the incomer and feeders were 5~10 ms faster than conventional hard-wired relays in various scenarios:

In Scenario 1, a bus bar fault could pose safety issues to non-arc contained switchboards in the network in the event of an arc flash event within the bus. Digital protection using GOOSE and SV have faster tripping ability which could react to such faults in 50~54 ms as opposed to 60-70 ms in a conventional method.

In Scenario 2, the experiment exhibited that the trip occurring due to feeder fault using IEDs were adequate to maintain self-healing process during a feeder fault in the network. In the event of a feeder fault, GOOSE blocking signals published by IED P341-F2 delayed the trip of the incomer and blocked P545-M1 from operating instantaneously. It kept other feeders up and running while clearing its fault. When the fault persisted for 10 ms the incomer protection IED operated after 8 ms.

In Scenario 3, the accidental disconnection provides stability to the network by tripping after 10 secs and not instantaneously losing a healthy feeder.

The above experiments of a digital bus protection system validate the robustness of BBP which is cost-effective and easy to implement in a Process plant scenario using multi-vendor equipment. The proposed practical simulations were tested in a laboratory set-up and it was proven that tripping and blocking of IEDs leveraging on SV and GOOSE frames was beneficial.

This digital bus bar proved:

1) faster tripping time using IEDs than relays
2) ease of interpreting, analysing, and filtering time of IEDs due to substantial reduction in processing time as most devices had smart computing and processing time
3) ease of handling GOOSE and SV frames which continuously are monitored with reduced termination and nodes
4) reduced delay time due to fast-acting characteristics of GOOSE and SV as these frames travel over FO wires
5) protection of blind spots within the bus, which is not easy to detect in a conventional system
6) identification and protecting a blind spot feeder as shown in Fig. 6.21; blind spot zone is a grey area which is not covered by differential protection or feeder protection, and this is detected and protected in the digital BBP scheme better than conventional schemes.

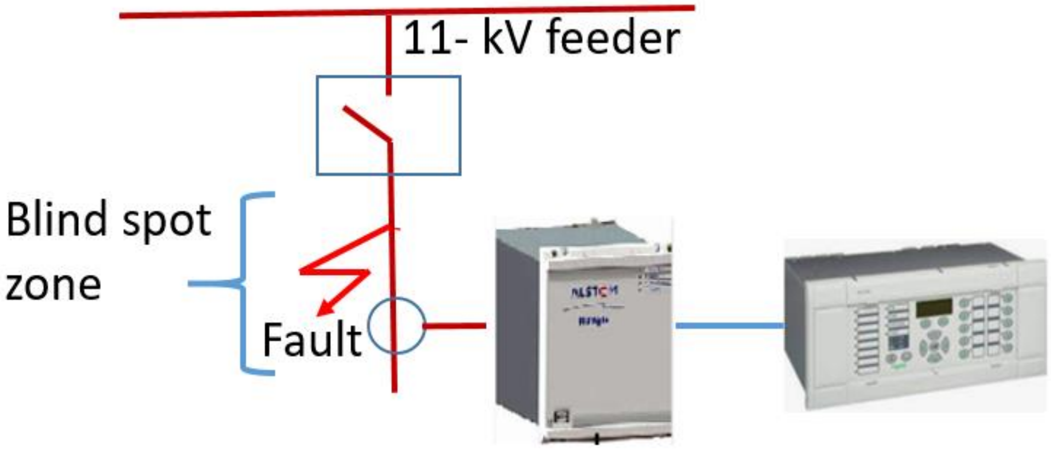


Fig. 6.20. Blind Spot Not Covered By Other Conventional Protection.

In another series of tests carried out relating to arc flash on the mentioned HV switchboard, the GOOSE method of testing performed better than the conventional methos of arc fault protection. The only disadvantage of this method of testing could be attributed to star network topology wherein all devices have been connected to one switch. Failure of this node could result in complete loss of arc fault and other associated protection. This could be periodic monitoring of GOOSE message by a device such as GOOSE manager. Table 6.6 summarises GOOSE form of arc flash protection versus conventional forms of protection6.

Table 6.6. Comparison Between a Conventional and IED Based Arc Flash Protection System.

	Conventional mode of Arc Flash Protection of a non-Arc Contained HV Switchboard	Digital Mode of Arc Flash protection of a non-Arc contained HV Switchboard
Selectivity	Average	High
Speed of operation	Slow	Very Fast
Reliability	Average	High
Complexity	More complex	Ease of operation
Security	Not entirely secured	Cyber threats exist
Cost	High	Low
Flexibility	May not be possible	Highly flexible
Maintenance and Testing	Periodic maintenance required	Condition monitoring of GOOSE shall give peace of mid

6.5 CHAPTER SUMMARY

The Process bus technology enumerated in IEC 61850-9-2LE guideline promises to have an interesting future in a digital substation paradigm. However, its performance with respect to protection needs to be validated prior to its large-scale deployment in the industry. This chapter details that experimenting in a laboratory set-up of a simple BBP in a mining substation using SV and GOOSE reinforces the need to go for digital system. The reason to progress these smart technologies are the benefits of faster communication, reduced wiring, and continuous condition monitoring of the pulses of IEDs.

Adding credentials to support digital SAS is the fact that digital protection of a BBP scheme is easily configurable and possesses the advantage of being extendable when the switchboard expands to accommodate further incomers and feeders. These schemes provide high speed operations and have lesser diagnostic efforts. It is recommended to have many more such schemes implemented by the resources industry.

Also, a highlight of this chapter has been the issue around arc flash protection in non-arc contained HV switchboards. The laboratory experimental results show the advantages of GOOSE based arc flash protection which the industry is expected to design and implement shortly; this could limit the incident energy.

6.6 REFERENCES

[1] T. S. Sidhu and Y. Yin, “Modelling and simulation performance evaluation of IEC 61850 based substation communication system”, *IEEE Trans. on Power Del.,* vol. 22, no. 3, 2007.

[2] M. G. Kanabar and T. S. Sidhu, “Performance of IEC 61850-9-2 Process bus and Corrective measure of digital relaying.” *IEEE Trans. on Power Del.,* vol. 26, no. 2, 2007.

[3] P. Schaub, J. Haywood, D. Ingram, A. Kenwrick, and G. Dusha, “Test and Evaluation of Non-Conventional Instrument Transformers and Sampled Value Process bus on PowerLink’s Transmission network*”, Cigre Panel B5*, SEAPAC 2011, Sydney, Australia.

[4] P. Crossley, L. Yang, A. Wen, R. Chatfield, M. Redfern and X. Sun, "Design and performance evaluation for a protection system utilising IEC 61850-9-2 process

bus," *2011 International Conference on Advanced Power System Automation and Protection,* Beijing, China, 2011, pp. 534-538, doi: 10.1109/APAP.2011.6180459.

[5] A.H. Ranta, O. Rintamaki, J Starck, “Utilizing Possibilities of IEC 61850 and GOOSE”, in the proc of 20th International Conference of on Electricity Distribution, Cired, Prague June 2009.

[6] S. Kumar, N. Das, S. Islam and A. Abu-Siada, "Toward a Substation Automation System Based on IEC," *2021*. Electronics 2021, 10, 310. https://doi.org/10.3390/electronics 10030310.

[7] J. Schmid and M. Schumarcher, “IEC 61850 Merging Unit for the universal connection of conventional and Non-Conventional Instrument Transformers,” Cigre, AS-306, 2008.

[8] K. Liu, X. Dong, and Z. Bo, “Current differential protection based on non-conventional instrument transformer and IEC 61850.” in proc. of the 43rd Universities Power Engineering Conference 2008 (UPEC 2008), 1~4 September 2008, Padova, Italy.

[9] IEC 61850-8-1 - Specific communication service mapping (SCSM) – Mappings to Manufacturing Message Specification MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3.

[10] X. Chen, H. Guo and P. Crossley, “Interoperability Performance Assessment of Multivendor IEC61850 Process Bus,” *IEEE Trans. on Power Del.*, vol. 31, no. 4, pp. 1934-1944, Aug. 2016, doi: 10.1109/TPWRD.2015.2509644.

[11] K. Hinkley and D. Batger, “TransGrid’s journey to a full digital substation”, SEAPAC 17-APB5, 14-15 September, Melbourne, Australia.

[12] ALSTOM cost comparison spreadsheet, Private Communications/ Consultations with Engineers, 2015.

[13] N. Das, W. Ma, and S. Islam, “Comparison study of various factors affecting end to end delay in IEC 61850 substation communication using OPNET”, in proc. of the Australasian Power Engineering Conferences 2012 (AUPEC 2012), Bali, Indonesia, 26-29 Sept. 2012.

[14] J. Schmid and M. Schumarcher, “IEC 61850 Merging Unit for the universal connection of conventional and Non-Conventional Instrument Transformers,” Cigre, AS-306, 2008.

[15] S. Kumar, A. Abu-Siada, N. Das and S. Islam, "Reverse Blocking Over Current Busbar Protection Scheme based on IEC 61850 Architecture," in *IEEE Transactions on Industry Applications*, 2022, doi: 10.1109/TIA.2022.3220727

[16] S. Kumar, N. Das, S. Islam and A. Abu-Siada, "Verification of Latency and Delays Related to a Digital Topology based on IEC 61850," *in proc. of the 2019 29th*

Australasian Universities Power Engineering Conference (AUPEC), Nadi, Fiji, Nov. 26-29, 2019. pp. 1-6, doi: 10.1109/AUPEC48547.2019.211964.

[17] S. Kumar, A. Abu-Siada, N. Das and S. Islam, "A Fast and Reliable Blocked Bus Bar Protection Scheme Leveraging on Sampled Value and GOOSE Protection based on IEC 61850 Architecture," *2021 31st Australasian Universities Power Engineering Conference (AUPEC)*, 2021, pp. 1-5, doi: 10.1109/AUPEC52110.2021.9597736.

[18] K Hinkley, C Mistry, “First Digital Substation in TransGrid – Australia: A journey, Business case, Lessons” DPSP Conference, Belfast 2016

[19] C. Cabrera, S. Chiu and N. K. C. Nair, "Implementation of Arc-Flash Protection using IEC 61850 Goose messaging," *2012 IEEE International Conference on Power System Technology (POWERCON)*, Auckland, New Zealand, 2012, pp. 1-6, doi: 10.1109/PowerCon.2012.6401467.

CHAPTER 7:

FUTURE WORKS IN SAS BASED IEC 61850 PROTOCOL

7.1 INTRODUCTION

In order for any SAS to be successful the operator should feel comfortable in operating it, and the system needs to be reliable. SAS must respond quickly to faults and isolate in the fastest possible manner without disruption of the power. Multivendor equipment need to communicate and coordinate in a reliable manner in order to obtain the best outcome. There are multivendor manufacturers who have been using proprietary protocols that make communication amongst the network switches, IEDs, Red Boxes and peripherals difficult, and hard to communicate leveraging on Profibus, Profinet, IEC 61870-5 etc. mode of communication [1]. However, the advancements in IEC 61850 protocol seem to have addressed many issues such as expandability, ease of communication, high-speed data transfer, and flexible adaptive data routing. Ease of control and communication of remote devices etc. laid down by the IEC Committee in 2002 in IEC 61850 protocol as set out in previous chapters tend provide data-oriented models which contain the whole data specification, enabling peer-to-peer communication and not master-slave communication. It provides data integrity and filters out malformed data that could compromise the SAS features while providing an integrated communication system. Many substations control systems in the modern world are still based on the SCADA system where communication with field devices is based on human control of the field devices via DNP3 or TCP/IP protocol, operating in a vertical command structure as shown in Fig. 7.1. These substations have a number of secondary cables and proprietary software embedded within the substation devices that make fault diagnostic difficult and operation a lot more difficult.

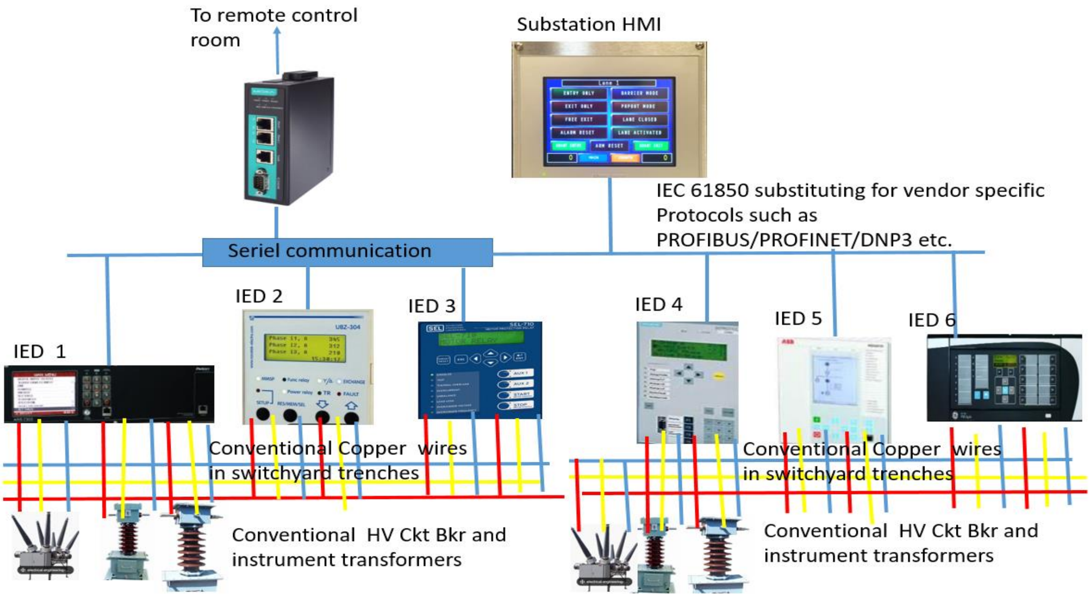

To remote control room
Substation HMI
IEC 61850 substituting for vendor specific Protocols such as PROFIBUS/PROFINET/DNP3 etc.
Seriel communication
IED 1
IED 2
IED 3
IED 4
IED 5
IED 6
Conventional Copper wires in switchyard trenches
Conventional Copper wires in switchyard trenches
Conventional HV Ckt Bkr and instrument transformers
Conventional HV Ckt Bkr and instrument transformers

Fig. 7.1. Vertical Communication Using HMI From a Control Room Based on IEC 61850.

In the future it is expected that these field devices shall have reduced number of control cables connecting the control room with the field devices, based on IEC 61850-9-2 standard, thereby reducing the project cost as the switchyard trenches shrink to conduits accommodating FO and Ethernet wires [2]. In the future, fault diagnoses shall be much easier as most of the digital frame circulating could be viewed remotely on hand-held devices. Remote operations and Inter of Things (IoT) shall guide the operational command of intelligent HV and LV circuit breakers as shown in Fig. 7.2.

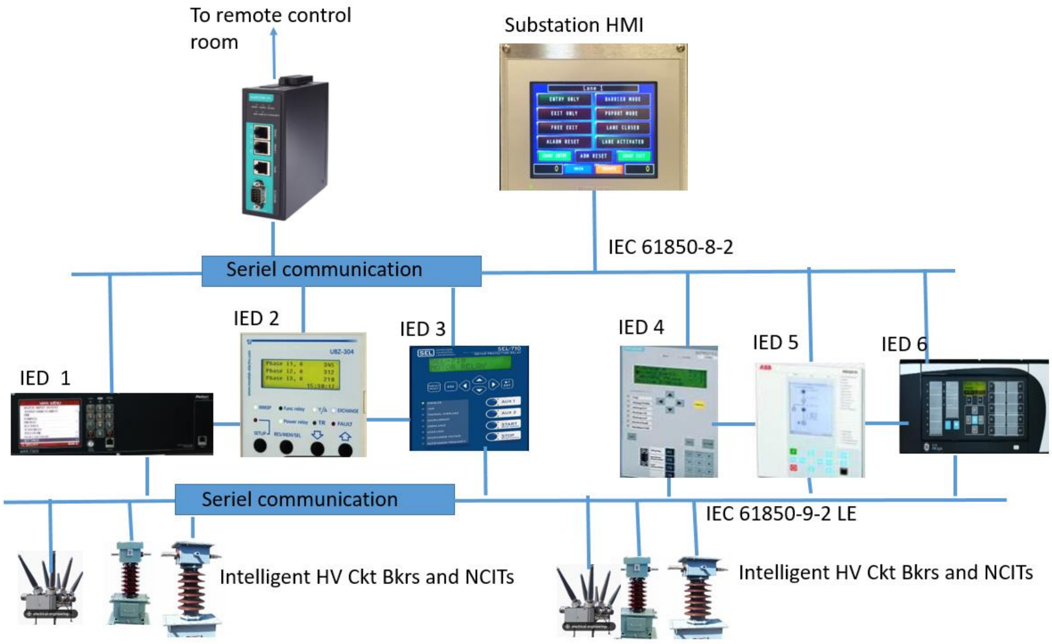


Fig. 7.2. Smart Substation of the Future With Reduced Number of Secondary Cables.

7.2 FUTURE OF SAS

In the previous section, it is mentioned that conventional system of SAS suffers from proprietary features attributed to multi-vendor products. In this section, Table 7.1 gives further details of issues that could be addressed better using IEC 61850 protocol [3].

Table 7.1. Conventional SAS versus Future SAS.

Functions of SAS	Conventional SAS	Future SAS	Remarks
Protection	√	√	Basic protection of 50/51 N / 27/ 87 (to ANSI Code) features are available in both networks
	x	√	Interoperability possible in future SAS but not in conventional relays including wireless uploading of setting files into IEDs
	x	√	Flexibility to upload and download protection files from remotely over IoT not possible in conventional networks
Control	~~√~~	√	Station and Process level control possible remotely for future SAS networks; this is partially possible in conventional IEDs
	x	√	Enhanced control function such as opening and closing HV switchgears over IoT using hand-held devices
Metering	x	√	Integration of multiple data and accumulating data for trend analysis possible in future SAS
Monitoring switchgear, isolator and earthing	x	√	Overall monitoring of the status of switchgear, isolating and earthing of the equipment from remote location is possible in future SAS
Analysis and Diagnostics	x	√	Analyse and Extract Disturbance records from network
	~~√~~	√	Automatic upload of disturbances and analysis; partially possible in conventional networks
Maintenance, Operation and Diagnostics	x	√	Condition monitoring of overall network is possible in a future smart network but not so in a conventional SAS
	X	√	Fault tolerance and self-healing after a fault occurrence is better achieved in a future SAS

As enumerated in Table 7.1 the future of a smart SAS network seems to hold a promise to better deliver power to the customers, leveraging on IEC 61850 standard as it shall reduce the operating costs of substation projects while enhancing the safety features of the network [4]. For example, protection testing that is currently being carried out needs a person to visit the substation and carry out testing on IED standing in front of non-arc contained 11-kV switchgear, exposing the person to severe risk of arc flash blast that could be triggered due to an internal short while the testing is in progress. This not so when the HV switchgear is remotely diagnosed for protection testing or analysis of a fault disturbance [5]. Future SAS shall have huge application of internet and communication technology (ICT) and, leveraging on this technology, asset management of primary plant equipment and monitoring of these critical power equipment's shall reach a new paradigm enhancing asset lifespan.

Future SAS can handle multiple substations in the network from information management, asset condition monitoring, and disturbance analysis perspectives as shown in Fig. 7.3 [6]. It offers the flexibility of retaining the existing substation network as a backup while upgrading to a newer technology based on IoT, providing a one-stop solution for the management of a network.

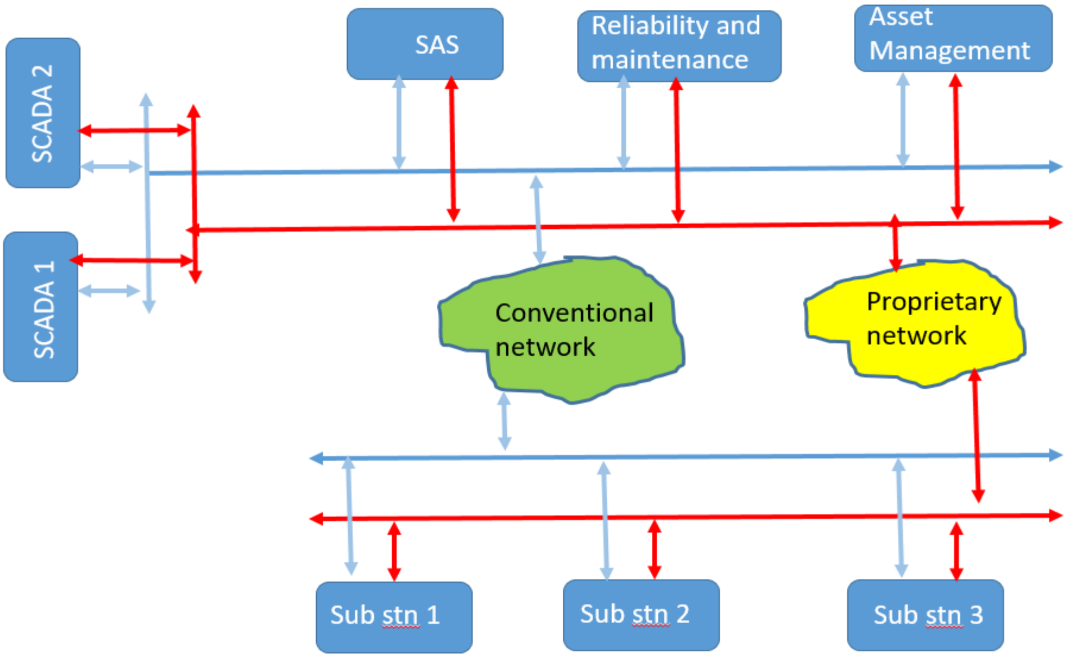


Fig. 7.3. Coexistence of Conventional and Digital Network of a Future Grid.

The SCADA systems 1 and 2 gather data from multiple substations related to protection, condition monitoring of assets, maintenance planning and management and enable the operator to take appropriate decisions [7]. To take such judicious decisions, complex algorithms have to be formulated and the parameters below (but not limited to) are considered for the operational/maintenance centre:

- loading on the fleet of transformers
- loading on transmission and distribution lines
- temperature rise on transformer during high demand
- protection settings check
- circulation of correct frames related to GOOSE and SV
- maintenance strategies for optimum asset life span.

Future SAS shall have smart equipment such as NCITs as described in Chapter 5, which use test methods developed at Curtin University to operate IEDs. These NCITs still have not gained popularity and need extensive testing from the interoperability perspective as only a very handful of vendor's manufacture these equipment specifically for their IEDs. In the absence of iron core and based on sensors/FO wires, these equipment's create a safe approach while reliably operating the IEDs, besides providing these advantages: coping with CT saturation, better frequency response and bandwidth than conventional types, superior auto-reclosing and detection of transformer internal fault isolation via smart protection [8]. The challenge for the future is upgrading the conventional equipment to adapt to future and newer technologies due to non-standardization in protocol and conventional hardwired topology. Also, it is a cumbersome process to extract data from conventional technologies as the software may need lots of restructuring, modification and upgradation of both the software and hardware platforms.

Future SAS shall have a number of hybrid topologies in tree or ring structure leveraging on IEC 62439-3 standard as enumerated in Chapter 4. These topologies shall provide protection X and Y like the conventional system would do. In a typical substation 132/11kV, PRP topology can work at 132-kV level while 11-kV could have HSR ring topology giving the best of future SAS, as shown in Fig. 7.4.

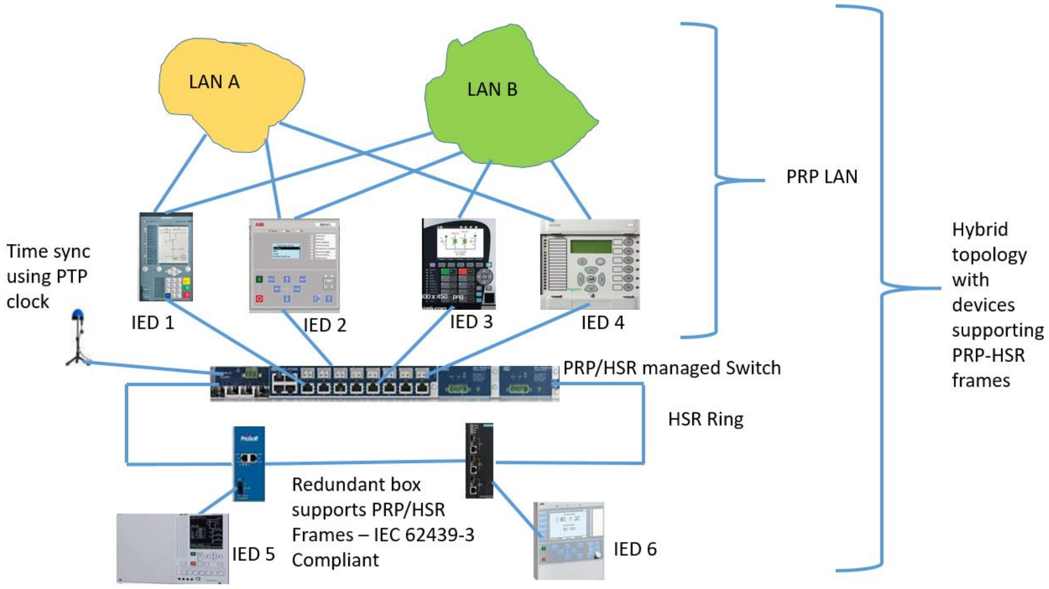

LAN A
LAN B
PRP LAN
Hybrid topology with devices supporting PRP-HSR frames
Time sync using PTP clock
IED 1
IED 2
IED 3
IED 4
PRP/HSR managed Switch
HSR Ring
Redundant box supports PRP/HSR Frames – IEC 62439-3 Compliant
IED 5
IED 6

Fig. 7.4. Hybrid of PRP-HSR Topology for Future SAS

The generation of the mix-based expansion of modern power grids has propelled the application of digital infrastructures. The introduction of SAS, advanced networks and communication technologies have drastically increased the complexity of the power system, which could compromise the entire power network to hackers. The exploitation of the cyber security vulnerabilities by an attacker may result in devastating consequences and can leave millions of people in severe power outage. To resolve this issue, future work has been proposed on network models developed in OPNET (subjected to various Denial of Service (DoS) attacks) to demonstrate cyber security aspect of an IEC 61850 based digital substations. The attack scenarios can exhibit significant increases in the system delay and the prevention of messages, i.e., transmission of GOOSE and Sampled Measured Values (SMV), within an acceptable period. In addition to that, it may cause malfunction of the devices such as unresponsiveness of IEDs, which could eventually lead to catastrophic scenarios, especially under different fault conditions.

7.3 OVERCOMING CHALLENGES IN A FUTURE SAS

7.3.1 Detecting and Mitigating Cyberattacks on a Substation Network

With the number of multivendor devices and proprietary software in action it has been a challenge to upgrade or modify software’s to make them compatible. Other challenges that researchers are trying to address are related to the huge variety of applications of internet and communication technologies in IEC 61850 protocol. Internet and wireless connectivity have led to cyberattacks on SAS networks causing serious issues to infrastructure security. With advances in digital technology, cyberattack has been on the rise. Digital substation automation is vulnerable to cyberattacks and could cause massive blackouts of power system networks. As utilities constantly increases their dependency on internet and digital platforms, cyberattacks are becoming a major concern. In recent decades, smart grid networks have become more vulnerable by relying on open standard communication protocols and subsequently opening the doors to outsiders to break into network security maliciously. For instance, raw sewage was spilled out into nearby parks and rivers in Maroochy shire, Queensland by a cyberattack on the network orchestrated by a disgruntled ex-employee. This incident occurred by injecting threats to Supervisory Control and Data Acquisition (SCADA) in attacking on a sewage treatment system. This caused death to marine life, stench, and environment pollution of water.

Furthermore, a December 2016 cyberattack on the Ukrainian power grid has presented a menacing puzzle and opened up new challenges related to cybersecurity of networks. Two days before Christmas in 2015, Russian hackers planted a unique specimen of malware in the network of Ukraine’s national grid operator, Ukrenergo. Just before midnight, they used it to open every circuit breaker in a transmission station north of Kiev. The result was one of the most dramatic attacks in Russia’s neighbour Ukraine. This was an unprecedented, automated blackout across Ukraine’s capital Kiev [9]. Digitalisation of smart grids has enhanced the user experience on the controls and analytics of power system immensely but that has led to cyberattacks where the hackers try to take control of entire systems for malicious purpose. This can lead to heavy loss of state’s economy and reputation.

Although IEC 61850 communication protocol have key features related to flexibility, interoperability and especially security, this opportunity can be turned into a threat if the system is not properly secured. If security is breached, system vulnerability and threat risk could escalate. Future work needs to focus on researching what needs to be undertaken to increase cyber safety and decrease cyberattacks. IEC 61850 is an international standard communication protocol that has multiple functions such as asset management, control, monitoring automation, protection etc. but the security and efficiency of the smart grid can easily be compromised. Although many vendor devices are interoperable and platform-independent, and their software covers all the main features of the IEC 61850 standards such as MMS, GOOSE and SV communication, a particular software tool that provides a further security layer such as PIS-10 could protect the network and prevent network vulnerability of the system at process and station level. Each vulnerability provides the opportunity to cyber attackers to disrupt and use the software for malicious purpose as shown in Fig. 7.5. Further analysis shall provide a mitigation plan after the attacks.

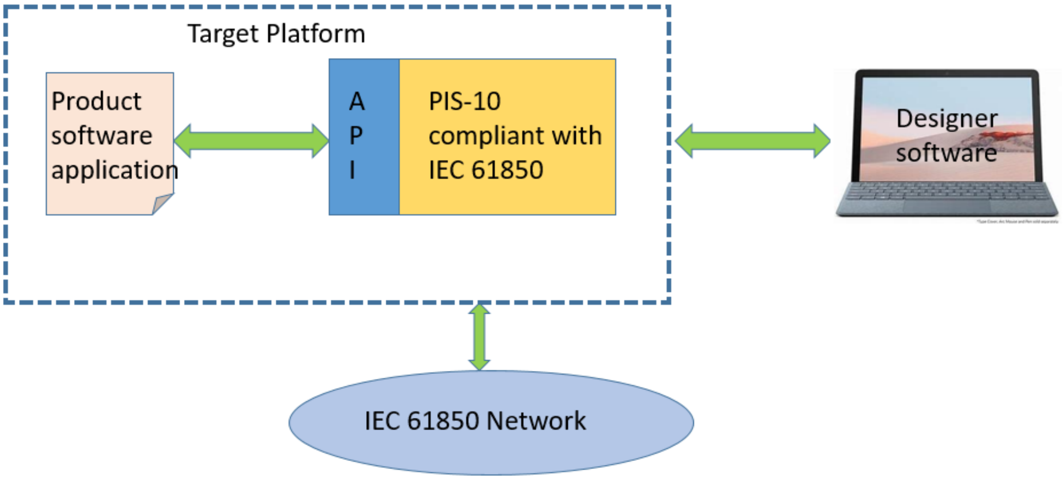


Fig. 7.5. Additional Security Layer in the Form of PIS-10 Software.

For future work, Curtin University laboratory has been equipped with 23 IEDs. These smart devices have been hard-wired connected to managed switches, and Red Boxes to form a virtual substation. Equipment has been donated by several manufacturers such as ABB, Siemens, Alstom, Schneider, SESL, Eaton, Omicron and others. This research centre could practically test a cyber-intrusion, detection and blocking system as shown in Fig. 7.6.

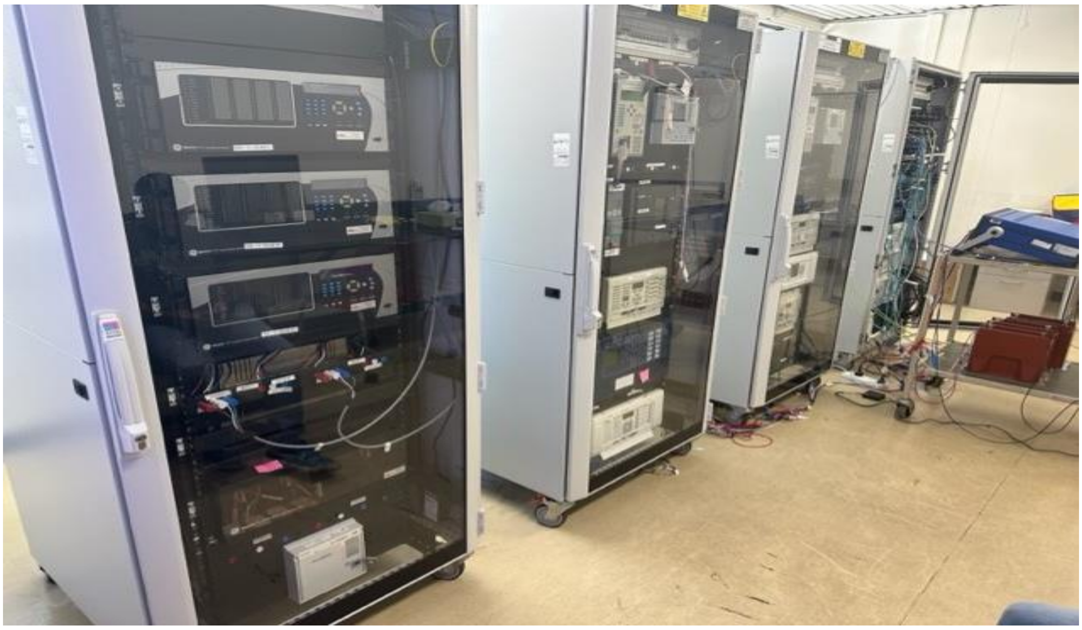


Fig. 7.6. Virtual SAS Network with Smart Technology and IEDs to Test For Cyberattack.

Analysis using a PIS-10 IEC 61850 software architecture and finding vulnerability at the key attack area is envisaged to make the smart grid more resilient to cyberattack. Future projects are intended to work on Powerfactory DigSilent, OPNET and MATLAB/Simulink software to process the network to gain understanding of the modus operandi of attacks by nefarious minds. The researcher's intention related to future project work is to increase of the quality of the samples and compare different results of the networks and models, considering previous results endorsed at an IEC Standard, Cigre or IEEE conference analysing, comparing, contrasting, and justifying the implementation of the proposed changes.

7.3.2 Condition Monitoring of Substation Assets

Condition monitoring of power equipment such as critical assets like transformers have huge advantage in being implemented without taking outages for maintenance. Although condition monitoring of transformers is not a new technology, with the advancement in technology end-of-life of this critical asset can be further enhanced. Application of IEC 61850 protocol could inform the operator of vital information on asset condition, enabling the care of transformer during a dynamic and normal event. In a modern power system with the advent of microprocessor-based digital relays, the environment becomes further challenging due to introduction of sophisticated IEDs. In such a state, coordination of information becomes more challenging due to proprietary and multi-vendor IEDs and component use.

Table 7.2 shows a typical comparison of data collected from power transformers, control rooms and field sensors using SCADA, substation automation and asset management using the latest asset management standard IEC 61850-90-3 [10].

Table 7.2. IEC 61850-90-3 Comparison.

Asset parameters	SCADA, DMS, EMS	Substation automation	Asset management
No. of points required for condition monitoring device IEDs	Small	Small to medium	Large
Type of system processing	Continuous	Continuous	Batch or continuous
Type of data acquisition	Online, realtime	On line, realtime	Deferred time series acquisition; manual entry; online; realtime
Source information	SA, IEDs, primary equipment	IEDs, primary equipment	IEDs, primary equipment, offline tests reports, SCADA, DMS , EMS, SA, Historian, ERP system

Modern IEDs must have capabilities to exchange data within the stipulated time and be free from proprietary issues as modelled by different manufacturers. The interoperability issue is one of the reasons for not having the desired confidence level in IEC 61850 based SAS. This could lead to loss of confidence amongst end users. However, GOOSE is one of the key components which enables high speed data exchange from one IED to other in less than 4 ms. It continuously publishes messages which are picked up by other IEDs subscribing to the GOOSE messages for control, alarm, and faults. Some of the messages that are required to monitor key substation equipment such as typical power transformers to make condition monitoring an effective tool for analysis:

- dissolved gases
- relative humidity
- oil temperature
- partial discharge of bushings
- direct winding resistance
- top oil temperature
- bottom oil temperature
- winding hot spots
- bushing leakage current
- bushing voltage sensors
- ambient temperature of transformer
- cooling bank status
- pump/fan current
- oil level
- pressure relief device status
- conservator membrane device
- loading of the transformer.

Once the above parameters are inputted to one device it makes it easy to assimilate and use the data for analysing the condition of the transformer. As a matter of fact, some of the CMD can perform multi-bank transformer condition monitoring in master-slave mode. As shown in Fig. 7.7 it can be communicated over IEC 61850 protocol for further assessment and trend analysis.

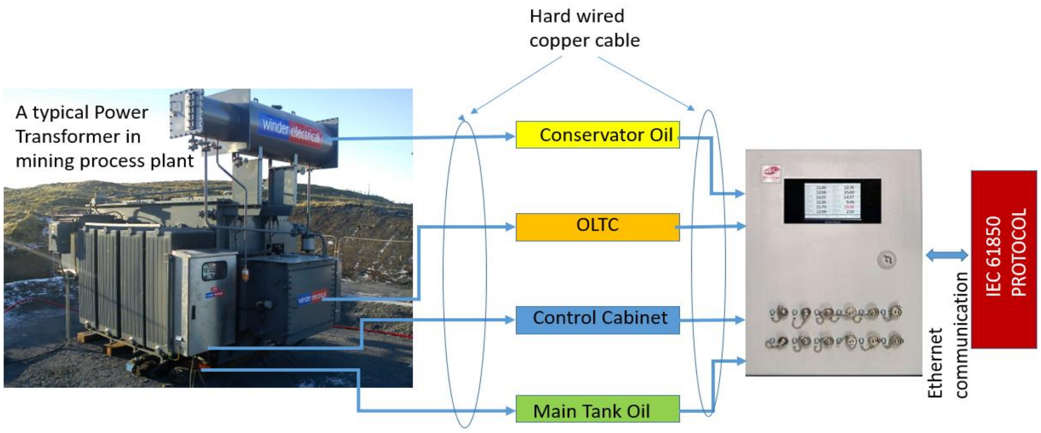


Fig. 7.7. Typical Online Condition Monitoring of a Large Power Transformer in a Substation.

Fig. 7.8 exhibits the modelling concept of a typical Condition Monitoring Device (CMD) that follows a pattern as set out in the block diagram.

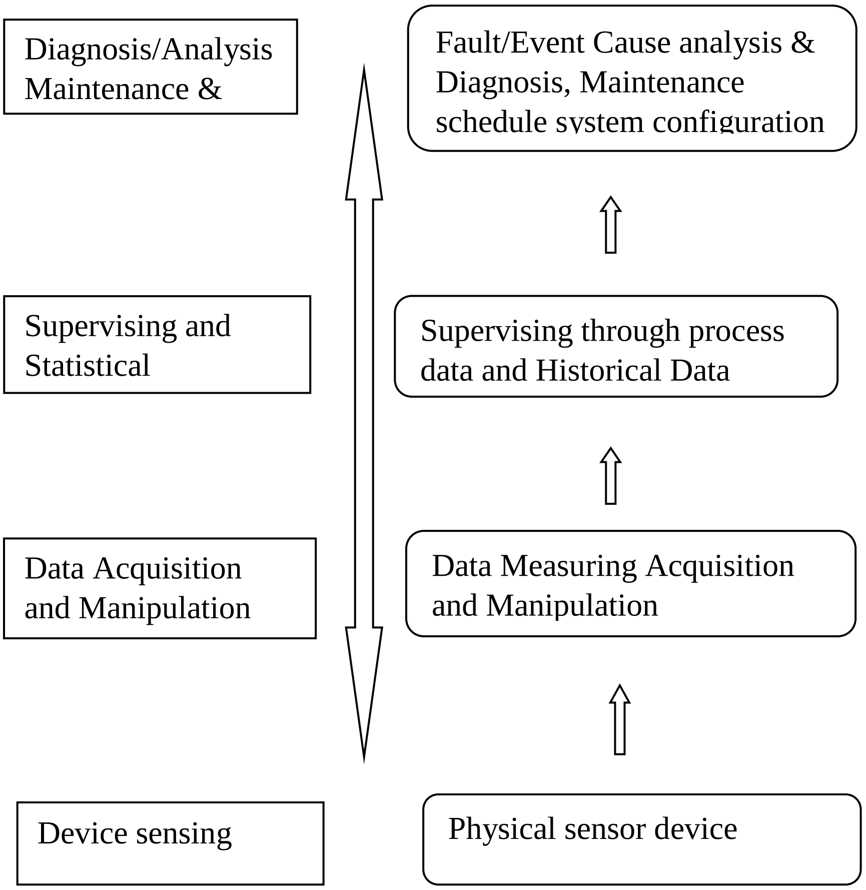


Fig. 7.8. IEC 61850 Based Condition Data Modelling Concept of a Power Transformer.

7.3.3 Implementation of R-GOOSE

R-GOOSE or Routable GOOSE research work has been out of scope in this thesis and needs future researchers to work on it as it could help achieve wide-area protection and control of substation assets. It could find large-scale application in distributed energy resource (DER) with its ability to conduct peer-to-peer communication.

Conventional protection schemes for transmission line protection have issues with instantaneous protection of protected lines. This could be overcome using R-GOOSE method of peer-to-peer communication and faster fault clearance within the protected zone.

Further application of R-GOOSE can be achieved at the transmission level by applying system integrity protection scheme (SIPS) to distributed automation schemes and accelerated protection schemes [11].

7.3.4 Protection against Arc Flash hazard

Arc Faults are rare, but it does happen. It has a huge reputational damage, other techno-commercial and legal impact due to high fatality, unreliability in power supply, unwarranted outages. conventional systems are slow to act due to mechanical and micro processer-based relays. On the other hand, GOOSE and SV IEDs act very fast in clearing faults as exhibited in Fig. 7.9. Although digital IEDs have not been hugely used across substations, future experiments shall prevent catastrophic failure of non-Arc contained cubicles with SAS in a complex network. Future Arc Flash protection systems shall operate when the signals from over current based protection as well as signals from light sensors that shall cross over the threshold level. Scenario1 exhibits conventional relay take longer time using standard electrical parameters i.e., current and voltage while digital relays leveraging on Ethernet and FO use data packets which acts much faster.

The GOOSE based digital Arc Flash system has multiple advantages over the conventional system such as reduced wires, interface with other legacy protocols and expandability of the network. The experimental results encompassing complex protection schemes could be substituted in place of conventional schemes by validating it in a laboratory environment, which is a future work. Fig.7.9 exhibits the huge margin between a conventional versus Digital Arc Flash protection in terms of rapidness to open the HV CB.

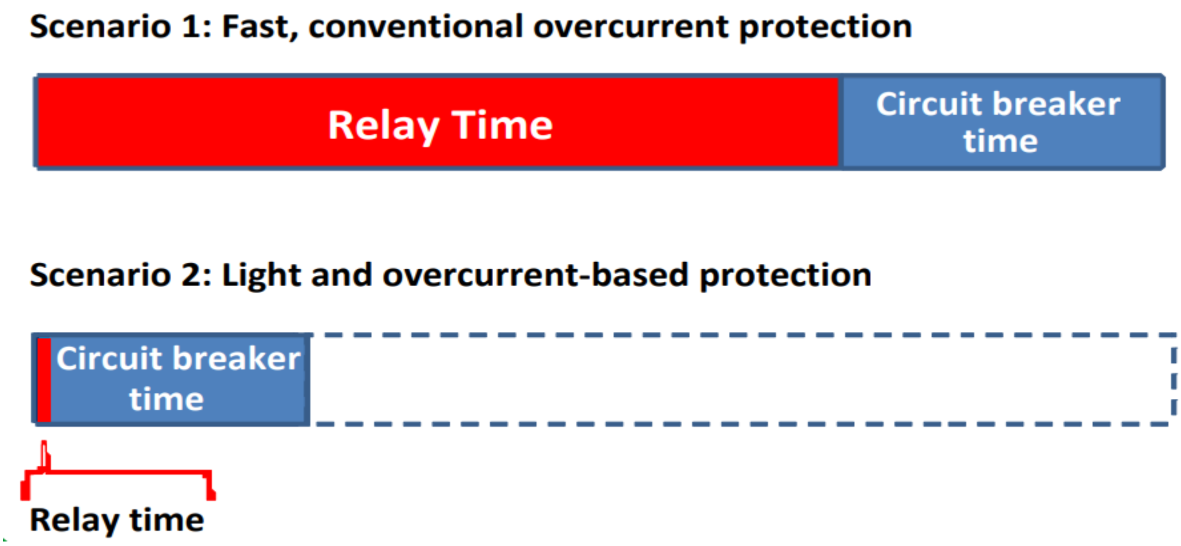

Scenario 1: Fast, conventional overcurrent protection
Relay Time
Circuit breaker time
Scenario 2: Light and overcurrent-based protection
Circuit breaker time
Relay time

Fig 7.9 Conventional versus Digital relay operating time

7.3.5 Functional Design of SAS based on IEC 61850

The future work shall entail functional design of SAS using GOOSE and SV. In order to conduct functional design, the important parameters required are computer design, system management and logic ladder. Future work could discuss the required features of a functional design language in this domain, including the need for an unambiguous formal specification, notation, and exchange format. The future work can also identify the modelling domains of such language, including primary process description, functional description and secondary system description. Others could take interest in international standards and the applicable features of IEC 61850 and IEC 61499 to substation automation that are gaps when functional design is concerned. The work should pursue the standards-based formal functional design languages applicable to SAS by building on the existing IEC 61850 series as an architectural foundation for the engineering of future SASs.

7.3.6 Cybersecurity of a digital protection system

The generation of the mix-based expansion of modern power grids has urged the utilization of digital infrastructures. The introduction of SAS, advanced networks and communication technologies have drastically increased the complexity of the power system, which could comprise the entire power network to hackers. The exploitation of the cyber security vulnerabilities by an attacker may result in devastating consequences and can leave millions of people in severe power outage. To resolve this issue, future projects may be undertaken which shall present a network model developed in OPNET (subjected to various Denial of Service (DoS) attacks) to demonstrate cyber security robustness aspect of an IEC 61850 based digital substations. The attack scenarios can exhibit significant increase in the system delay and the prevention of messages, i.e., transmission of GOOSE and Sampled Measured Values (SMV), within an acceptable period.

7.3.7 Reliability centric digital protection system

Based on the multi-vendor equipment used at Curtin lab, a fault-tree analysis approach to evaluate quantitatively reliability of the digital SAS could be conducted by others. Future work could encompass implementing the proposed method on a modern SAS, using multivendor equipment on a HV Substation creating different scenarios. Reliability centric digital protection scheme could be used to establish and validate a digital architecture which shall be compared with an equivalent conventional protection system. Furthermore, several different ranges of mean time between failures (MTBF) could be checked for the reliability of the system. The proposed method may provide rate of change of system mean time to failure index. Using this index can be a useful tool to choose the best range of IEDs interoperability environment.

7.3.8 Bi-directional flow of electricity with the introduction of renewables

With the introduction of renewables into the system, the unidirectional flow of power from generation to distribution has metamorphosed. Future works by others shall give a better understanding of the bi -directional flow of power with number of substation assets being protected by SAS. Modern society is unquestionably heavily reliant on supply of electricity. Hence, the power system is one of the important infrastructures for future growth. However, the power system of today was designed for a stable radial flow of electricity from large power plants to the customers and not for the type of changes it is presently being exposed to, like large scale integration of electric vehicles, wind power plants, residential photovoltaic systems etc. One aspect of power system control when exposed to these changes is the design of power system control and protection functionality. Problems occur when the flow of electricity changes from a unidirectional radial flow to a bidirectional. Such an implication requires redesign of control and protection functionality as well as introduction of new information and communication technology (ICT). To make matters worse, the closer the interaction between the power system and the ICT systems the more complex the matter becomes from a reliability perspective. This problem is inherently cyber-physical which has been requested in section 7.1, including everything from system software to power cables and transformers, rather than the traditional reliability concern of only focusing on power system components. The contribution of this proposal can be a framework for reliability analysis, utilizing system-modelling concepts that supports the industrial engineering issues that follow with the implementation of modern substation automation systems. This can base the framework on a Bayesian probabilistic analysis engine represented by Probabilistic Relational Models (PRMs) in combination with an Enterprise Architecture (EA) modelling formalism. The work can demonstrate the gradual development of the framework through a number of applications such as information security, since any falsifications may trigger mal-operations, and result in damages to power usage. Others can aim at the authentication and integrity protections in SAS, by an experimental approach on a small-scale SAS prototype, in which messages with commonly used data origin authentication schemes can be transmitted. Through experimental results, others could discover that they cannot apply the current security solutions directly into the SAS due to insufficient performance considerations in response to application constraints, including limited device computation capabilities, stringent timing requirements and high data sampling rates. Moreover, intrinsic limitations of security schemes can be easily hijacked by malicious attackers, to undermine message deliveries, thus becoming security vulnerabilities, these include;-

√ Complicated computations
√ Shorter key valid time, and
√ Limited key supplies.

7.3.9 Authentication and Integrity of protections in SAS

The Smart Grid is an emerging technology that integrates power infrastructures with information technologies to enable intelligent energy managements. As one of the most important facilities of power infrastructures, electrical substations undertake responsibilities of energy transmissions and distributions by operating interconnected electrical devices in a coordinated manner. Accordingly, it imposes a great challenge on information security, since any falsifications may trigger mal-operations, and result in damages to power usage. Future projects could aim at the authentication and integrity protections in SAS, by an experimental approach on a small-scale SAS prototype, in which he can transmit messages with commonly used data origin authentication schemes, such as public-key encryption like RSA, Message Authentication Code, and One-Time Signature. Through experimental results, new project scope shall encompass new security solutions directly into the SAS due to insufficient performance considerations in response to application constraints, including limited device computation capabilities, stringent timing requirements and high data sampling rates.

7.3.10 Future Trends in Instrument Transformers

Although sufficient experiments have been carried out in this thesis related to NCIT, there exists more research work to be done on NCITs which are the key equipment in SAS network. There have been number of publications in IEC 61869-6 and IEC 61869-9 by TC 38 on Instrument Transformers. This raises the question about the standards for digitally interfaced protection functions. IEC TC 95 (Measuring relays and protection equipment) charged a working group to investigate this subject and to elaborate recommendations concerning requirements and testing of protection IED with digital inputs and outputs for protection standards (IEC 60255-1xx series). For protection functions, publisher/subscriber-based data streams are supposed to comply with IEC 61850 and IEC 61869 standards. This holds for SV representing energising inputs of the protection function, applicable to GOOSE, and used for input or output of protection functions. Quality attributes of published data depend on the operational and connection status of the function and the hosting IED. In addition, protection functions must take into account the information regarding the time synchronisation of the received SV and other parameters. Other researchers could give an overview of these features and the proposed way to consider them in the IEC 60255 standard series. These future research works could find a place in the IEC - WG 2 standard committee and relate it to the existing standardization documents.

7.3.11 Fully Digital Protection, Automation and Control Systems (FD-PACS)

Globally there is now introduction of fully digitalized substations using IEC 61850 process bus. Numerous utilities have featured pilot projects, demonstrators or even industrial scale deployment of these Fully Digital Protection, Automation and Control Systems (FD-PACS). Product standards developed include profiles for Instrument Transformers have and been published in IEC 61869-6 and IEC 61869-9 by TC 38 —Instrument Transformers. This raises the question about the standards for digitally interfaced protection functions. IEC TC 95 (Measuring relays and protection equipment) charged a working group to investigate this subject and to elaborate recommendations concerning requirements and testing of protection IED with digital inputs and outputs for protection standards (IEC 60255-1xx series). For protection functions, publisher/subscriber-based data streams are supposed to comply with IEC 61850 and IEC 61869 standards. This holds in particular for Sampled Values (SV) representing energising inputs of the protection function, applicable to GOOSE, and used for input or output of protection functions. Quality attributes of published data depend on the operational and connection status of the function and the hosting IED. In addition, protection functions have to take into account the information regarding the time synchronisation of the received SV and other parameters. Future projects could research and provide an overview of these features and the proposed way to consider them in the IEC 60255 standard series. Research projects need to correlate describe the progress of WG 2 committee and relate it to existing standardization documents.

7.3.12 Application of Internet of Things (IoT) & Constrained Application Protocol (CoAP)

The aim of the SAS network is to improve energy saving and efficiency. Within Smart Grids, different devices and electrical substations communicate with each other and need to be accessible from the outside. Thus, the need of embracing standards, such as those of IEC is pivotal. IEC 61850 is a standard that covers such a need, and it proposes to use different communication protocols, to fulfil the features that the standard proposes. Most proposals focus on heavyweight protocols. However, the growth of the Internet of Things (IoT) demands resource-constrained devices to participate in IoT networks. In this regard, there is design and development of new protocols like Constrained Application Protocol (CoAP). Other researchers could adopt CoAP to provide a full mapping of the functionalities specified in IEC 61850 for electrical substations. Furthermore, future research work can provide an analytical and critical review of the already proposed mapping approaches that could lead towards accelerating the adoption of IoT and Web of Things standards in Smart Grid scenarios.

7.4. CHAPTER SUMMARY

Future research shall focus on different methodologies applied to carry out newer trends leveraging on communication protocols. It shall focus on network traffic management of GOOSE and SV to reduce the traffic flow by designing an integrated system, developing a hardware and software platform that works well on IoT system. At the same time, the research should have a cybersecurity component, as mentioned in the previous section, to detect and block malicious attacks on the infrastructure. The prototype models to be tested based on IEC 61850 protocol need to carry out as desktop modelling as well as practical testing on IEDs, implementing real SAS devices available at Curtin University's substation laboratory including:

7. Real Time Simulation on Station bus and Process bus communication.
8. Studying true interaction of the protection IEDs with power system using R-GOOSE,
9. Analysing CMD information and predicting health index of the power transformer.
10. Providing maximum simulation efficiency (i.e. more contingencies can be investigated in less time).
11. Application of a packet scheduling and traffic management scheme within the substation SAS network.
12. Detecting and blocking cyberattacks on vulnerable points.
13. Checking on the performances of various topologies.
14. Simulating R-GOOSE in the network and checking its performance.
15. Applying CMD to field devices such as Power Transformers, CTs, VTs and other switchyard equipment and monitoring loading under dynamic condition based on IEC 61850.
16. Application and performance monitoring of NCITs on protection IEDs.
17. Monitoring WAN substations in a complex network.
18. Time synchronization of protection devices during evolving faults.

7.5 REFERENCES

[1] W. Bao, H. Zhang, H. Li, W. Huang and D. Peng, "Analysis and Research on the Real-Time Performance of Profibus & Fieldbus," *2009 WRI World Congress on Software Engineering*, Xiamen, China, 2009, pp. 136-140, doi: 10.1109/WCSE.2009.181.

[2] Cost Benefit Analysis for IEC 61850 Implementation - Quanta Technology (quanta-technology.com).

[3] M. S. Thomas and I. Ali, "Reliable, Fast, and Deterministic Substation Communication Network Architecture and its Performance Simulation," in *IEEE Transactions on Power Delivery*, vol. 25, no. 4, pp. 2364-2370, Oct. 2010, doi: 10.1109/TPWRD.2010.2042824.

[4] S. Kumar, N. Das and S. Islam, "High Voltage Substation Automation and Protection System Based on IEC 61850," *2018 Australasian Universities Power Engineering Conference (AUPEC), New Zealand, 2018*, pp. 1-6, doi: 10.1109/AUPEC.2018.8757995.

[5] M. Vadiati, M. A. Ghorbani, A. R. Ebrahimi and M. Arshia, "Future trends of substation automation system by applying IEC 61850," *2008 43rd International Universities Power Engineering Conference, Padua, Italy, 2008, pp. 1-4, doi: 10.1109/UPEC.2008.4651480.*

[6] M. Vadiati, M. Basirifar and B. Shahbazi, "Future trends in smart grid by applying digital modern substations," *2011 IEEE PES Innovative Smart Grid Technologies*, Perth, WA, Australia, 2011, pp. 1-6, doi: 10.1109/ISGT-Asia.2011.6167109.

[7] F. Li, X. Yan, Y. Xie, Z. Sang and X. Yuan, "A Review of Cyber-Attack Methods in Cyber-Physical Power System," *2019 IEEE 8th International Conference on Advanced Power System Automation and Protection (APAP)*, Xi'an, China, 2019, pp. 1335-1339, doi: 10.1109/APAP47170.2019.9225126.

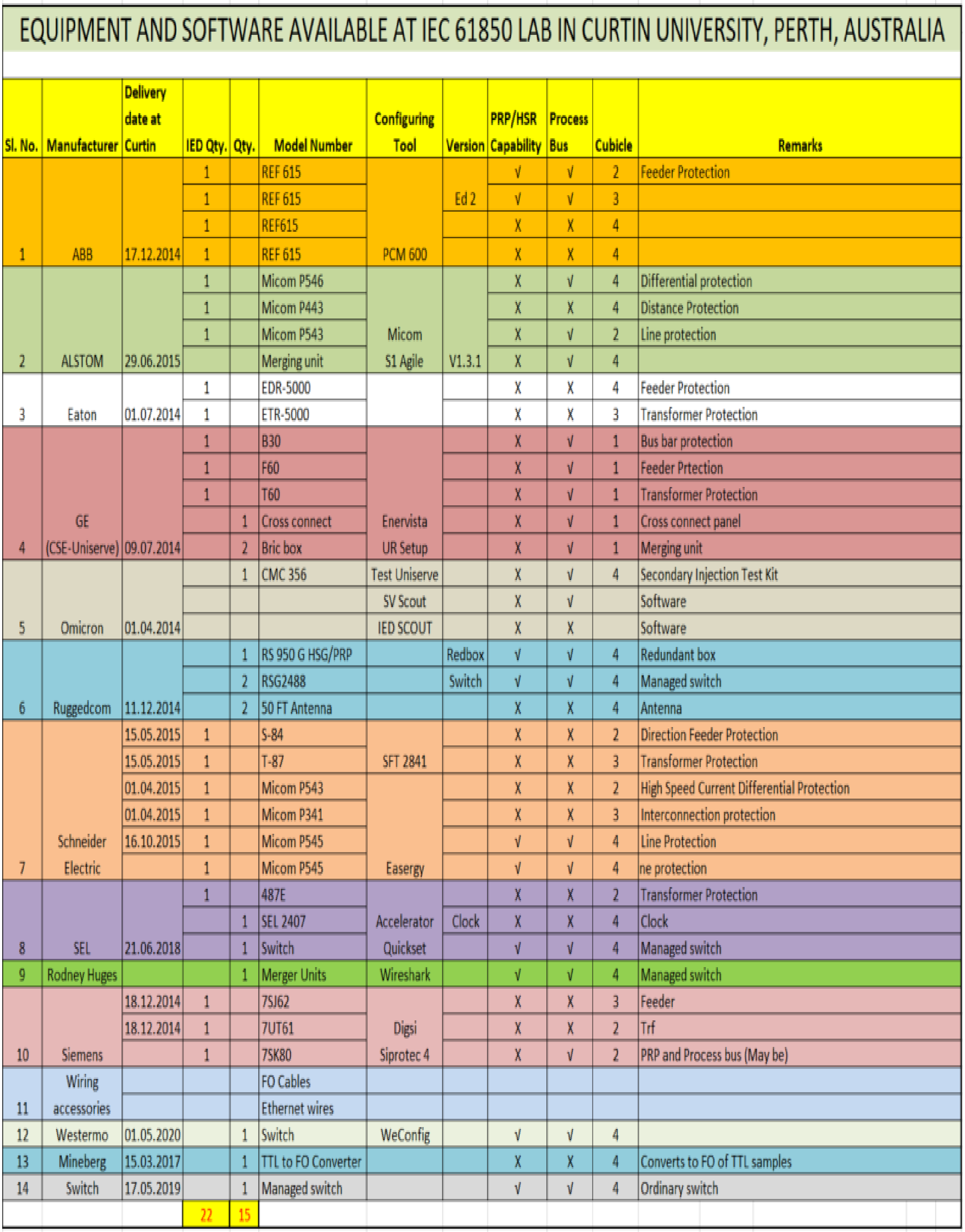
[8] IEC TR 61850-90-3:2016 - Using IEC 61850 for condition monitoring diagnosis.

[9] Proceedings of Australian Protection Symposium, Aug 16-17, 2016, Melbourne, Australia.

[10] Hai-Bin Zhou, M. Dong and Dai-Yong Yang, "An intelligent monitoring and diagnosis system for 330kV oil-immersed power transformer," *Proceedings of 2011 International Symposium on Electrical Insulating Materials*, Kyoto, Japan, 2011, pp. 257-260, doi: 10.1109/ISEIM.2011.6826281.

[11] T. S. Ustun, S. M. Farooq and S. M. S. Hussain, "Implementing Secure Routable GOOSE and SV Messages Based on IEC 61850-90-5," in *IEEE Access*, vol. 8, pp. 26162-26171, 2020, doi: 10.1109/ACCESS.2020.2971011.

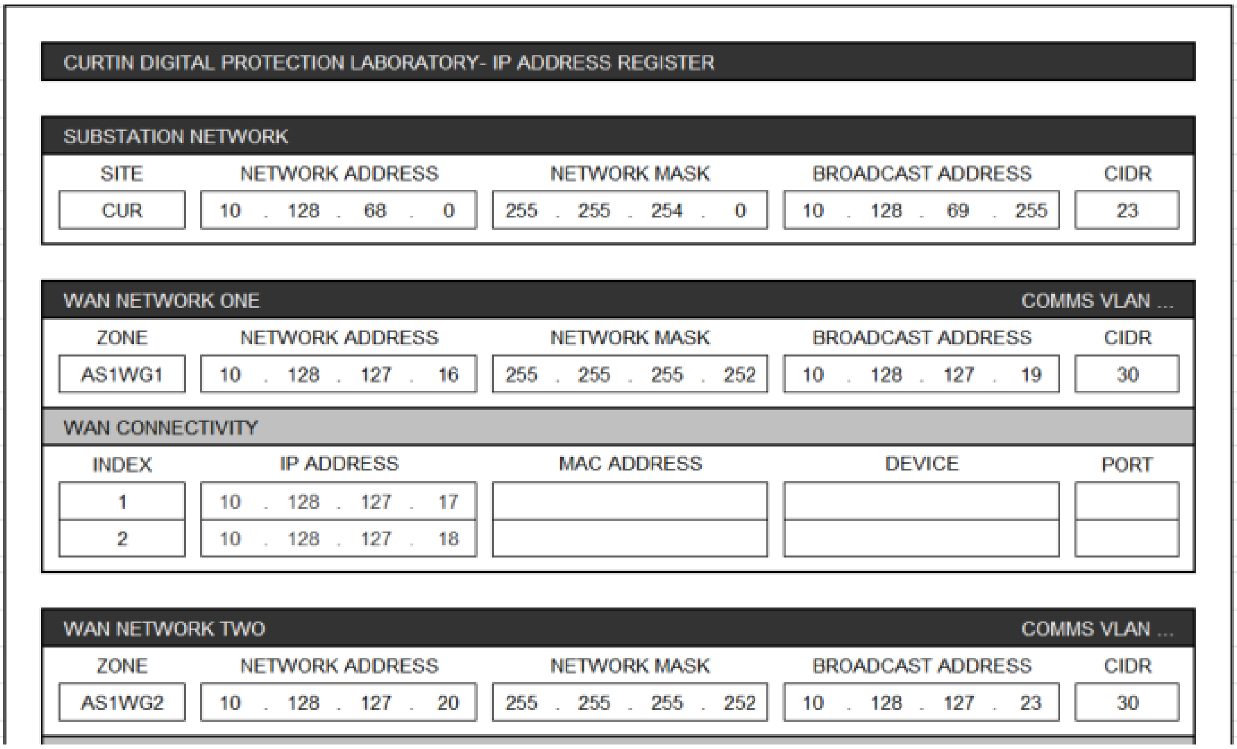
APPENDIX A. EQUIPMENT AND SOFTWARE AT CURTIN UNIVERSITY IEC LABORATORY



EQUIPMENT AND SOFTWARE AVAILABLE AT IEC 61850 LAB IN CURTIN UNIVERSITY, PERTH, AUSTRALIA

Sl. No.	Manufacturer	Delivery date at Curtin	IED Qty.	Qty.	Model Number	Configuring Tool	Version	PRP/HSR Capability	Process Bus	Cubicle	Remarks
1	ABB	17.12.2014	1		REF 615	PCM 600	Ed 2	√	√	2	Feeder Protection
			1		REF 615			√	√	3	
			1		REF615			X	X	4	
			1		REF 615			X	X	4	
2	ALSTOM	29.06.2015	1		Micom P546	Micom S1 Agile	V1.3.1	X	√	4	Differential protection
			1		Micom P443			X	X	4	Distance Protection
			1		Micom P543			X	√	2	Line protection
					Merging unit			X	√	4	
3	Eaton	01.07.2014	1		EDR-5000			X	X	4	Feeder Protection
			1		ETR-5000			X	X	3	Transformer Protection
4	GE (CSE-Uniserve)	09.07.2014	1		B30	Enervista UR Setup		X	√	1	Bus bar protection
			1		F60			X	√	1	Feeder Prtection
			1		T60			X	√	1	Transformer Protection
				1	Cross connect			X	√	1	Cross connect panel
				2	Bric box			X	√	1	Merging unit
5	Omicron	01.04.2014		1	CMC 356	Test Uniserve		X	√	4	Secondary Injection Test Kit
						SV Scout		X	√		Software
						IED SCOUT		X	X		Software
6	Ruggedcom	11.12.2014		1	RS 950 G HSG/PRP		Redbox	√	√	4	Redundant box
				2	RSG2488		Switch	√	√	4	Managed switch
				2	50 FT Antenna			X	X	4	Antenna
7	Schneider Electric	15.05.2015	1		S-84	SFT 2841		X	X	2	Direction Feeder Protection
		15.05.2015	1		T-87			X	X	3	Transformer Protection
		01.04.2015	1		Micom P543	Easergy		X	X	2	High Speed Current Differential Protection
		01.04.2015	1		Micom P341			X	X	3	Interconnection protection
		16.10.2015	1		Micom P545			√	√	4	Line Protection
			1		Micom P545			√	√	4	ne protection
8	SEL	21.06.2018	1		487E	Accelerator Quickset		X	X	2	Transformer Protection
				1	SEL 2407		Clock	X	X	4	Clock
				1	Switch			√	√	4	Managed switch
9	Rodney Huges			1	Merger Units	Wireshark		√	√	4	Managed switch
10	Siemens	18.12.2014	1		7SJ62	Digsi Siprotec 4		X	X	3	Feeder
		18.12.2014	1		7UT61			X	X	2	Trf
			1		7SK80			X	√	2	PRP and Process bus (May be)
11	Wiring accessories				FO Cables						
					Ethernet wires						
12	Westermo	01.05.2020		1	Switch	WeConfig		√	√	4	
13	Mineberg	15.03.2017		1	TTL to FO Converter			X	X	4	Converts to FO of TTL samples
14	Switch	17.05.2019		1	Managed switch			√	√	4	Ordinary switch
			22	15							

APPENDIX B. IP ADDRESS REGISTER OF LABORATORY EQUIPMENT



CURTIN DIGITAL PROTECTION LABORATORY- IP ADDRESS REGISTER

SUBSTATION NETWORK

SITE	NETWORK ADDRESS	NETWORK MASK	BROADCAST ADDRESS	CIDR
CUR	10 . 128 . 68 . 0	255 . 255 . 254 . 0	10 . 128 . 69 . 255	23

WAN NETWORK ONE COMMS VLAN ...

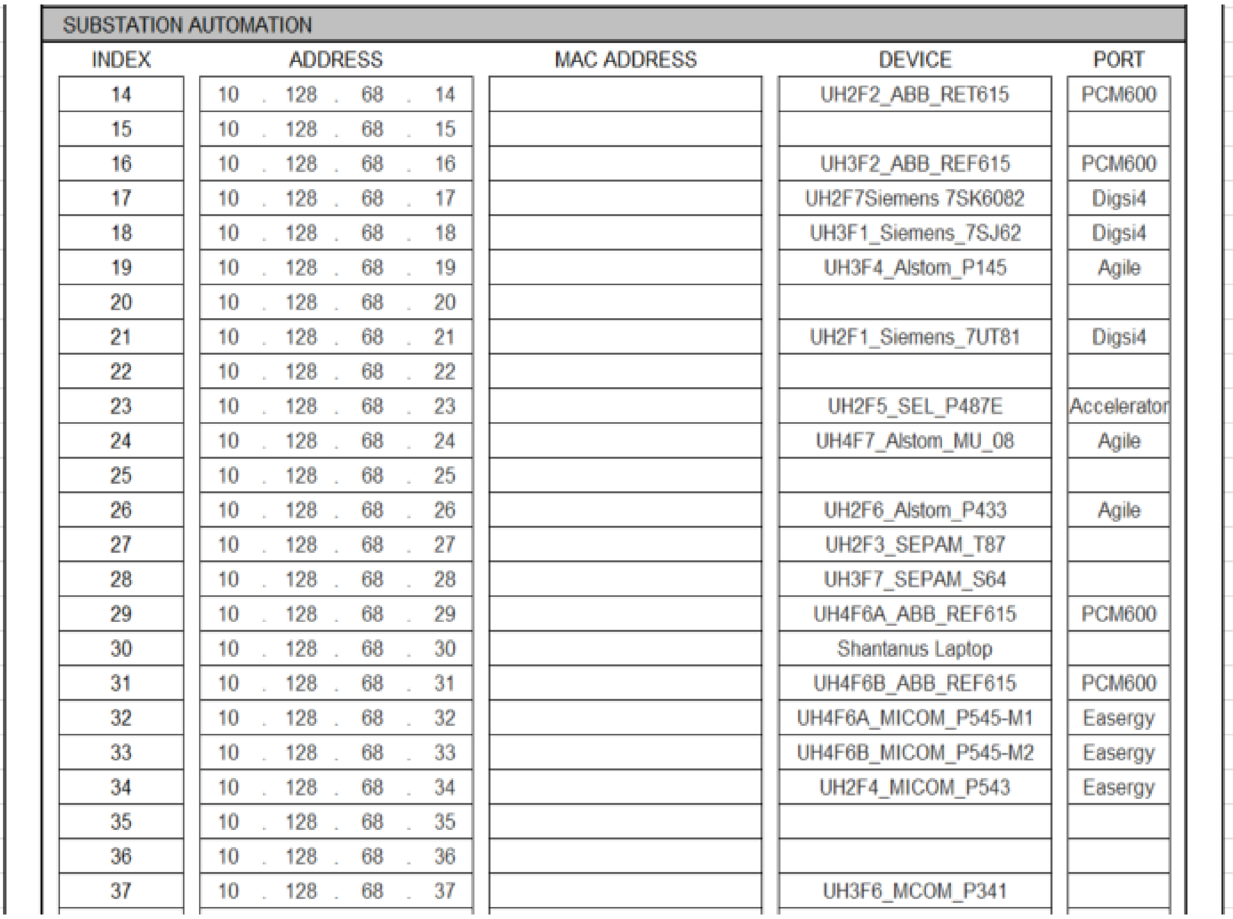
ZONE	NETWORK ADDRESS	NETWORK MASK	BROADCAST ADDRESS	CIDR
AS1WG1	10 . 128 . 127 . 16	255 . 255 . 255 . 252	10 . 128 . 127 . 19	30

WAN CONNECTIVITY

INDEX	IP ADDRESS	MAC ADDRESS	DEVICE	PORT
1	10 . 128 . 127 . 17			
2	10 . 128 . 127 . 18			

WAN NETWORK TWO COMMS VLAN ...

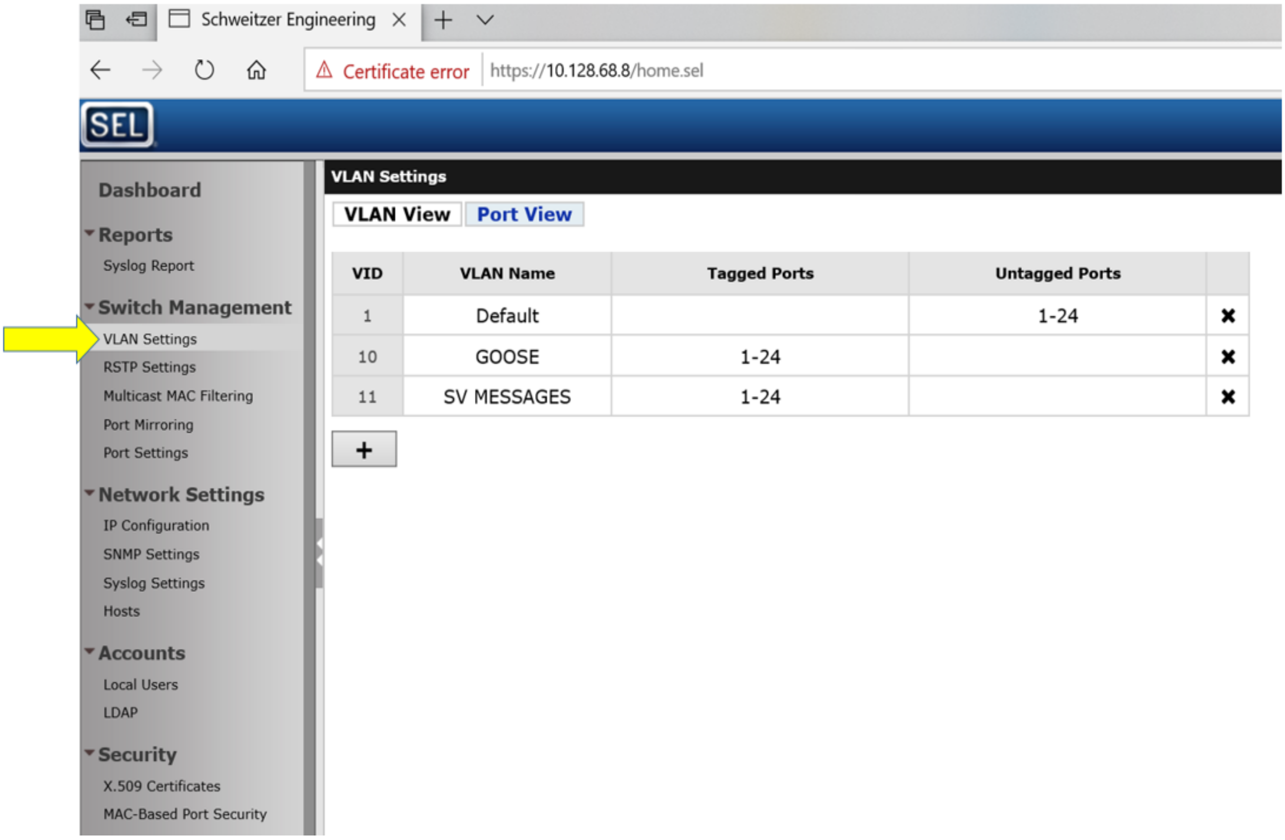
ZONE	NETWORK ADDRESS	NETWORK MASK	BROADCAST ADDRESS	CIDR
AS1WG2	10 . 128 . 127 . 20	255 . 255 . 255 . 252	10 . 128 . 127 . 23	30



SUBSTATION AUTOMATION

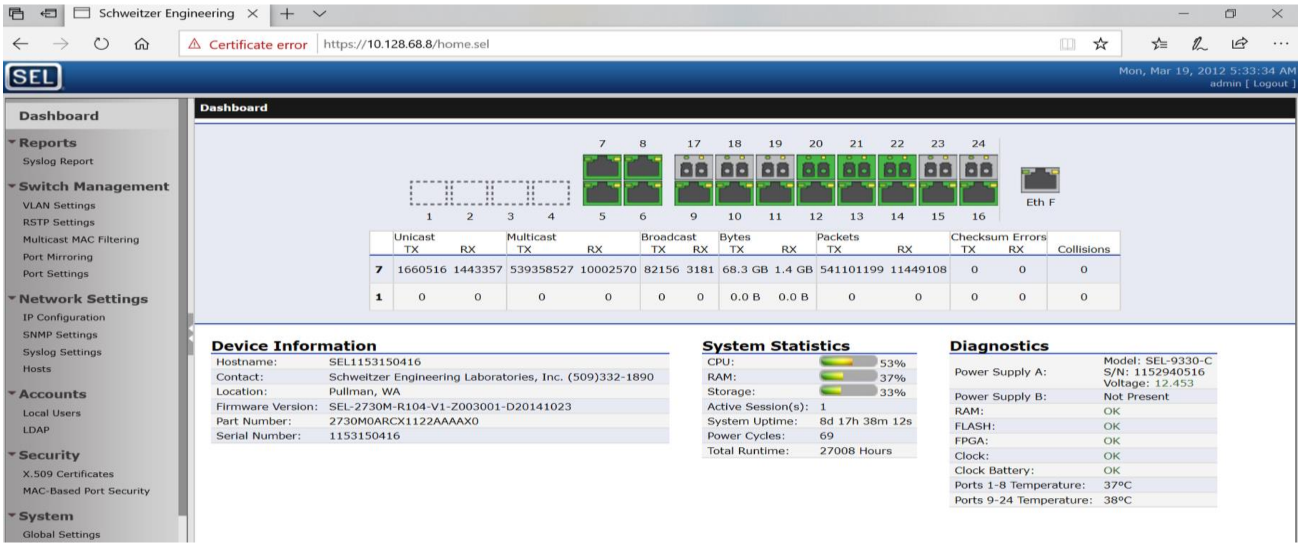
INDEX	ADDRESS	MAC ADDRESS	DEVICE	PORT
14	10 . 128 . 68 . 14		UH2F2_ABB_RET615	PCM600
15	10 . 128 . 68 . 15			
16	10 . 128 . 68 . 16		UH3F2_ABB_REF615	PCM600
17	10 . 128 . 68 . 17		UH2F7Siemens 7SK6082	Digsi4
18	10 . 128 . 68 . 18		UH3F1_Siemens_7SJ62	Digsi4
19	10 . 128 . 68 . 19		UH3F4_Alstom_P145	Agile
20	10 . 128 . 68 . 20			
21	10 . 128 . 68 . 21		UH2F1_Siemens_7UT81	Digsi4
22	10 . 128 . 68 . 22			
23	10 . 128 . 68 . 23		UH2F5_SEL_P487E	Accelerator
24	10 . 128 . 68 . 24		UH4F7_Alstom_MU_08	Agile
25	10 . 128 . 68 . 25			
26	10 . 128 . 68 . 26		UH2F6_Alstom_P433	Agile
27	10 . 128 . 68 . 27		UH2F3_SEPAM_T87	
28	10 . 128 . 68 . 28		UH3F7_SEPAM_S64	
29	10 . 128 . 68 . 29		UH4F6A_ABB_REF615	PCM600
30	10 . 128 . 68 . 30		Shantanus Laptop	
31	10 . 128 . 68 . 31		UH4F6B_ABB_REF615	PCM600
32	10 . 128 . 68 . 32		UH4F6A_MICOM_P545-M1	Easergy
33	10 . 128 . 68 . 33		UH4F6B_MICOM_P545-M2	Easergy
34	10 . 128 . 68 . 34		UH2F4_MICOM_P543	Easergy
35	10 . 128 . 68 . 35			
36	10 . 128 . 68 . 36			
37	10 . 128 . 68 . 37		UH3F6_MCOM_P341	

APPENDIX C. VLAN SET-UP FOR GOOSE AND SV IN SEL-2730 M



VID	VLAN Name	Tagged Ports	Untagged Ports	
1	Default		1-24	✖
10	GOOSE	1-24		✖
11	SV MESSAGES	1-24		✖

SEL-2730 M Overall setup



	Unicast		Multicast		Broadcast		Bytes		Packets		Checksum Errors		
	TX	RX	TX	RX	TX	RX	TX	RX	TX	RX	TX	RX	Collisions
7	1660516	1443357	539358527	10002570	82156	3181	68.3 GB	1.4 GB	541101199	11449108	0	0	0
1	0	0	0	0	0	0	0.0 B	0.0 B	0	0	0	0	0

Device Information

Hostname:	SEL1153150416
Contact:	Schweitzer Engineering Laboratories, Inc. (509)332-1890
Location:	Pullman, WA
Firmware Version:	SEL-2730M-R104-V1-Z003001-D20141023
Part Number:	2730M0ARCX1122AAAAX0
Serial Number:	1153150416

System Statistics

CPU:	53%
RAM:	37%
Storage:	33%
Active Session(s):	1
System Uptime:	8d 17h 38m 12s
Power Cycles:	69
Total Runtime:	27008 Hours

Diagnostics

Power Supply A:	Model: SEL-9330-C S/N: 1152940516 Voltage: 12.453
Power Supply B:	Not Present
RAM:	OK
FLASH:	OK
FPGA:	OK
Clock:	OK
Clock Battery:	OK
Ports 1-8 Temperature:	37°C
Ports 9-24 Temperature:	38°C

Engaged Ethernet ports are in green.