January 14, 2013

Communications Technology for Protection Systems

Power System Relaying Committee

Relaying Communications Subcommittee

Special report prepared by WG H9

Assignment

Prepare a document that would assist engineers in understanding the communications technology for protective relaying.

Members of the Working Group

René Midence, Chair

Moh Sachdev, Vice Chair

Members

Antonova, G.	Ariza, J.	Bell, T.	Benou, M.
Bolado, O.	Brahma, S.	Brettschneider, S.	Castro, L.
Chaparro, R.	Chelmecki, Chris	Dahlin, T.	De La Quintana, A.
Ebrecht, J.	Gauci, A.	Gers, J.M.	Harada, R.
Hamilton, R.	Higinbotham, B.	Huerta C.	Iadonisi, D.
Ince, B.	Kwan, M.	Li, T.	Lu, Y.
MacKie, B.	McHale, E.	McLaren, P.	Murphy, J.
Niemira, J.	Nordell, D.	Oba, E.	Pathirana, V.
Rizvi, I.	Sambasivan, S.	Sidhu, T.	Simon, M.
Thompson, S.	Tournier, J.C.	Ward, S.	Yang, Y.

Table of Contents

1. Introduction 10
   1.1 The Introduction of Digital Communications 13
   1.2 Data Communications for Protection and Control 13
   1.3 Substation Automation Examples 22
   1.4 Substation Automation with Electromechanical Relays 22
   1.5 Substation Automation with Numerical Relays 26
      1.5.1 Numerical Relays and Serial Communications RS-232 27
      1.5.2 Numerical Relays and Serial Communications RS-485 28
      1.5.3 Numerical Relays and Ethernet Networks 30
2. Analog and Discrete Signals 31
3. Synchronous communication 33
4. Asynchronous communication 34
5. Bit Error and Bit Error Correction 34
   5.1 Bit Errors 34
   5.2 Bit Error Correction 35
   5.3 Alarms 36
6. Channel Delay 36
   6.1 Resynchronization 37
7. Jitter and wander 37
   7.1 Why jitter is important 38
   7.2 Symptoms of Jitter/Wander Issues 38
8. Basic Considerations in Digital Communications 39
   8.1 Speed / Delay 39
   8.2 Dependability and Security 41
   8.3 Redundancy 41
   8.4 Reliability and Availability of Communications Networks 42
   8.5 Noise 44
      8.5.1 Noise in Digital Circuits 44
      8.5.2 Noise in Analog Circuits 44
      8.5.3 Power system coupled noise 45
      8.5.4 Noise Detection 45
9. OSI Protocol Model 45
10. Multiplex Channel, SDH, PDH, SONET 47
   10.1 Multiplexing 47
      10.1.1 Frequency Division Multiplexing 47
      10.1.2 Wave Division Multiplexing 47
      10.1.3 Time Division Multiplexing 48
      10.1.4 Code Division Multiplexing (Spread Spectrum) 48
   10.2 Digital Hierarchies 48
      10.2.1 PDH - Plesiochronous Digital Hierarchy 49
   10.3 SONET (Synchronous Optical Network) and SDH (Synchronous Digital Hierarchy) 50
      10.3.1 Basic SONET Signal 51
      10.3.2 Synchronous Digital Hierarchy (SDH) 51
      10.3.3 SONET/SDH network topologies and network resilience 52

10.3.4 GR-1230 4-Fiber Bi-directional Line Switched Ring (BLSR) 58
10.3.5 SONET Delay Characteristics 58
10.3.6 SONET Restoration Characteristics 58
10.4 SONET/SDH for power system protection 59
10.4.1 PDH/SONET/SDH Networks 59
10.5 SONET Synchronization 61
10.5.1 Stratum Clock Hierarchy 61
10.5.2 Synchronization Status Messages (SSM) 62
11. Physical Communications Media- Electrical 63
11.1 Serial Communications RS-232 63
11.1.1 Voltage levels 64
11.1.2 RS-232 Data Structure 65
11.1.3 RS-232 Physical Properties 66
11.1.4 Maximum cable lengths 66
11.1.5 Error detection 68
11.1.6 Disadvantages of the parity system 68
11.2 Serial Communications RS-485 69
11.2.1 Uses of EIA-485 70
11.2.2 Differential signals with RS-485 70
11.2.3 Network topology with RS-485 72
11.2.4 RS-485 functionality 73
11.3 Electrical Interfaces 73
11.3.1 Metallic media (coax and twisted pair) 73
11.3.2 Digital Electrical Interfaces 74
11.3.3 RS-232 Electrical Interface 75
11.3.4 RS449 Electrical Interface 75
11.3.5 V.35 Electrical Interface 77
11.3.6 G.703 Electrical Interface 78
11.3.7 RS530 Electrical Interface 80
11.3.8 Electrical Interface Comparison 82
11.3.9 Serial Communications RS-422 82
12. Physical Communication Media- Fiber Optic 83
12.1 Introduction 83
12.2 Fiber Optic Connectors 86
12.3 Design 86
12.3.1 ST 86
12.3.2 SC 87
12.3.3 FC 87
12.3.4 LC 88
12.3.5 MT-RJ 88
13. Physical Communications Media- Microwave and Wireless 89
13.1 Microwave 89
13.1.1 Microwave losses 91
13.1.2 Digital Microwave Channel Performance 92
13.2 Wireless (other than microwave) 93
13.2.1 Spread Spectrum Radio 93

13.2.2 Cellular Telephone 93
13.3 Digital Radio 93
14. TCP/IP 94
14.1 History 94
14.2 TCP/IP Layers 95
14.3 IP Addressing 97
14.4 Static and dynamic IP addresses 98
14.4.1 Method of assignment 98
14.4.2 Uses of dynamic addressing 98
15. Ethernet 99
15.1 Ethernet Brief History 100
15.2 The OSI Model - Ethernet 100
15.3 The Ethernet Packet 101
15.4 An Introduction to IP- Internet Protocol 103
15.4.1 What is IP? 103
15.4.2 Ethernet and IP- how do they work? 103
15.5 Ethernet OSI Layer 1- Physical Layer 105
15.5.1 Physical cabling 105
15.6 Ethernet OSI Layer 2 107
15.6.1 Ethernet Layer 2 Structure 107
15.6.2 Ether Layer 2 Protocols and Functions 108
15.7 Ethernet OSI Layer 3- IP Layer Routers and Router redundancy 114
15.7.1 Introduction 114
15.7.2 IP Addressing and Subnetting 116
15.7.3 IPv4 Subnetting 116
15.8 Ethernet Network Types and Orientations 117
15.8.1 Cascade 117
15.8.2 Star Topology 118
15.8.3 Ring 118
15.8.4 Hybrid Architecture 119
15.8.5 Mesh Topology 120
15.8.6 Scalability 121
15.9 Comparing Serial with Ethernet Communications 121
15.10 Ethernet in Substation Environment 122
15.11 Enabling Peer-to-Peer Communications 123
15.12 Multiple Master Access to IEDs 124
15.13 Transfer Rate vs. Media Type 124
16. High availability Ethernet protocols 126
16.1 Media Redundancy Protocol (MRP) 126
16.2 Parallel Redundancy Protocol (PRP) 126
16.3 High-availability Seamless Redundancy (HSR) 127
16.4 Cross-network Redundancy Protocol (CRP) 127
16.5 Beacon Redundancy Protocol (BRP) 128
16.6 Distributed Redundant Protocol (DRP) 128
16.7 Summary 128
17. Utility Oriented Protocols 129

17.1 Proprietary protocols 129
17.2 Modbus Protocol 130
17.2.1 Introduction 130
17.2.2 Message structure 131
17.2.3 Addressing 132
17.2.4 Function codes 132
17.2.5 Limitations 132
17.2.6 Modbus messaging on TCP/IP 133
17.3 Distributed Network Protocol (DNP) 3 135
17.3.1 History 135
17.4 IEC 60870-5 136
17.4.1 IEC 60870-5-101 136
17.4.2 IEC 60870-5-103 138
17.4.3 IEC 60870-5-104 139
17.5 IEC 61850 Standard 140
17.5.1 Introduction 140
17.5.2 Description of IEC 61850 standard 140
17.5.3 Approach of IEC61850 142
17.5.4 Organization of logical device 142
17.5.5 OSI-7 stack for message communication 144
17.5.6 Substation Configuration Language (SCL) 145
18. Serial to Ethernet Conversion 146
18.1 Introduction 146
18.2 Serial to Ethernet Technologies 147
18.2.1 Overview 147
18.2.2 What is Ethernet Encapsulation? 148
18.3 RaW Socket TCP/IP 149
18.4 Serial Server – Serial to TCP Protocol Converter 151
18.5 Gateway Approach 155
19. IEEE 1588 Precision Time Protocol (PTP) 157
19.1 Brief history of Precision Time Protocol 157
19.2 What is Precision Time Protocol? 158
19.3 How PTP works… 159
19.4 PTP Applications 163
19.4.1 Utility- IEC 61850 Process Bus 163
19.4.2 Utility- Distributed generation of IRIG-B cyclic timing 164
20. Power Line Carrier 165
20.1 Media 165
20.2 System Overview 166
20.3 Coupling 166
20.3.1 Coupling Schemes 166
20.3.2 Line Trap 169
20.3.3 Tuning Device 170
20.3.4 Protective Device 170
20.3.5 Coupling Capacitor 170
20.3.6 Line Tuner 171

20.4 PLCC Equipment 172
20.4.1 FSK PLCC 173
20.4.2 ON/ OFF PLCC 173
20.4.3 Multifunction 174
20.4.4 Analog PLCC 174
20.4.5 Digital PLCC 177
21. Networks Communication Topologies 183
21.1 Point-to-Point 184
21.2 Star 184
21.3 Linear Drop and Insert 184
21.4 Ring 185
22. Role of Telecommunications in Protection Schemes 185
22.1 Introduction 185
22.2 Communication assisted schemes (Phase and Directional Comparison) 185
22.3 Current Differential Schemes 186
22.3.1 Pilot Wire Relays 186
22.3.2 Digital Current Differential Relays 188
22.3.3 Phase Comparison and Current Differential 191
22.3.4 Directional Comparison 192
22.4 Transfer Trip Schemes 193
22.4.1 Permissive Overreaching Transfer Trip (POTT) Scheme 193
22.4.2 Permissive Underreaching Transfer Trip (PUTT) Scheme 194
22.4.3 Directional Comparison Blocking (DCB) 195
22.4.4 Directional Comparison Unblocking (DCUB) 196
22.4.5 Direct Transfer Trip (DTT) Scheme. 197
22.4.6 Concluding Engineering Considerations 199
23. Substation Automation and SCADA 199
23.1 Overview of EMS/SCADA Communications 199
23.2 SCADA RTU to Control Center Communications 201
23.3 Inter-Control Center Communications 203
23.4 SCADA System Security 204
24. Setting Changes via Telecommunication Channels 205
25. Fault Recorder 205
26. Fault Location 206
27. Wide Area Protection including Synchrophasor Applications 207
27.1 Synchrophasor Systems 207
28. Event Recorder 208
Appendix 1 209
Glossary of terms 209
Appendix 2 214
Acronyms 214
Appendix 3 220
List of Standards 220
References 223

List of Tables

Table 1 Medium Propagation Times (microseconds) 36
Table 2 Teleprotection Requirements According to IEC 60834-1 41
Table 3 North American Digital Hierarchy 49
Table 4 International Digital Hierarchy 50
Table 5 SONET Digital Hierarchy 51
Table 6 Synchronous Digital Hierarchy 51
Table 7 Logical Equivalence of the Terminology 52
Table 8 2-Fiber BLSR OC-1 Channel plan under normal conditions 57
Table 9 2-Fiber BLSR OC-1 Channel plan during fiber break between Nodes B and C 57
Table 10 Stratum Clock Hierarchy 61
Table 11 Stratum Clocking Accuracy Timing Requirements 62
Table 12 Cables Lengths 67
Table 13 Characteristics of RS-485 compared to RS-232, and RS422 71
Table 14 V.35 Connector Pinning 77
Table 15 Some Definitions 78
Table 16 Some Electrical Characteristics 79
Table 17 Some Electrical Characteristics 79
Table 18 Some Electrical Characteristics 79
Table 19 Some Electrical Characteristics for T1 80
Table 20 Some Electrical Characteristics for E1 80
Table 21 Pinning Specifications 80
Table 22 RS530 Pinning Specifications 81
Table 23 Electrical Interface Comparison Table 82
Table 24 Some Electrical Characteristics for RS422 83
Table 25 Optical Budget 85
Table 26 Protocol Grouping by Layers 97
Table 27 Categories of Unshielded Twisted Pair 105
Table 28 IP Address Classification 116
Table 29 Guide to Ethernet Coding 124
Table 31 Modbus Message Structure 131
Table 32 Modbus Address Ranges 132
Table 33 Modbus Typical Function Codes 132
Table 34 Modbus TCP Facts 134
Table 35 IEC 101 Frame Format & Variable Length 137
Table 36 IEC 103 Frame Format & Variable Length 138
Table 38 Timing Protocol Hierarchy 157
Table 39 Timing Requirements for Applications 158

Table of Figures

Figure 1 – Typical Electromechanical Relay Diagram 14
Figure 2 – The Introduction of RTUs / PLCs 14
Figure 3 – Numerical Relays Communication Example 17
Figure 4 – Introduction of the Gateway 18
Figure 5 – Ethernet in the Substation 19
Figure 6 – The router as the interface between LAN and WAN 20
Figure 7 - Substation Single Line Diagram 22
Figure 8 - RTU / PLC Interfaces 24
Figure 9 - Substation Automation Communication System 26
Figure 10 - Substation Network - Serial Communications RS-232 27
Figure 11 - Substation Network - Serial Communications RS-485 29
Figure 12 - Basic Ethernet Network 30
Figure 13 – Analog Signal 32
Figure 14 – Digital Signal 32
Figure 15 – Jitter as Viewed on an Oscilloscope 37
Figure 16 – Phase Variation Between Two Signals 38
Figure 17 – Frequency ranges of jitter and wander (ref. G.810) 38
Figure 18 – Pilot relay communication 40
Figure 19 – Representation of a reliability function and MTTF with a failure rate of 0.99 42
Figure 20 – Illustration of the reliability calculation of the network communication using a reliability block diagram approach. 43
Figure 21 – OSI Model 45
Figure 22 – Example of the OSI Model in Use 46
Figure 23 – Path Terminating Equipment Circuit Level 53
Figure 24 – Path Terminating Equipment Circuit Level Switch 53
Figure 25 – 2-Fiber Unidirectional Path 54
Figure 26 – Protected traffic flow in 2-Fiber UPSR 54
Figure 27 – Example of unequal channel delay 55
Figure 28 – 2-Fiber Bi-directional Line Switched Ring 56
Figure 29 – Protected traffic flow in 2-Fiber BLSR 56
Figure 30 - Diagrammatic oscilloscope trace of voltage levels 64
Figure 31 – Data Structure 66
Figure 32 – Noise in Straight and Twisted Pair Cables 71
Figure 33 – RS-485 Network Topology 73
Figure 34 – DTE and DCE devices 75
Figure 35 – RS-232 Typical Connectors 75
Figure 36 – RS449 Pinouts 76
Figure 37 – Optical Fibers 85
Figure 38 – Losses in dedicated fiber applications 85
Figure 39 - ST Connector 87
Figure 40 - SC Connector 87
Figure 41 - FC Connector 88
Figure 42 - LC Connector 88
Figure 43 - MT-RJ Connector 89

Figure 44 – Analog Microwave FDM Carrier System 90
Figure 45 - Typical digital microwave system 91
Figure 46 - Microwave propagation and multi-path delay impairment 92
Figure 47 - Space diversity (left) and Frequency diversity (right) 92
Figure 48 – TCP / IP Layers 96
Figure 49 – Location of TCP/IP and Communication Protocols within the OSI model Stack 96
Figure 50 – Example of Ethernet Frame Hierarchy 97
Figure 51 – OSI Model Ethernet 100
Figure 52 – The Ethernet Packet 102
Figure 53 – Example of Ethernet Packet in Actual Orientation 103
Figure 54 – Unshielded twisted pair 105
Figure 55 – RJ-45 Connector 106
Figure 56 – MAC Address Format 108
Figure 57 – Example of a Spanning Tree Ethernet Network 112
Figure 58 – Spanning Tree in a Mesh Network 112
Figure 59 – Spanning Tree in a Ring 113
Figure 60 – Example of an LACP based Ethernet connection between switches 113
Figure 61 – VRRP Example 115
Figure 62 – Cascade topology in the substation [9] 117
Figure 63 – Ethernet star topology in the substation [9] 118
Figure 64 – Ethernet ring topology in the substation [9] 119
Figure 65 – Star/ring hybrid topology tolerant to link and core node faults [9] 120
Figure 66 – HSR example for a ring multicast traffic. 127
Figure 67 – OSI Model for Modbus TCP 133
Figure 68 – IEC61850 approach to standardization 142
Figure 69 – Organization of Logical device, logical nodes, data classes and data 143
Figure 70 – Building functions from multiple logical nodes 143
Figure 71 – Message communication OSI-7 stack 144
Figure 72 – Reference model for information flow in the configuration process 146
Figure 73 – Serial Server in a SCADA Application 148
Figure 74 – RaW Socket Operation 149
Figure 75 – OSI Model of RaW Socket TCP/IP 150
Figure 76 – RaW Socket Packatization 151
Figure 77 – Modbus Operation 151
Figure 78 – Modbus Serial - Link Layer 152
Figure 79 – OSI Model of Modbus TCP/IP 153
Figure 80 – TCP Modbus Application Data Unit (ADU) 154
Figure 81 – MODBUS Master-Slave Connection 155
Figure 82 – Gateway in a SCADA Application 156
Figure 83 – IEEE 1588 Hardware Device Diagram 159
Figure 84 – Inter-device timestamp movement for PTP 160
Figure 85 – IEEE 1588 v2 Overall PTP Network Example with Transparent Clocks 161
Figure 86 – IEEE 1588 v1 Boundary clock example 161
Figure 87 – Basic PTP Synch Message Operation 162
Figure 88 – PTP Message Interaction with Ethernet Switch 163
Figure 89 – PTP Applied for Process Bus Time Synchronization 164

Figure 90 – Time Synchronization Methods 165
Figure 91 – PLC System Diagram 166
Figure 92 - Single Phase-to-Ground (Center Phase) Coupling 167
Figure 93 - Phase-to-Phase Coupling 168
Figure 94 - Mode 1 Coupling 168
Figure 95 – Line Trap 169
Figure 96 – Tuning Device Circuit Diagrams 170
Figure 97 – Coupling Capacitor and Line Trap Assembly 171
Figure 98 – Typical Line Tuning Assembly 172
Figure 99 – Line Tuner Circuit Diagram 172
Figure 100 – FSK PLCC Block Diagram 173
Figure 101 – ON/ OFF PLCC Block Diagram 174
Figure 102 – Analog PLCC System Architect Block Diagram 175
Figure 103 – Data / Voice Multiplexing 176
Figure 104 – Typical Analog PLCC Human Machine Interface 177
Figure 105 – Digital PLC Bit Error Rate vs. Signal-to-Noise Ratio Diagrams 177
Figure 106 – Digital PLC System Architect 178
Figure 107 – Typical Digital PLC Human Machine Interface 180
Figure 108 – PLCC Power Network Configuration 181
Figure 109 – Line Noise Diagrams 183
Figure 110 – Drop and Insert System 184
Figure 111 – Pilot wire relay operating current as a function of channel delay at external faults 186
Figure 112 – Interconnecting Relays with Digital Channels 188
Figure 113 – Ping-pong time delay measurement 189
Figure 114 – Channel delay compensation 190
Figure 115 – False differential current due to channel delay error 191
Figure 116 – Permissive Overreach Transfer Trip (POTT) 194
Figure 117 – Permissive Underreach Transfer Trip (PUTT) 194
Figure 118 – Directional Comparison Blocking with non-directional carrier start 195
Figure 119 – Directional Comparison Blocking with directional carrier TX 196
Figure 120 – Directional Comparison Unblocking 197
Figure 121 – Direct Transfer Trip scheme 198
Figure 122 – Control Center Platform Communications 201
Figure 123 – Mapping of communication standards to IEC 62351-xx 205
Figure 124 – Synchrophasor System Components 207

1. Introduction

The objective of this document is to provide protection and control engineers with detailed information on communications technology associated to protective relaying. In order to achieve this goal, we will start by looking back to the time when Protection & Control Engineers did not have to worry too much about understanding communications.

The history of protection and substation automation goes back to the turn of the previous century. [1] The first protection relay was developed in the early years of 1900 while the first installation was made in 1905. The evolution can be divided in three main stages; the first stage was the era of

electromechanical relays, which started over 100 years ago. The next era was static or electronic relays, which were introduced in the 1960s. The present era with microprocessor based relays started in the beginning of the 1980s, where microprocessor performed the logics, but the filtering was analogue. The first fully numerical relay was introduced 1986.

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

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

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

Energy management systems and their associated SCADA need not only more and more bandwidth, but high resilience and flexibility. Many utilities currently implement backup control centers that are geographically remote from the main control facility. Transferring substation connections between control centers in the event of a major incident—or as part of normal operation—makes further demands on the communications network.

Deregulation has split the power delivery system into complementary or competing entities, while growing numbers of specific Information and Communication Technologies (ICT) applications are being dispersed across power networks. It has become critical to have a comprehensive view of the system's status in real time to ensure constant situation awareness and power system stability. A key capability in this respect is a whole spectrum of "wide-area applications" using time-synchronized measurements across the network. These applications rely on telecommunications to enable time-sensitive information exchange between substations, substations and control platforms, and control centers and generating plants.

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

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

telecommunications industry products with modifications made for this industry, such as, surge withstand capability, wide temperature variations, abnormal vibrations, and immunity to electromagnetic, electrostatic and radio interference. This is the case for the protective relaying digital communications systems as well.

In the new era of protection and control, it is very important that protection and control engineers understand digital telecommunication system architecture, since the telecommunications equipment is applied as used in the telecommunications industry.

It is the intention of this document to illustrate the evolution of the communications for protection and control which through the years, has gone through several transformations as follows:

- From serial communications with data rates of 300 bps to Ethernet communications with data rates of 1,000 Mbps
- From maximum distances of 4000 ft or 1200 m using serial cables to 70 km and longer using optical fiber cables
- From one-to-one or master-slave communications to one-to-multiple clients and peer-to-peer communications
- There was a migration from serial communications RS-232, RS-485 or RS422 to Ethernet
- The type of connectors also went through changes as well. They went from DB9 or DB25 type serial communications to RJ45, ST, SC, LC and MTRJ connectors for Ethernet
- To cope with the demands for reliability in harsh environments, distance and data through put, fiber optics came to replace twisted copper wires
- The need for intelligent networks, hubs were replaced by managed switches
- A variety of proprietary and open communications protocols have been introduced, each one with its own set of rules for data representation, signaling, authentication and error detection, including features intended to ensure reliable interchange of data over an imperfect communication channel
- IEC 61850, a standard for the design of electrical substation automation, was introduced to allow the interoperation of devices from different vendors. An IEC project group of about 60 members from different countries worked in IEC working groups from 1995 and the objectives set for the standard were:
    - A single protocol for complete substation considering modeling of different data required for substation.
    - Definition of basic services required to transfer data so that the entire mapping to communication protocol can be made future proof.
    - Promotion of high interoperability between systems from different vendors.
    - A common method/format for storing complete data.
    - Define complete testing required for the equipment which conforms to the standard.
- Access to information is much easier with the use of Ethernet networks

Protection and Control engineers and technicians are now considering communications as an important component of the Power System and it has become necessary to be understood.

1.1 The Introduction of Digital Communications

Digital Communications started as an evolutionary change from Amplitude Modulated signaling to little ones and zeros, bits in a stream; binary communication. This provided a data condition that was better able to handle changes in signal strength and noise due to the data being the pulse itself and not the amplitude of the pulse. It also brought the ability to bring together multiple messages into a single digital bit steam using a process known as multiplexing.

Almost all modern-day communications architectures use the same communication model known as the Open Systems Interconnect (OSI) Model described in *Section 9.0 OSI Protocol Model* below. They may not use all the layers, but they all use some to provide the necessary structure to send data from a source to a destination through the transmitter, channel and receiver. Further definitions of Digital Communication will be in a later chapter.

The overall purpose of the digital communication system is to collect information from the source and carry out necessary electronic signal processing such that the information can be delivered to the end user (information sink) with acceptable quality.

While error free transmission of information can never be guaranteed, 'acceptable quality' close to error free transmission is possible. This 'possibility' of almost error free information transmission in digital communication systems has driven significant research over the last five decades in multiple related areas such as digital encoding and modulation, error control and correction, modeling and characterization of channel.

In the simplest form, a digital transmission-reception system is a three-block system, consisting of:

1. Transmitter (encoder)
2. Channel (transmission medium)
3. Receiver (decoder)

In protection and control, these three concepts started with the introduction of Remote Terminal Unit (RTU) and Programmable Logic Controller (PLC) as described in *Section 1.2 Data Communications for Protection and Control*. The intention of this document is to provide details on how communications have transformed and continue transforming to date.

1.2 Data Communications for Protection and Control

In the protection and control world, the source of information data has evolved with time. If electromechanical relays and meters are used to monitor, protect and control the power system, they will be connected to Current and Voltage Transformers and their way of communicating is via a meter dial or via auxiliary contacts which are connected to other devices designed to provide the corresponding audio / visual information. In the past, such information was available locally via the meter's dial, the local annunciator, and horn. The operator was responsible to communicate events to other stake holders. A similar approach was followed after the introduction of electronic (static) single function relays that followed.

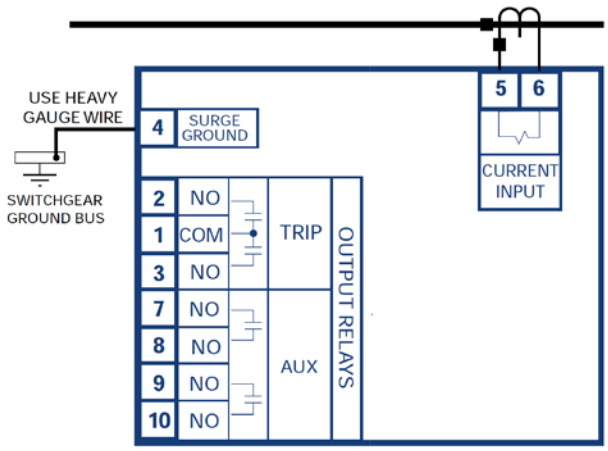


Figure 1 – Typical Electromechanical Relay Diagram

The need for information in real time to improve productivity and to reduce operation cost has been the driving factors for the introduction of new technologies that allow the collection and transmission of data. With this in mind and to expedite the availability of information to other stake holders, the RTU and PLC are introduced.

An RTU is a microprocessor controlled electronic device which interfaces objects in the physical world to a distributed control system or SCADA (supervisory control and data acquisition system) by transmitting telemetry data to the system and/or altering the state of connected objects based on control messages received from the system.

A PLC is a digital computer used for automation of electromechanical processes. PLCs are used in many industries and machines. Unlike general-purpose computers, the PLC is designed for multiple inputs and output arrangements, extended temperature ranges, immunity to electrical noise, and resistance to vibration and impact. Programs to control process operation are typically stored in battery-backed or non-volatile memory.

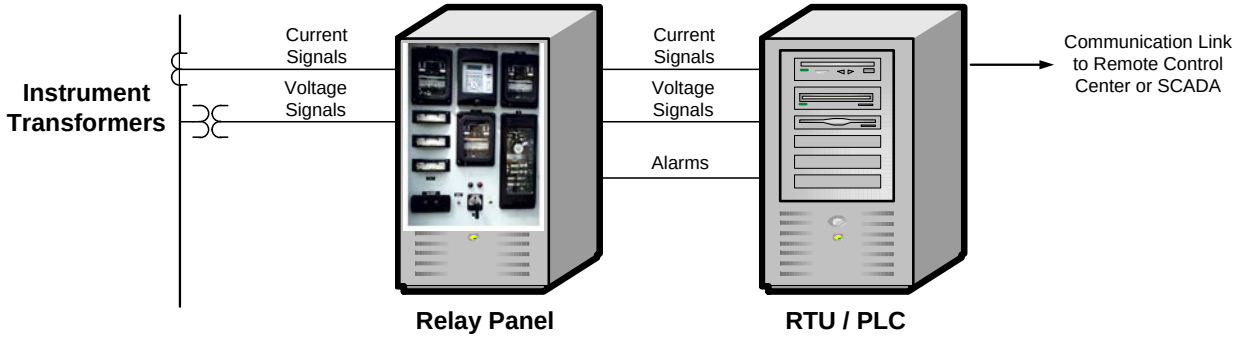


Figure 2 – The Introduction of RTUs / PLCs

RTUs and PLCs are fitted with interfacing equipment such as transducers and multiple Inputs / Outputs (I/Os) to collect information which is digitized and transmitted to remote locations such as

control centers. Current and voltage signals are collected directly from the instrument transformers and additional information such as trips and alarms are collected from the relays via the I/O cards.

RTUs and PLCs allow remote control centers to receive information via some means of communications link. The remote control center is where the SCADA system is located.

With RTUs and PLCs, serial communication becomes the communications technology of choice and with it protection and control engineers and technicians face the need to understand unfamiliar concepts such as communications media (type of cable, connectors), installation issues to minimize noise interference, data baud rate, and communication protocols (Modbus RTU, Profibus, DeviceNet, ASCII, proprietary protocols, etc.)

In this new communications system, the transmitter and receiver are in the equipment responsible to exchange information between the substation and the remote control center where the SCADA is located. At the substation end, the communications link starts at the RTU using any one of the following communication systems:

- Power Line Carrier
- Dial up connection using the telephone network through Modems
- Synchronous Optical Network (SONET) system
- Ethernet Local Area Network (LAN)

At the SCADA location, the communications link ends at the SCADA master computer which can also be connected to one of the above communication systems.

In North America, SCADA refers to a large-scale, distributed measurement and control system, while in the rest of the world SCADA may describe systems of any size or geographical distribution. SCADA systems are typically used to perform data collection and control at the supervisory level. Some systems are called SCADA despite only performing data acquisition and not control.

A SCADA system includes input/output signal hardware, controllers, human machine interface (known as HMI), networks, communication, database and software.

The term SCADA usually refers to a central system that monitors and controls a complete site or a system spread out over a long distance (kilometers/miles). The bulk of the site control is actually performed automatically by a RTU or by a PLC. Host control functions are almost always restricted to basic site over-ride or supervisory level capability. For example, a PLC may control the starting sequence of a power generator, but the SCADA system may allow an operator to change the control set points for voltage and frequency, and will allow any alarm conditions such as over-voltage or under-frequency to be recorded and displayed. The feedback control loop is closed through the RTU or PLC; the SCADA system monitors the overall performance of that loop.

Data acquisition begins at the RTU or PLC level and includes meter readings and equipment statuses that are communicated to SCADA as required. Data is then compiled and formatted in

such a way that a control room operator using the Human Machine Interface (HMI) can make appropriate supervisory decisions that may be required to adjust or over-ride normal RTU (PLC) controls. Data may also be collected into a Historian, often built on a commodity Database Management System, to allow trending, sequence of event reports, waveform capture, and other analytical work.

SCADA systems typically implement a distributed database, commonly referred to as a tag database, which contains data elements called tags or points. A point represents a single input or output value monitored or controlled by the system. Points can be either "hard" or "soft". A hard point is representative of an actual input or output connected to the system, while a soft point represents the result of logic and math operations applied to other hard and soft points. Most implementations conceptually remove this distinction by making every property a "soft" point (expression) that can equal a single "hard" point in the simplest case. Point values are normally stored as value-timestamp combinations; the value and the timestamp when the value was recorded or calculated. A series of value-timestamp combinations is the history of that point. It is also common to store additional metadata with tags such as: path to field device and PLC register, design time comments, and even alarm information.

Since about 1998, virtually all major PLC manufacturers have offered integrated HMI/SCADA systems, many of them using open and non-proprietary communications protocols. Numerous specialized third-party HMI/SCADA packages, offering built-in compatibility with most major PLCs, have also entered the market, allowing mechanical engineers, electrical engineers and technicians to configure HMIs themselves, without the need for a custom-made program written by a software developer.

Advances in the electronic technology facilitated the introduction of numerical relays, a new generation of multifunction protection and control devices that combine multiple protection function in one device able to communicate directly to the RTU, PLC, or other devices and gateways.

The numerical relays exchange information with the substation data concentrator i.e. RTU, PLC or Gateway known as Level 1 Communication. The Level 1 communications link starts at the numerical relays using any one of the following communication systems:

- Serial communication RS-232, RS-485 or RS422
- Ethernet communication via RJ45 or fiber optic cables

The second level of communications is established between the data concentrator at the substation and the remote control center. At the substation end, the communications Level 2 link starts at the data concentrator using one of the following communication systems:

- Power Line Carrier system
- Dial up connection using the telephone network via Modem
- The SONET system
- Ethernet LAN

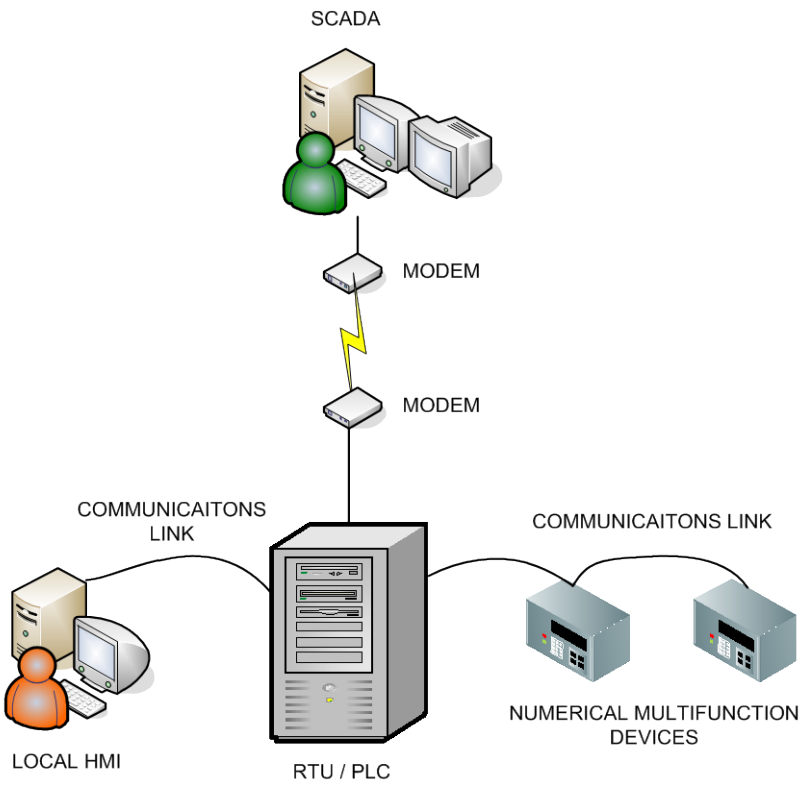


Figure 3 – Numerical Relays Communication Example

At the SCADA end, the communications link ends at the SCADA master computer which can also be connected to one of the above communication systems.

As the amount of data transfer increases due to the number of devices communicating data, additional communication assisting devices are needed to increase efficiency and to speed up the transfer of information from the relays to the master control center or SCADA. Gateways and communication processors are introduced in the communication systems to take care of the following challenges:

- Protocol conversion
- Communication between devices and system components
- Support for legacy devices and control centers
- Equipment monitoring and control (I/O)

Gateways and communications processors do not address other challenges introduced by the dramatic increase of data interchange between the substation equipment and the SCADA, newer protocols such as IEC 61850 that enable communication between protection and control devices without the intervention of a master control system, and the limited access to information by multiple clients. Although there are several LAN technologies, Ethernet is predominantly being used in the substation environment. With the advent of the Utility Communications Architecture (UCA), and its standardization by IEC 61850, new and more advanced functions have been added to this local communication interface, and its field of applications has been extended from the

communication room to the bay level and switchyard. For more details, refer to *Section 15 Ethernet* and *Section 18 Serial to Ethernet Conversion*.

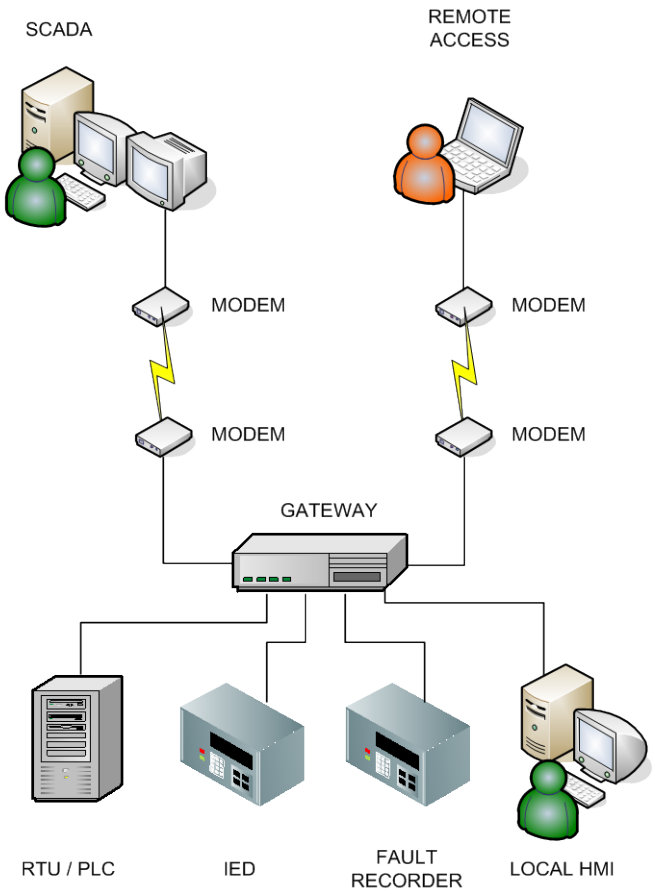


Figure 4 – Introduction of the Gateway

As it will be described later on in this report, protection and control engineers have to adopt Ethernet technology to address new challenges in Substation Automation as follows:

- Peer-to-Peer Communications
- Multiple Masters
- Client – Server vs. Master – Slave
- Higher data transfer
- Higher bandwidth

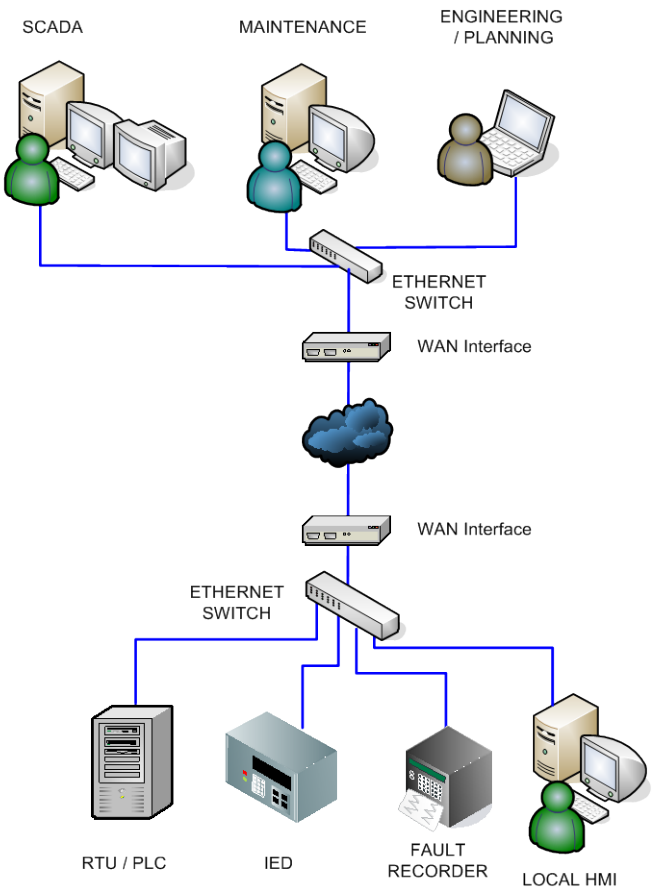


Figure 5 – Ethernet in the Substation

Substation engineers and designers are moving forward accepting and using Ethernet, recognizing its advantages for substation automation applications.

A key requirement of most substations Intelligent Electronic Devices (IEDs) and the Ethernet LAN is that they must operate properly under the influence of a variety of EMI phenomena commonly found in the substation. The new IEC 61850 standard specifies a variety of type withstands tests designed to simulate Electromagnetic Interference (EMI) phenomena such as inductive load switching, lightning strikes, electrostatic discharges from human contact, radio frequency interference due to personnel using portable radio handsets, ground potential rise resulting from high current fault conditions within the substation and a variety of other EMI phenomena commonly encountered in the substation.

IEEE 1613, a standard for "Environmental and Testing Requirements for Communications Networking Devices in Electric Power Substations" goes one step further by defining "Class 2" operation that requires no communications errors, delays or interruptions occur during the application of the type tests.

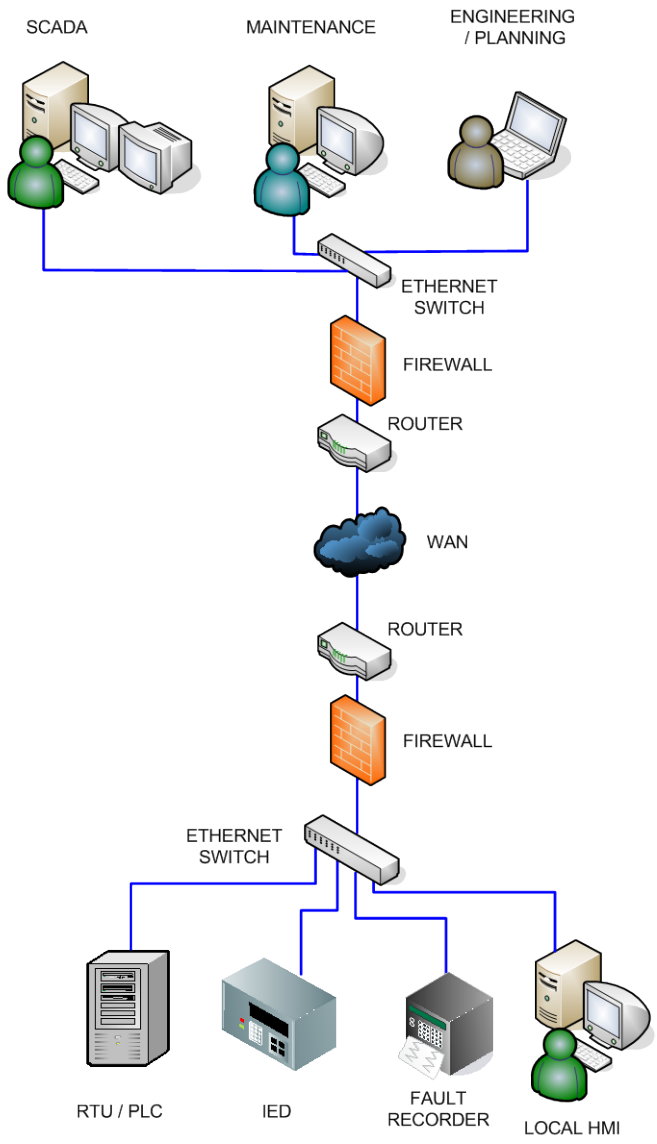


Figure 6 – The router as the interface between LAN and WAN

Often the Ethernet switches will be installed in the same compartment or even on the same rack as protective relaying IEDs. Therefore, it is necessary that the Ethernet equipment be "substation hardened", from an EMI immunity perspective, to the same level as protective relaying IEDs. The need for environmental robustness becomes extremely imperative when a LAN based tripping schemes via Generic Object Oriented Substation Events (GOOSE) is implemented; one lost message could be the difference between success and failure. The designer of the automation system must ensure that Ethernet equipment vendors demonstrate conformance to IEC 61850-3 type tests. What we have briefly covered to this point is the different communication scenarios that can be found in a local area network (LAN) utilized for substation automation and data collection. We have indicated that the data eventually will be transmitted to the SCADA at a remote control center. Station LAN connects all of the IEDs to one another and to a router or other device for communicating outside the substation with wide area network (WAN).There are three basic types of networking:

- LAN (local area network),
- MAN (metropolitan area network)
- WAN (Wide area network).

A wide area network is a geographically dispersed large network. It can be privately owned or rented and it covers a large geographical area such as a city, province or a country.

A wide area network may consist of a multiple LANs or MANs. The world's most popular wide area network in the world is the internet. WANs are the corporate network that utilizes leased lines.

Wide area networks generally utilize much expensive equipment. The main communication technologies that are included in the WAN are SONET, Frame Relay and ATM. The computers that are connected to the WANs are generally connected through the public networks and they can also be connected through the satellites. Covering WAN systems and protocols in full details is out of the scope of this report. Figure 6 shows one possible network showing the router as the interface between the LAN and the WAN.

The need to transmit protection and control data via a communications media introduced a whole lot of new concepts and complexities which will be covered in more details throughout this report.

1.3 Substation Automation Examples

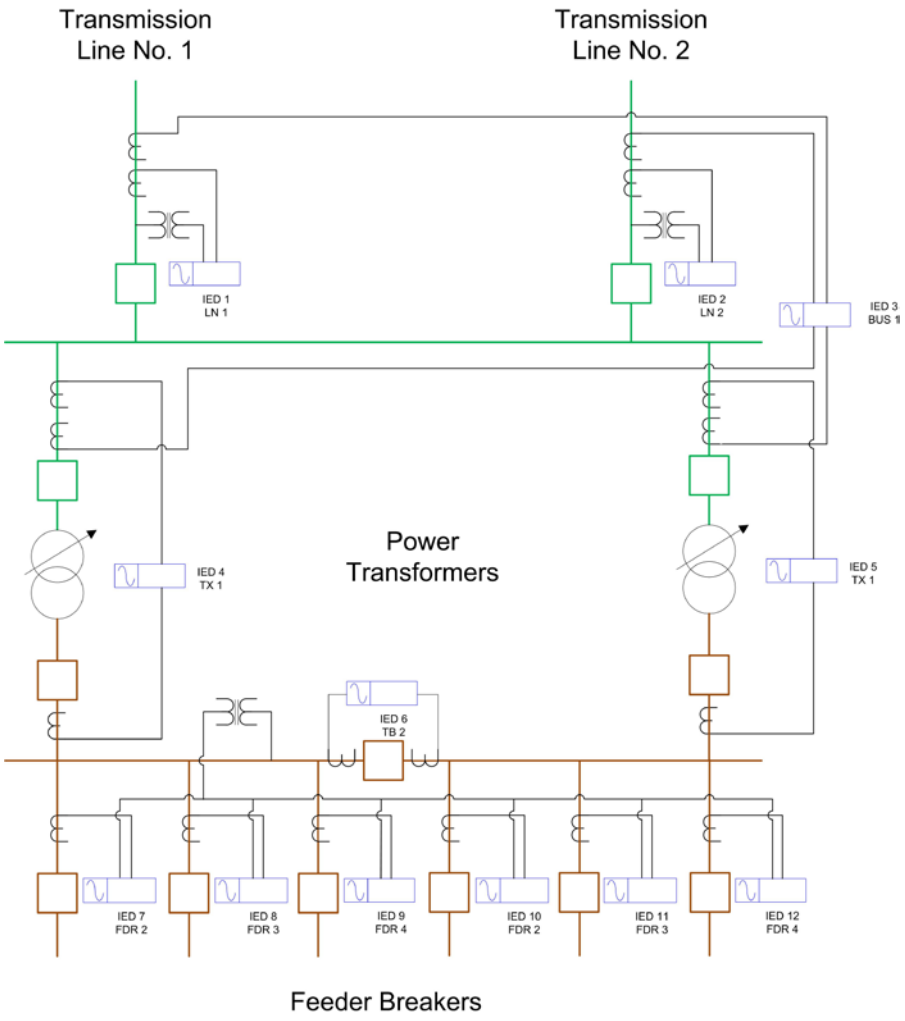


Figure 7 - Substation Single Line Diagram

In this section, we will provide some examples of communications systems found in modern substations, showing possible scenarios based on the different technologies described in Section1.2 Data Communications for Protection and Control.

Each example will make reference to the single line diagram of a typical distribution substation shown in Figure 7.

1.4 Substation Automation with Electromechanical Relays

In cases where the substation is fitted with electromechanical or electronic relays that are not able to communicate, an intermediate device such as an RTU or a PLC is installed to collect information such as:

- Analog Quantities – Current, Voltage, Power, Energy, Frequency
- Relay Alarms
- Breaker Status
- Disconnect Switch status
- Transformer Pressure
- Transformer Temperature
- Transformer Oil Levels
- On Load Tap Changer position
- Breaker Commands – Open / Close
- Disconnect Switch Commands – Open/Close

All this information is collected in an analog format via transducers and input / output cards contained in the RTU or PLC to be digitized and transmitted to the SCADA control center. Figure 8 shows typical connections to the RTU or PLC from instrument transformers, relays, circuit breakers, transformer instruments, etc.

As it was explained in Section 1.2 Data Communications for Protection and Control, the RTU or PLC will utilize any of the following communication systems:

- Power Line Carrier system
- Dial up connection using the telephone network via Modem
- The SONET system
- Ethernet LAN

Once the analog signals, inputs and outputs are connected to the RTU or PLC, the next steps are done to make sure that the RTU and PLC are properly connected to the substation communications system.

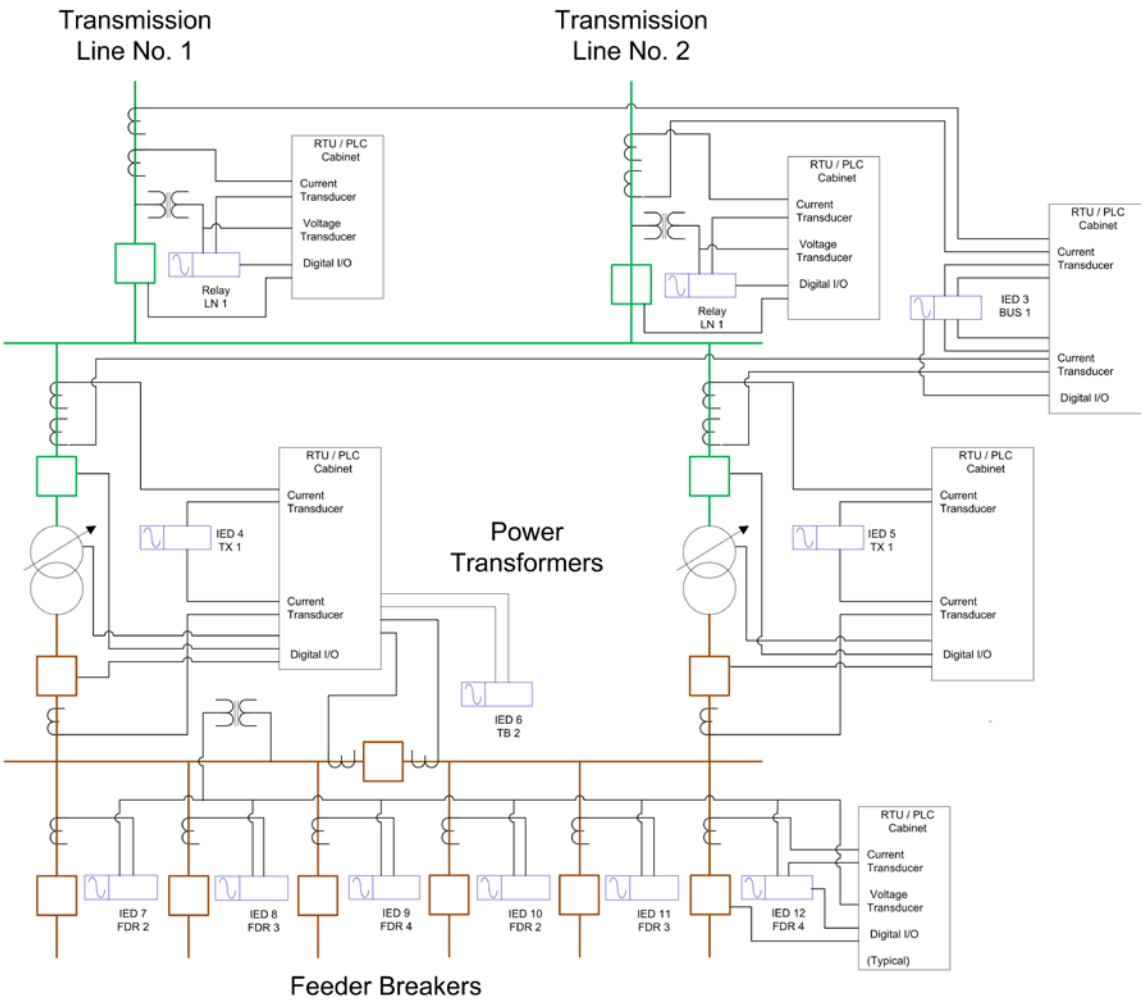


Figure 8 - RTU / PLC Interfaces

If serial communications is chosen, the following should be considered during the design and installation process:

- What type of serial cable will be used between the RTU or PLC and the Power Line Carrier serial port or the Modem that will be the interface to the telephone system or the SONET System? In most cases the serial communication between the RTU or PLC and the communications system is RS-232. For information on Serial Communications RS-232 refer to *Section 11.1 Serial Communications RS-232*, and for information on the electrical interface refer to *Section 11.3.3 RS-232 Electrical Interface*.
- What is the protocol that will be used to communicate the information to the SCADA system? The protocol will depend on the manufacturer of the communications system. For information on protocols refer to *Section 17 Utility Oriented Protocols*.
- In addition to the physical interfaces, there is information such as Slave Addresses, Baud Rates and Parities that may be needed to ensure the communication between the RTU and the Communications Equipment is established.

If Ethernet communications is chosen, take into consideration the following points during the design and installation process:

- What type of Ethernet cable will be used between the IEDs and the Substation Ethernet LAN? There are two options, copper twisted pair or fiber optic cables. The deciding factors can be attributed to distance and environmental interference. For information on Ethernet communications refer to *Section 15 Ethernet*, for information on the electrical interface refer to *Section 15.5 Ethernet OSI Layer 1- Physical Layer*, and for information of fiber optic cables refer to *Section 12 Physical Communication Media- Fiber Optic*.
- What type of connectors will be used? For Unshielded Twisted Pair (UTP) type cables, the connector will be RJ 45. For fiber optics cables, then typically the connector choices are type ST, SC, LC, FC or MT-RJ. For additional information on Ethernet connectors refer to *Section 15.5 Ethernet OSI Layer 1- Physical Layer*, and for fiber option cables and connectors refer to *Section 12 Physical Communication Media- Fiber Optic*.
- What are the Internet Protocol (IP) addresses for the network components? A unique IP address will be assigned to each network component which will be provided by the network administrator.
- How do I assign the IP address to my RTU or PLC? Usually entering the IP address to the RTU or PLC is done either via serial or Ethernet ports using application software running on standard PC. There will be three values that need to be entered:
    - IP Address: For example 192.168.100.44. For additional information about IP address refer to *Section 15.7.2 IP Addressing and Subnetting*.
    - IP Subnet Mask: For example 255.255.255.0. For additional information about IP address and subnetting *Section 15.7.2 IP Addressing and Subnetting*.
    - Gateway IP Address: For example 192.168.100.1. This is the IP address of the router in the substation that will connect to the Wide Area Network (WAN)
- What are the protocols that will be used to communicate the information from the RTU or PLC to the local HMI computer and then to the SCADA system? The protocol will be the one used by the manufacturer of the RTU or PLC. For information on protocols refer to *Section 17 Utility Oriented Protocols*.
- What kind of system will be used for WAN? As described in *Section 1.2 Data Communications for Protection and Control*, the main communication technologies that are included in the WAN are SONET, Frame Relay and Asynchronous Transfer Mode (ATM). A popular WAN technology used for substation automation is SONET; for additional information refer to *Section 10.1 Multiplex Channel, SDH, PDH, SONET*.

1.5 Substation Automation with Numerical Relays

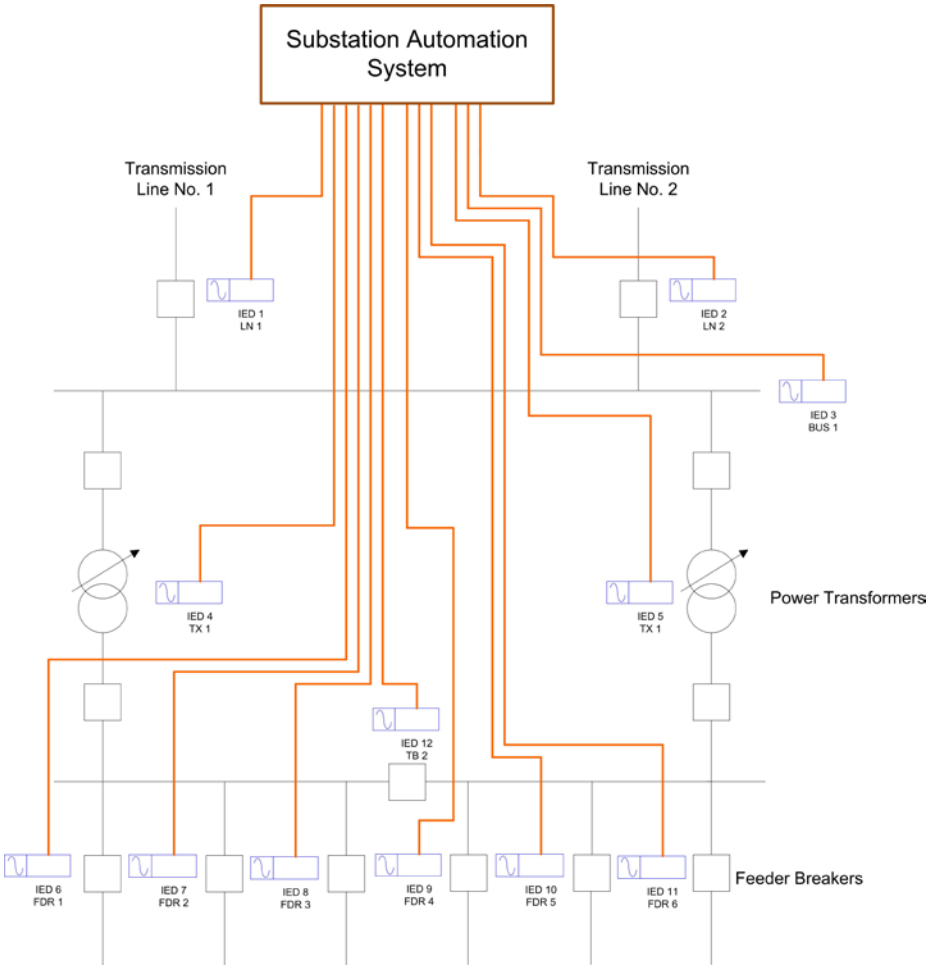


Figure 9 - Substation Automation Communication System

Figure 9 shows a simple diagram of substation IEDs connected to the Substation Automation System. The topology shown in this diagram does not reflect the actual connections, which will depend on the type of communications that will be used i.e. serial RS 232 or RS 485, or Ethernet.

In cases where the substation is fitted with numerical multifunction relays also known as intelligent electronic devices (IED), able to communicate either directly to a Master Computer or via an intermediate device such as RTU, PLC, or Gateway, simply called Data Concentrator. As it was explained in *Section 1.2 Data Communications for Protection and Control*, the communication options are:

- Power Line Carrier system
- Dial up connection using the telephone network via Modem
- The SONET system
- Ethernet LAN

1.5.1 Numerical Relays and Serial Communications RS-232

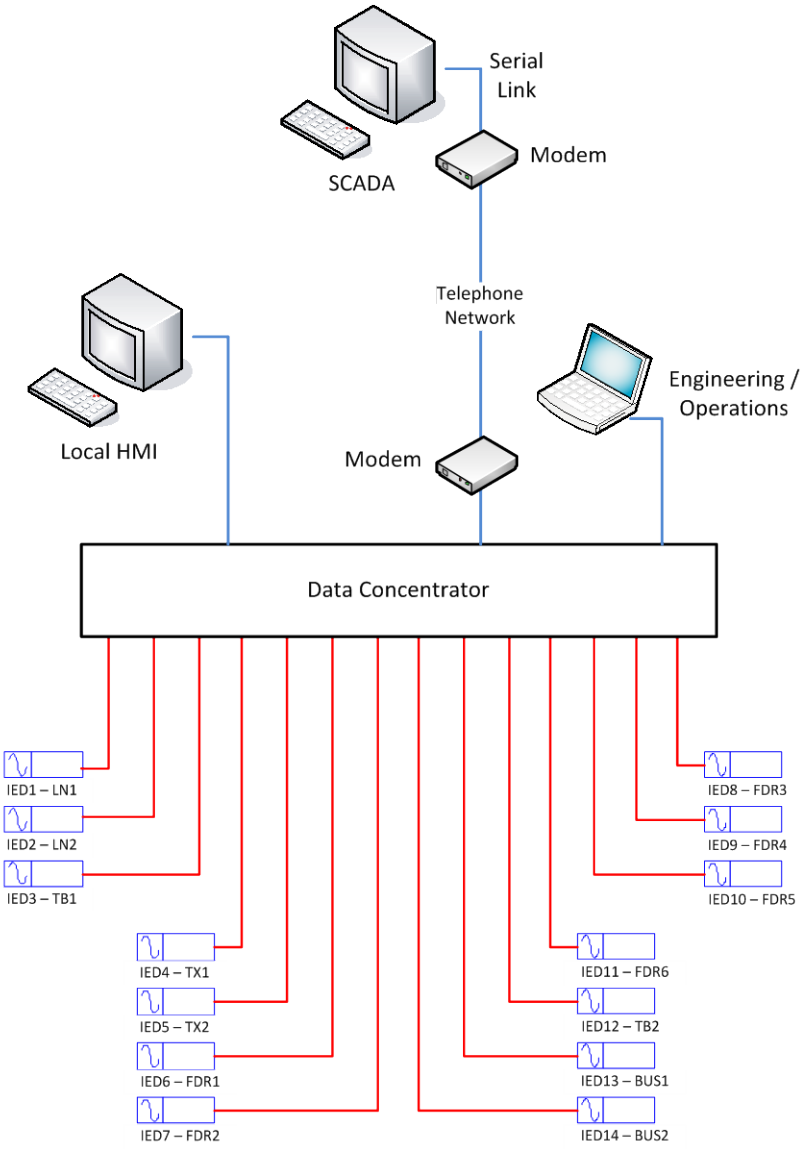


Figure 10 - Substation Network - Serial Communications RS-232

Figure 10 shows a typical network where the IEDs are connected via serial communications RS-232 to a data concentrator.

In order to differentiate between communications taking place locally at the substation versus communications between the substation and the remote control center or SCADA, the local communications between IEDs and the local HMI computer is called Communications Level 1 and communication between the local computer and the remote computer is called Communications Level 2.

In this scenario, the communications Level 1 network is connected in a star topology to the data concentrator and communications Level 2 is also serial communication connected to SCADA via a dial up through modems.

The following should be considered during the design and installation of the substation automation communications network:

- What type of serial cable will be used between the Data Concentrator and the IEDs? In this case it will be a serial cable RS-232. For information on Serial Communications RS-232 refer to *Section 11.1 Serial Communications RS-232*, and for information on the electrical interface refer to *Section 11.3.3 RS-232 Electrical Interface*. Note that some relay manufacturers may specify the connections to the serial connector, which may differ from the standard.
- What are the protocols that will be used to communicate the information from the IEDs to the data concentrator and then to the SCADA system? In a typical substation, Level 1 and Level 2 may not use the same protocol. For information on protocols refer to *Section 17 Utility Oriented Protocols*.
- In addition to the physical interfaces, there is information such as Slave Addresses, Baud Rates and Parities that may be needed to ensure the communication between the RTU and the Communications Equipment is established.

1.5.2 Numerical Relays and Serial Communications RS-485

Figure 11 shows a typical network where the IEDs are connected via serial communications RS-485 to a data concentrator. In this scenario the communications Level 1 network is connected in a daisy chain topology to the data concentrator. Note that in the case of serial communications RS-485, a termination network is installed at the end of the line. The purpose of the terminator network is to eliminate reflections in the communications line.

It can be seen as well that the IEDs are not connected together forming a single daisy chain. The number of IEDs per daisy chain is selected with the objective to expedite data polling. The SCADA integration engineer selects the number of IEDs per daisy chain based on baud rate and the amount of data that will be collected from each IED. In addition, there is a limit on the maximum number of IEDs connected to a daisy chain. RS-485 allows multiple devices (up to 32) to communicate at half-duplex on a single pair of wires, plus a ground wire (more on that later), at distances up to 1200 meters (4000 feet). Both the length of the network and the number of nodes can easily be extended using a variety of repeater products on the market. For more information about RS-485 Serial Communications refer to *Section 11.2 Serial Communications RS-485*.

Communications Level 2 is also serial communication connected to SCADA via dial up through modems. Normally the communication links between the Data Concentrator and the Local HMI, the local modem and the Engineering Computer is done via RS32 connection. For information on Serial Communications RS-232 refer to *Section 11.1 Serial Communications RS-232*, and for information on the electrical interface refer to *Section 11.3.3 RS-232 Electrical Interface*.

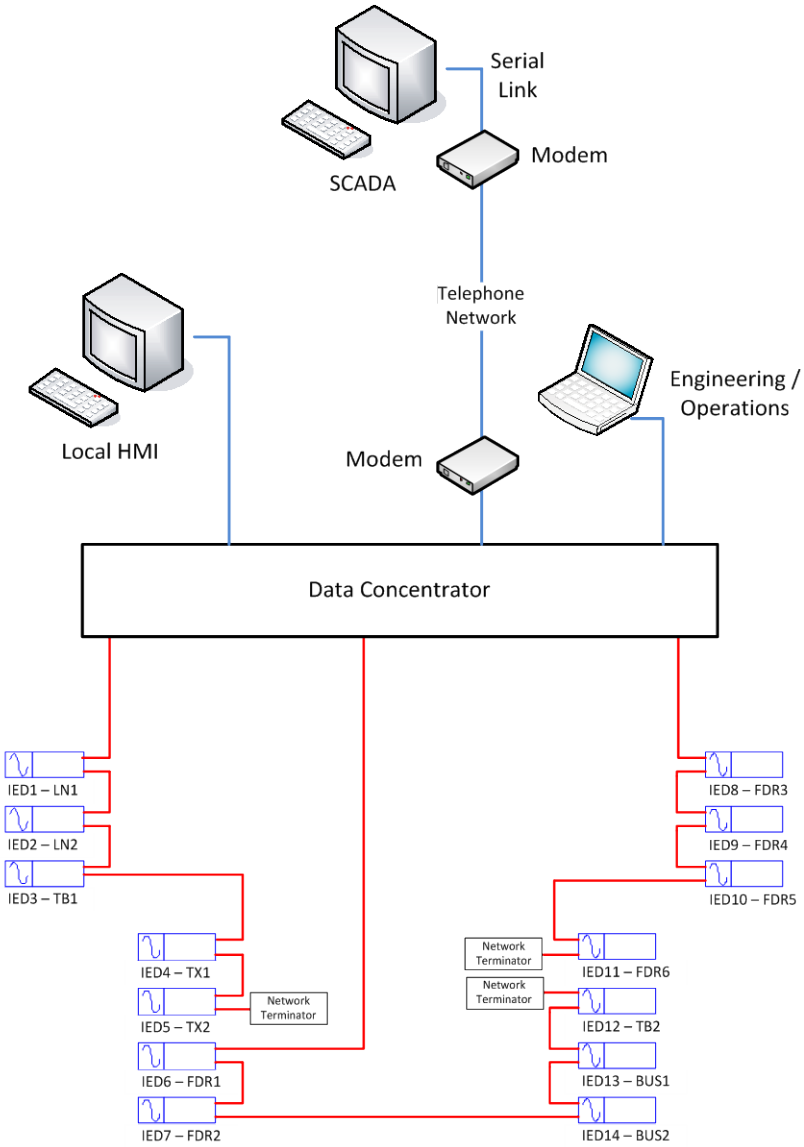


Figure 11 - Substation Network - Serial Communications RS-485

The following should be considered during the design and installation of the substation automation communications network:

- What type of serial cable will be used between the Data Concentrator and the IEDs? In this case it will be a serial suitable for RS-485. For information on Serial Communications RS-485 refer to *Section 11.2 Serial Communications RS-485*. Note that some relay manufacturers may specify the connections to the serial connector, which may differ from the standard.
- What are the protocols that will be used to communicate the information from the IEDs to the data concentrator and then to the SCADA system? In a typical substation, Level 1 and Level 2 may not use the same protocol. For information on protocols refer to *Section 17 Utility Oriented Protocols*.

- In addition to the physical interfaces, there is information such as Slave Addresses, Baud Rates and Parities that may be needed to ensure the communication between the RTU and the Communications Equipment is established.

1.5.3 Numerical Relays and Ethernet Networks

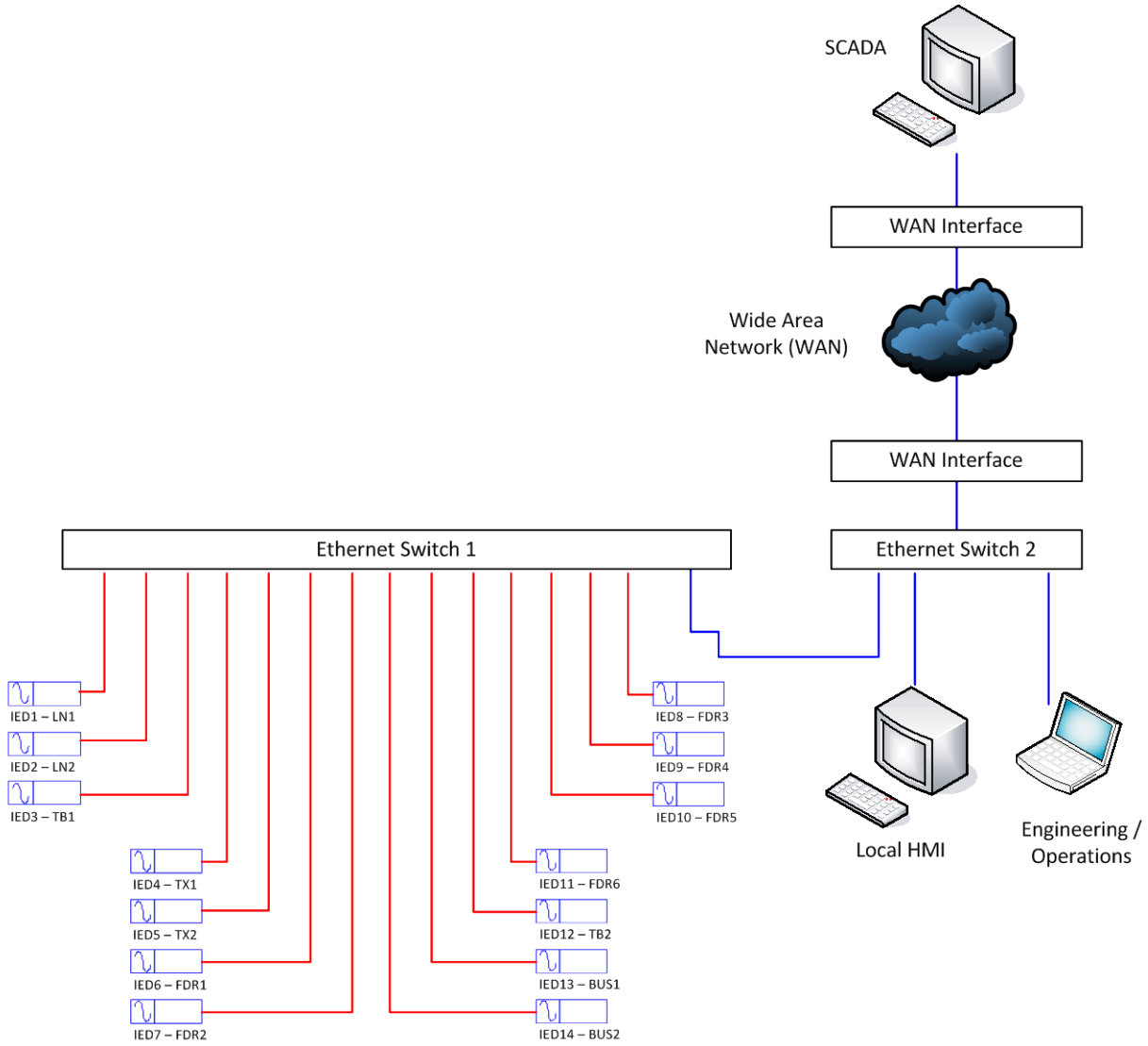


Figure 12 - Basic Ethernet Network

Figure 12 shows a basic schematic where the IEDs are connected to an Ethernet network. In this scenario the communications Level 1 network is connected in star topology to two Ethernet switches. The Level 2 network starts at the second Ethernet switch connected to SCADA via the wide area network.

The complexity of Ethernet networks makes it difficult to describe everything that needs to be considered for the proper design of the Ethernet LAN; however the following guidelines should be followed:

- What type of Ethernet cable will be used between the IEDs and the Substation Ethernet LAN? There are two options, copper twisted pair or fiber optic cables. The deciding factors can be attributed to distance and environmental interference. For information on Ethernet communications refer to *Section 15 Ethernet*, for information on the electrical interface refer to *Section 15.5 Ethernet OSI Layer 1- Physical Layer*, and for information of fiber optic cables refer to *Section 12 Physical Communication Media- Fiber Optic*.
- What type of connectors will be used? For cables type UTP, the connector will be RJ 45. For fiber optics cables, the connector type choices are ST, SC, LC, FC or MT-RJ. For additional information on Ethernet connectors refer to *Section 15.5 Ethernet OSI Layer 1- Physical Layer*, and for fiber option cables and connectors refer to *Section 12 Physical Communication Media- Fiber Optic*.
- What are the IP addresses for the network components? A unique IP address will be assigned to each network component which will be provided by the network administrator.
- How do I assign the IP address to my IEDs? Usually entering the IP address to the IEDs can be done via the IED front panel man-machine-interface (MMI) or via either serial or Ethernet ports using application software running on standard PC. There will be three values that need to be entered:
    - IP Address: For example 192.168.100. 44. For additional information about IP address refer to *Section 15.7.2 IP Addressing and Subnetting*.
    - IP Subnet Mask: For example 255.255.255.0. For additional information about IP address and subnetting *Section 15.7.2 IP Addressing and Subnetting*.
    - Gateway IP Address: For example 192.168.100.1. This is the IP address of the router in the substation that will connect to the WAN
- What are the protocols that will be used to communicate the information from the IEDs to the data concentrator or local HMI computer and then to the SCADA system? In a typical substation, Level 1 and Level 2 may not use the same protocol. For information on protocols refer to *Section 17 Utility Oriented Protocols*.
- How can I connect Serial Devices to the Ethernet LAN? There may be cases where some of the IEDs may not have direct connectivity to Ethernet networks; however, they can be connected to the LAN via Serial Terminal Servers as explained in *Section 18 Serial to Ethernet Conversion*.
- What kind of system will be used for WAN? As described in *Section 1.2 Data Communications for Protection and Control*, the main communication technologies that are included in the WAN are SONET, Frame Relay and ATM. A popular WAN technology used for substation automation is SONET; for additional information refer to *Section 10.1 Multiplex Channel, SDH, PDH, SONET*.

2. Analog and Discrete Signals

Analog signals are continuous electrical signals that vary in time as shown in Figure 13. Most of the time, the variations follow that of the non-electric (original) signal. Therefore, the two are analogous hence the name analog.

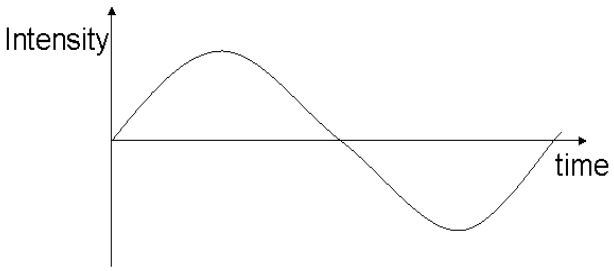


Figure 13 – Analog Signal

Not all analog signals vary as smoothly as the waveform shown in Figure 13. Analog signals represent some physical quantity and they are a 'MODEL' of the real quantity.

Example:

Telephone voice signal is analog. The intensity of the voice causes electric current variations. At the receiving end, the signal is reproduced in the same proportion. Hence the electric current is a 'MODEL' but not one's voice since it is an electrical representation or analog of one's voice.

Discrete signals or digital signals are non-continuous, they change in individual steps. They consist of pulses or digits with discrete levels or values. The value of each pulse is constant, but there is an abrupt change from one digit to the next. Digital signals have two amplitude levels called nodes. The value of which are specified as one of two possibilities such as 1 or 0, HIGH or LOW, TRUE or FALSE and so on. In reality, the values are anywhere within specific ranges and we define values within a given range.

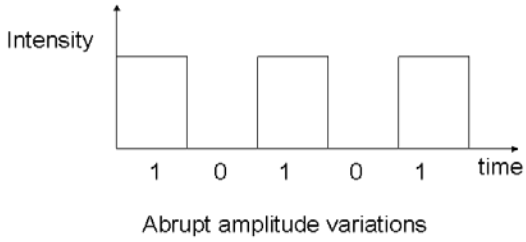


Figure 14 – Digital Signal

There are benefits in moving from analog to digital signaling; some are lower transmission power requirements, greater resistance to bit errors, higher information density, lesser equipment expense, greater differentiation of transmission mediums and greater information security options.

Digital-to-Analog conversion or modulation is the process of changing one of the characteristics of an analog signal based on the information in a digital signal. This is used for telephone modem based transmission to and from the telephone network. This technology is slowly being superseded as digital technology moves further into the Plain Old Telephone System (POTS) space.

Pulse Code Modulation.

Pulse Code Modulation (PCM) is the process by which analog signals are digitally represented. PCM uses four steps to digitize voice. These processes are:

1. Sampling an analog signal: Pulse Amplitude Modulation (PAM)
2. Quantization: assigning integral values
3. Binary encoding: translating into binary values
4. Digital encoding: digital-to-digital conversion known as time division multiplexing (TDM)

The first step in the PCM process is to sample the incoming analog signal at a rate of 8,000 times per second*, a rate sufficient to adequately represent voice information. These sample values are then converted to pulses using a process known as Pulse Amplitude Modulation (PAM).

The next step in the PCM process is to assign a numerical value to the pulse height of each pulse. Once quantized, the pulse height is converted into an 8-bit binary word, with the first bit designating the positive (0) or negative (1) polarity of the pulse.

The last step of the PCM process is to combine (multiplex) the data for transmission over a single communications link.

*To accurately replicate voice in a digital format, the Nyquist Theorem states that the sampling rate must be twice the highest frequency. The highest frequency in the voice band is 4 kHz, so a sampling rate of 8,000 times per second is required. In the PCM process, analog signals are converted into an 8-bit digital word, which is sampled at 8,000 times per second, giving a data rate of 64 Kbps. This is known as a Digital Signal level 0 or DS0.

3. Synchronous communication

Data transfer method in which sent (upstream) and received (downstream) data flows at the same speed, and is spaced by timing signals. Synchronous Transmission is a Data transfer method in which a continuous stream of data signals is accompanied by timing signals (generated by an electronic clock) to ensure that the transmitter and the receiver are in step (synchronized) with one another. The data is sent in blocks (called frames or packets) spaced by fixed time intervals.

In a few words, synchronous communication is direct communication where the communicators are time synchronized. This means that all parties involved in the communication are present at the same time. This includes, but is not limited to, a telephone conversation (not texting), a company board meeting, a chat room event and instant messaging.

Synchronous communications is the more efficient method of communications. One advantage of synchronous is that control information is easily inserted at the beginning and end of each block to ensure constant timing, or synchronization. Another advantage of synchronous is that it is more efficient than asynchronous.

4. Asynchronous communication

Asynchronous communication is transmission of data without the use of an external clock signal. Any timing required to recover data from the communication symbols is encoded within the symbols. The most significant aspect of asynchronous communications is variable bit rate, or that the transmitter and receiver clock generators do not have to be exactly synchronized. Through asynchronous communications, data is transmitted one byte at a time with each byte containing one start bit, eight data bits, and one stop bit, thus yielding a total of ten bits. Asynchronous transmission works in spurts and must insert a start bit before each data character and a stop bit at its termination to inform the receiver where it begins and ends.

Asynchronous communications is the method of communications most widely used for PC communication and is commonly used for e-mail applications, Internet access, and asynchronous PC-to-PC communications. With asynchronous communications, there is a high amount of overhead because every byte sent contains two extra bits (the start and stop bits) and therefore a substantial loss of performance. It does not require that all parties involved in the communication to be present at the same time.

Some examples are e-mail messages, discussion boards, blogging, and text messaging over cell phones. In distance (specifically online) education asynchronous communication is the major (sometimes the only) method of communication. Usually, we use different discussion boards in each class with each having its own purpose. Although all parties may be present at the same time, they don't necessarily communicate in a synchronized fashion. Telephone conversations, board room conversations, and chat sessions are asynchronous in nature due to the fact that each participator can interrupt at any given moment which makes them inherently asynchronous

For example, a 56 Kbps dial-up synchronous line can carry 7000 bytes per second (56000/8) compared to a 56 Kbps dial-up asynchronous line which can only carry 5600 bytes per second (56000/10). When transmitting large amounts of information, this translates into a significant difference in speed and performance.

5. Bit Error and Bit Error Correction

5.1 Bit Errors

Bit error occurs when the data bits that are sent are not the same as the ones that are received. Bit errors can be caused by the transmission media and/or transmitting or receiving equipment problems. The received signal strength, its level, its noise content, and signal jitter are directly related to resultant bit error rate. Elevated equipment temperature, power supply input voltage, high humidity and altitude, etc. may add bit errors. All equipment should have a specified maximum bit error rate (BER) and the conditions that the equipment must operate under to achieve that rate.

Bit errors will result in the protective communication equipment detecting incorrect information. The way that this affects the protective communication equipment's output depends greatly on the equipment design and the end to end communication protocol used. In most cases the equipment

will ignore erroneous bits. If errors occur during the transmission of a command, the result will be either a delayed signal or a missed signal. If the bit errors become excessive the likelihood of false operation increases.

Fiber optic systems are typically engineered to give a typical BER of 10^{-12} with a worse case BER of 10^{-6}. With a BER worse than 10^{-6}, the channel may be considered seriously impaired. A voice application at 10^{-6} BER would not exhibit significant noise but a data application could have serious problems. Fiber optic systems will exhibit bit errors due to electrical and optical malfunctions. Signal rerouting to secondary or protected paths also can cause bit errors.

Most telecommunications systems will operate with a BER at least 10^{-3}. Most teleprotection can operate at BER levels approaching 10^{-3} but dependability and security start to suffer. Teleprotection systems are most susceptible to security problems from bursts of errors and dependability problems from random errors. A burst of errors on a digital channel is more likely to mislead error checking circuitry than a continuous stream of data errors. Random long term errors pose dependability problems because teleprotection tends to have long term squelching to help provide security.

5.2 Bit Error Correction

Definitions of error detection and error correction:

Error detection is the ability to detect the presence of errors caused by noise or other impairments during transmission from the transmitter to the receiver. Error correction is the additional ability to reconstruct the original, error-free data.

There are two basic ways to design the channel code and protocol for an error correcting system:

- Automatic repeat-request (ARQ): The transmitter sends the data and also an error detection code, which the receiver uses to check for errors, and requests retransmission of erroneous data. In many cases, the request is implicit; the receiver sends an acknowledgement (ACK) of correctly received data, and the transmitter re-sends anything not acknowledged within a reasonable period of time.
- Forward error correction (FEC): The transmitter encodes the data with an **error-correcting code** (ECC) and sends the coded message. The receiver never sends any messages back to the transmitter. The receiver decodes what it receives into the "most likely" data. The codes are designed so that it would take an "unreasonable" amount of noise to trick the receiver into misinterpreting the data.

It is possible to combine the two, so that minor errors are corrected without retransmission, and major errors are detected and a retransmission requested. The combination is called hybrid automatic repeat-request.

5.3 Alarms

Generally teleprotection equipment will alarm when BER levels of 10^{-3} are exceeded. At this level the digital receiver produces an Alarm Indication Signal (AIS) of all 'ones'. The teleprotection receiver is designed to recognize this pattern and respond according to user selection.

6. Channel Delay

Channel delay is the sum of the communication electronics and the communication path delays. The equipment delay varies from a few to several hundred microseconds and is of concern for current differential relaying. The speed of light in optical fiber is approximately 70% of the speed of light in air, since its reciprocal, the index of refraction of glass, is 1.4677. Metallic cables generally have a similar velocity. Digital microwave paths propagate at the speed of light in air, resulting in times slightly faster than that of fiber.

Both the actual time delay and delay changes may be of concern. With certain types of Phase Comparison and Directional Comparison equipment, changes in the path delay will have an effect on the relay's ability to determine the proper direction of system faults. Changes in delay are caused automatically by variation in path from path/line switching, or due to operation or design changes. It is very important that the protective relay communication scheme be designed to assure proper operation if any of these changes should occur. If the communication path could be operated in several configurations, the scheme should be checked in each configuration to assure proper operation.

The following table shows the propagation time for various path lengths.

Table 1 Medium Propagation Times (microseconds)

Kilometers	Miles	Fiber	Microwave
1	0.6	4.9	3.3
10	6.2	48.9	33.3
20	12.4	97.8	66.7
50	31.1	244.6	166.7
100	62.1	489.2	333.3
250	155.4	1223.1	833.3
500	310.7	2446.2	1666.7
1000	621.4	4892.3	3333.3

Some protective relay devices now have the ability to self adjust for variations in channel time delay. This type of equipment is desirable for path switched systems. If this feature is not available, separate communication equipment may be needed for each path operated by suitable type of output logic. Note that equipment could misoperate if path switching should occur during a fault.

6.1 Resynchronization

Upon circuit switching, the Bellcore SONET specifications state that resynchronization time may be 60 ms. This is quite acceptable for voice communications and most digital communications. For relaying applications this may be unacceptable, especially during relay fault operation. Several relay channel bank and SONET manufacturers have reduced this time to approximately 10 ms. Fortunately, resynchronization is a rare event. Experience will show how often it occurs at the same time relays are needed to operate.

7. Jitter and wander

As per the ITU-T G.810 standard, jitter is defined as “the short-term variations of the significant instants of a timing signal from their ideal positions in time (where "short-term" implies that these variations are of frequency greater than or equal to 10 Hz).” As for wander, it is defined as “the long-term variations of the significant instants of a digital signal from their ideal position in time (where long-term implies that these variations are of frequency less than 10 Hz).”

Most engineers' first introduction to jitter is viewed on an oscilloscope (Figure 15). When triggered from a stable reference clock, jittered data is clearly seen to be moving in relation to a reference clock.

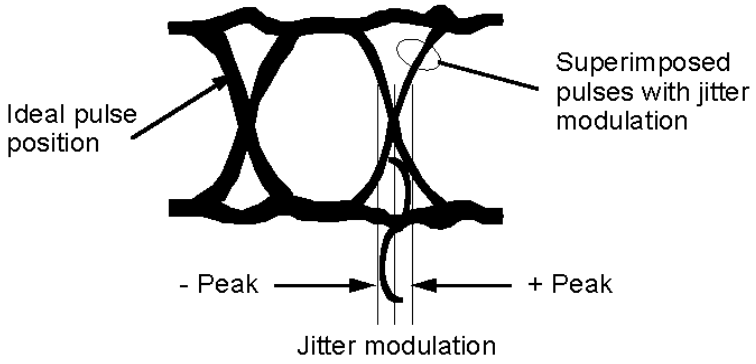


Figure 15 – Jitter as Viewed on an Oscilloscope

In fact, jitter and wander on a data signal are equivalent to a phase modulation of the clock signal used to generate the data (Figure 16). Naturally, in a practical situation, jitter will be composed of a broad range of frequencies at different amplitudes.

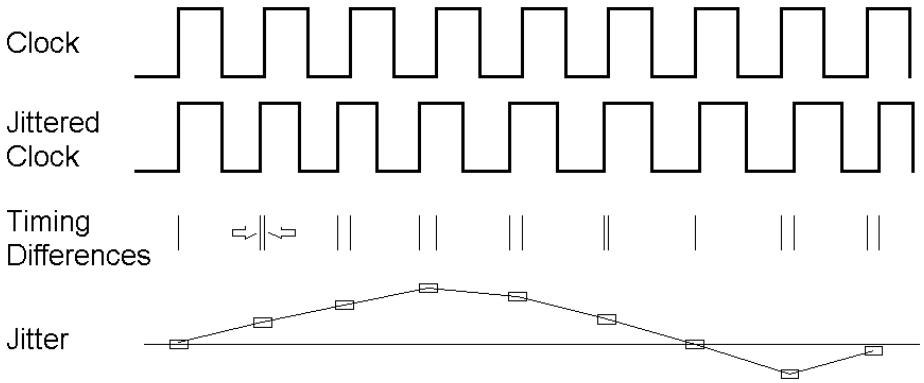


Figure 16 – Phase Variation Between Two Signals

Jitter and wander have both an amplitude: how much the signal is shifting in phase - and a frequency: how quickly the signal is shifting in phase. Jitter is defined in the ITU-T G.810 standard as phase variation with frequency components greater than or equal to 10 Hz whilst wander is defined as phase variations at a rate less than 10 Hz (Figure 17).

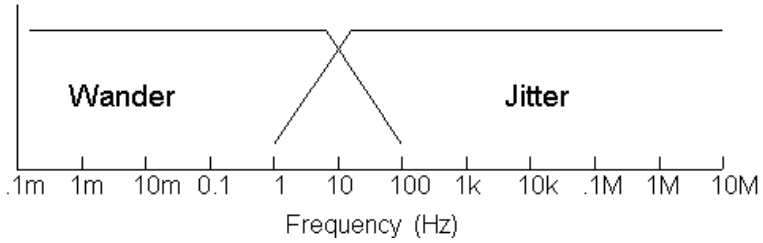


Figure 17 – Frequency ranges of jitter and wander (ref. G.810)

When measuring jitter or wander, always be sure what the reference clock is. By definition, a signal has no phase variation when referenced to itself - jitter or wander always refers to a difference between one timed signal and another.

7.1 Why jitter is important

[4] Error free communications is something every user would like to enjoy. Digital transmission, with its ability to completely avoid cumulative noise-induced degradation, should provide this. One reason for the digital reality not meeting expectations is mis-timing inside transmission equipment when data is regenerated. When mis-timing becomes large, errors are produced and the system can become unusable. Even at low values of mis-timing, sensitivity to amplitude and phase variations is increased and performance suffers.

7.2 Symptoms of Jitter/Wander Issues

Should jitter be at the root of a network problem, the following symptoms would appear:

- Bit errors
- Burst of errors (B1/B2/B3)

- Loss of framing/out-of-frame alarms

Too much wander, on the other hand, can create various problems, depending on the type of signal. The result is unreliable network service, which in turn means higher cost of operation and lower revenues. Here are a few examples of the problems caused by high wander:

- Unreadable characters in faxes
- Sudden click sounds in voice calls
- Data retransmission (lower throughput)
- Lost calls in GSM networks

8. Basic Considerations in Digital Communications

8.1 Speed / Delay

A concern for any communication over digital channels is timing. The speed or bits per second that a system is potentially able to utilize is good to know from the standpoint of how much data is sent per second. Delay is important to note and be aware of due to the time sensitive nature of the data that is typically sent in substation equipment communication.

End-to-end delay- cumulative delay measured for all the interconnecting equipment from the sending port to the receiving port.

Variable delay- as with all equipment, devices handle internal data transmission at different speeds, resulting in variable delay on a per device basis. Variable delay can also be attributed to changes in traffic utilization between devices.

Excessive delay due to intermediate devices- this can be caused by excessive bandwidth utilization at critical junctions within a communications network. This is also known as bottlenecking. This should be monitored as a communications network grows over time.

Asymmetry- the data transmission aspect that there is more traffic heading in one direction versus the other.

Different transmit and receive delay paths- this can happen in communications networks either by design (upstream and downstream links operate at different rates and/or are implemented using different technologies) or unintentionally (damaged network with link loss). Data goes from A to B on one path and comes back from B to A by a different path.

Interruptions- loss of communication due to outages and possible connectivity issues.

Re-synchronization following a switching operation on the network- Can happen under conditions where a redundancy protocol is used to allow the network to automatically heal around a damaged link or equipment. This may require a re-establishment of the data path along a new pathway if there are alternatives.

Figure 18 shows what is considered End-to-End Communications to illustrate the term End-to-End delay as described above.

A concern for relay communications over digital channels is timing issues:

- End-to-end delay
  - Variable delay
  - Excessive delay due to intermediate devices
- Asymmetry
  - Different transmit and receive delay paths
- Interruptions
  - Re-synchronization following a switching operation on the network

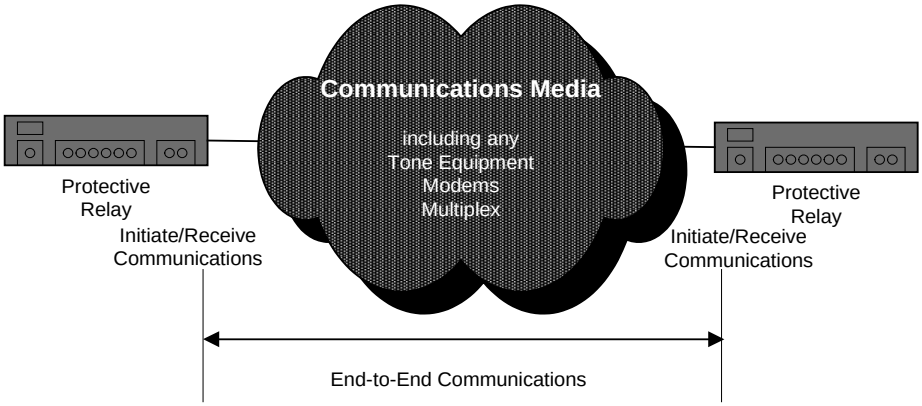


Figure 18 – Pilot relay communication

In SONET systems, the requirements are to detect signal failure within 10 ms and to switch over to a healthy channel in less than 50 ms. During the 10 ms fault detection interval, the multiplexer may deliver erroneous data to the receiving device. The relay securely needs to detect this and block its operation, and discard the faulty data.

The IEC 60834-1 teleprotection standard specifies maximum actual transmission times in the range 15 ms for Direct Comparison Blocking (DCB) to 40 ms for Direct Transfer Tripping (DTT) for analog channels. Digital channels are given 10 ms end-to-end delay. Synchronous digital channels should have no problems fulfilling these requirements, as long as the number of any intermediate devices in the path is minimized. Ethernet channels might require their own discussion.

To establish the total channel delay from one relay terminal to the other, the delays for each possible node (drop and insert) between the locations and the signal delay through the fiber itself (8 μs/mile) need to be considered. Typical SONET ring delays are in the order of 1-2 ms. However, depending on the network's size, topology, and distances, an alternate path might add several millisecond transmission time delay between relays. Still, even the worst case delay should not be a problem for a teleprotection or pilot relay scheme, with the exception of pilot wire relaying which cannot accept longer delays than 1 or 2 ms.

One concern is whether communications network switching results in unequal transmit and receive delays. If there is a risk that the relays can be subjected to asymmetrical delays, the relay performance for this condition should be evaluated.

Change in delays following a path switch is handled by most modern relays as they automatically measure and adjust for actual channel delay. Relays that do not have this ability will suffer degraded performance and might even misoperate as a result of the current from the remote relay being time shifted with respect to the local current.

8.2 Dependability and Security

In addition to high speed data transfer, protective relaying has very high requirements on reliability. Reliability comprises two contradictory components; dependability and security. Dependability and security can be defined as:

Dependability The facet of reliability that relates to the assurance that a relay or relay system will respond to faults or conditions within its intended zone of protection or operation. (The ability of the relay system to trip when it is supposed to trip.)

Security The facet of reliability that relates to the assurance that a relay or relay system will restrain from faults or conditions outside of its intended zone of protection or operation. (The ability of the relay system to refrain from tripping when not required to trip.)

When a digital communications system is used for teleprotection or pilot protection, the dependability and security of the communications network will have to be considered for overall protection system reliability.

The teleprotection standard IEC 60834-1 (1999) provides guidelines for dependability and security (refer to Table 2). The SONET standards define neither. However, as an example, SONET equipment manufacturers often specify availability, which can be translated as (1 – dependability) x 100, expressed in percent.

Table 2 Teleprotection Requirements According to IEC 60834-1

Scheme	Dependability	Security
Blocking (DCB)	$<10^{-3}$	$<10^{-3}$
Permissive Underreach (PUTT)	$<10^{-2}$	$<10^{-4}$
Permissive Overreach (POTT)	$<10^{-3}$	$<10^{-3}$
Intertripping (DTT)	$<10^{-4}$	$<10^{-6}$

8.3 Redundancy

Redundancy is defined as ”the existence of more than one means for performing a given function” [1]. It is obvious that protective relay system dependability can be increased by added redundancy as if one of the systems does not trip for an in-zone fault, a redundant system may. Security on the

other hand, is generally decreased by increased redundancy as there are added devices in the system that may trip when not called upon to do so.

8.4 Reliability and Availability of Communications Networks

From a network communication point of view, reliability and availability are the measures that quantify the ability of the network to perform its required functions, i.e. its ability to transport data from one point to another. Network reliability and availability are required to achieve teleprotection dependability, but are not sufficient.

More formally, the function used to describe reliability is the failure rate noted $\lambda(t)$. The failure rate is usually considered constant for network communication equipment, i.e. $\lambda(t)= \lambda$, and an exponential distribution is used for the reliability and availability analysis. In the IEEE Standard 493, failure rate is defined as the mean number of failures of a component per unit exposure time. Usually exposure time is expressed in years and failure rate is given in failures per year.

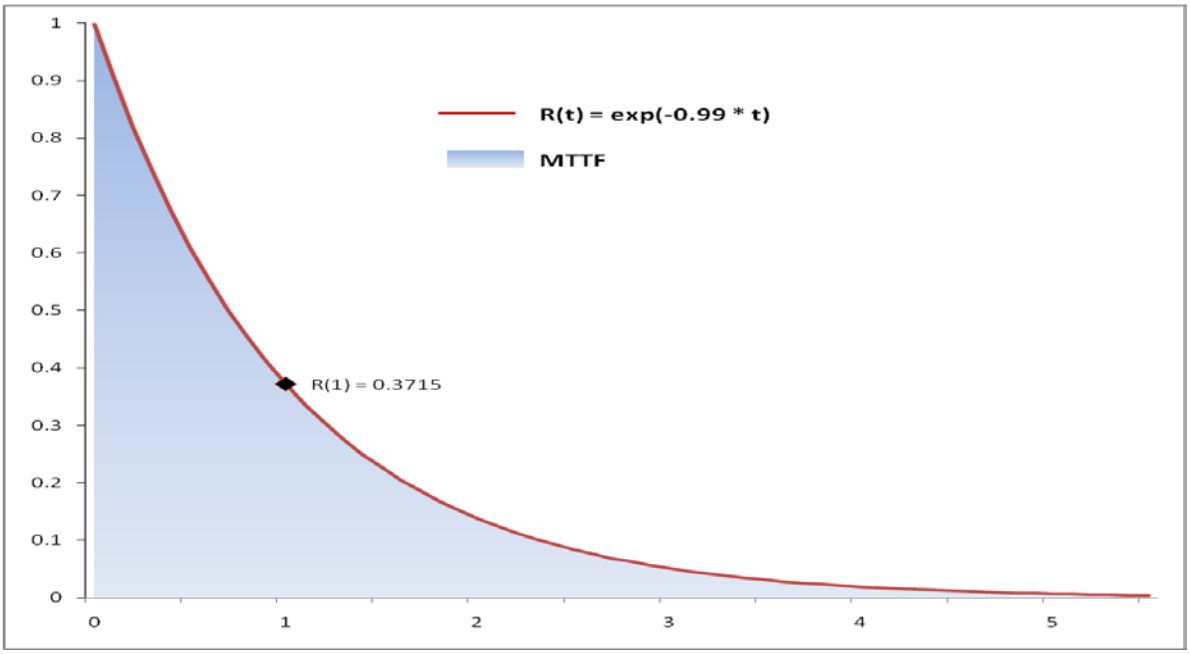


Figure 19 – Representation of a reliability function and MTTF with a failure rate of 0.99

Therefore, reliability function is defined by: $R(t) = \exp(-\lambda.t)$. The reliability function gives the probability of the equipment working at a given time, while the integral of the function defines the mean time to failure, or MTTF. Figure 19 illustrates a reliability function with a failure rate of 0.99. In this example the probability of having the equipment working at t=1 is equal to 37.15%, while the MTTF value is represented by the area covered by the function R(t).

On the other hand, availability of equipment is a ratio defined as: A=MTTF/(MTTF+MTTR), with MTTR representing the mean time to repair of the specific equipment.

Given the reliability figure of the equipment, the reliability of the overall communication network depends on the arrangement of the equipment composing the network. In the case where the equipment components are considered in series, i.e. each equipment needs to be working, then the overall reliability if the product of the reliability of each element: $Rs(t) = \prod Ri(t)$. If the equipment components are considered in parallel, e.g. redundant link or redundant switch, their combined reliability is the sum of both reliability, minus their product: $Rs(t) = R1(t)+R2(t)-R1(t).R2(t)$. From the system reliability, the MTTF of the system can be calculated as presented previously, i.e. by integrating the function. The challenge when calculating the reliability of an overall communication network is to determine which equipment is in series and which one is in parallel (e.g. ring network) and to clearly define the "correct behavior" of the network (e.g. being able to transport from A to B). Reliability analysis is usually performed through a reliability block diagram which is a graphical representation of the series and parallel equipment. Figure 20 illustrates the different stages to calculate the network communication reliability using the reliability block diagram approach.

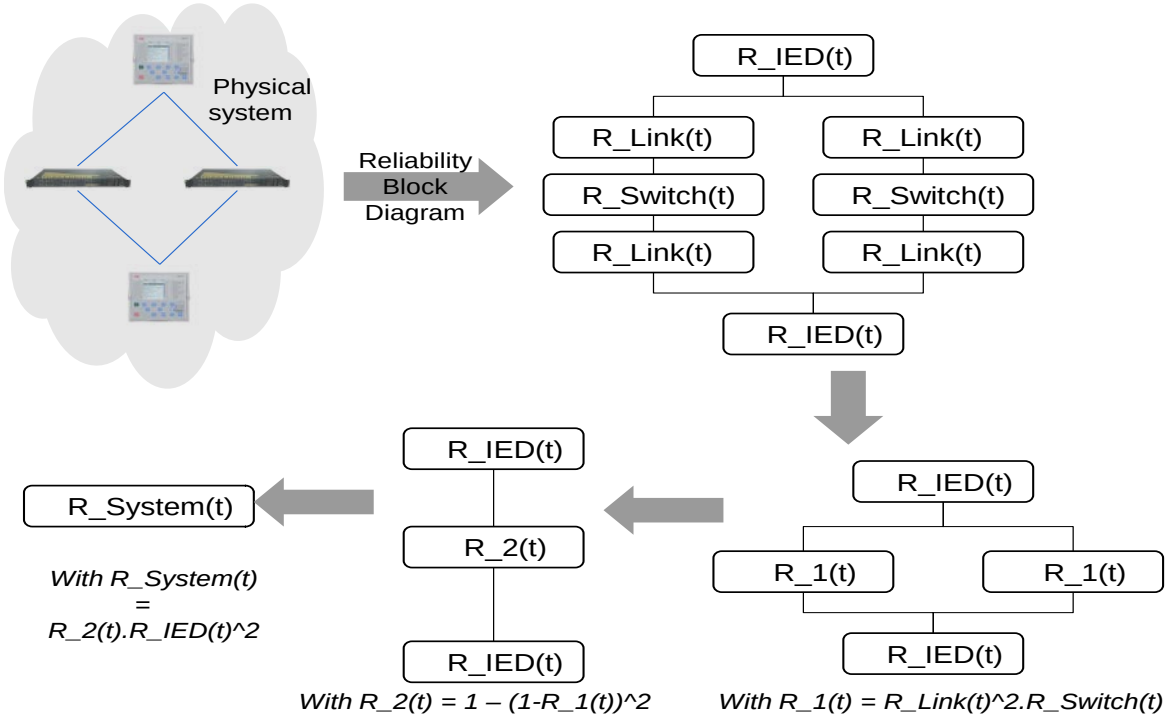


Figure 20 – Illustration of the reliability calculation of the network communication using a reliability block diagram approach.

In Figure 20:

R_IED(t) = Reliability of IED
R_Link(t) = Reliability of Link
R_Switch(t) = Reliability of Switch

System availability is computed from the individual equipment availability using a similar pattern used for reliability: for equipment in series the system availability is equal to: $As = \prod Ai$, while for two equipment in parallel the availability is equal to: As=A1+A2-A1.A2.

Reference – Readers should refer to the standard IEEE 493 (2007) "Design of Reliable Industrial and Commercial Power System" for a more detailed understanding of the reliability topic.

8.5 Noise

Noise is considered to be extraneous potentials tending to interfere with the correct and easy perception of those signals which it is desired to receive.

Noise can come from many sources and affect digital and analog systems differently. The type of communications technology that is employed determines the kinds of methods that may be used to prevent a misoperation of the receiver.

8.5.1 Noise in Digital Circuits

In digital systems, the reliability of data sent over a channel is related to bit errors. In a perfect system data is error free (bits in = bits out). Bit errors occur when the data bits that are sent are not the same as the ones that are received (bits in ≠ bits out). Bit errors can be caused by the transmission media and/or transmitting or receiving equipment problems. The received signal strength, its level, its noise content, and signal jitter are directly related to resultant bit error rate. Elevated equipment temperature, power supply input voltage, high humidity and altitude, etc. may add bit errors.

Bit errors will result in the communication equipment detecting incorrect information. The way that this affects the communication equipment's output depends greatly on the equipment design, communication transport system, and the end to end communication protocol used. In most cases the equipment will ignore or correct erroneous bits by using one of several methods, such as cyclical redundancy checks (CRC), repeating packets, or bit error correction. Bit errors can result in a delayed or missed signal. If the bit errors become excessive the likelihood of false operation increases.

8.5.2 Noise in Analog Circuits

Unlike digital signals that are bits transferred as 1's and 0's, analog communications uses one or several frequencies sent at a particular level, measured in dBm, to transmit data. Noise is the random disturbance or variations of the line by the addition of unwanted frequencies. Noise voltage sensitivity is the level of noise voltage, in dBm, measured at the output of the squelch receiver filter, required to disable the receiver. This is the condition referred to as receiver squelched. The receiver signal level should be well above the background or quiescent noise level, so that the receiver will be secure against operation due to strong impulse noise such as can be generated within the power station or by lightning.

8.5.3 Power system coupled noise

- **Inductive.** This is related to current either in parallel distribution, transmission circuits or control cables in the substation yard. Typically noise is at increased levels at times when the loading is higher on the power system. Twisting of pairs and increasing the distance from the noise sources are solutions. Noise is typically heard as hum at multiples of the power system frequency. Noise at 180 Hz is typically due to three-phase imbalance.
- **Capacitive.** This is related to the electrostatic coupling related to Voltage. The higher the voltage the higher the noise. Distance from the noise source and shielding helps. This noise is generally detected audibly as a sizzling sound although it can cause a measurable circulating current in the shield depending on the drainage connections.

8.5.4 Noise Detection

Typically test equipment or diagnostic capabilities built into the communication equipment will detect, alarm, and log noise on a digital system. There is always some level of noise on an analog pair. Analog noise is often noticeable only when the noise is high enough to disrupt the communication path. Test equipment typically “bridges” onto the analog communication path and may rely on the capabilities of the operator for successful detection.

9. OSI Protocol Model

The Open Systems Interconnect (OSI) reference model is the International Standards Organization (ISO) structure for the “ideal" network architecture. This Model outlines seven areas, or layers, for the network. These layers are (from highest to lowest):

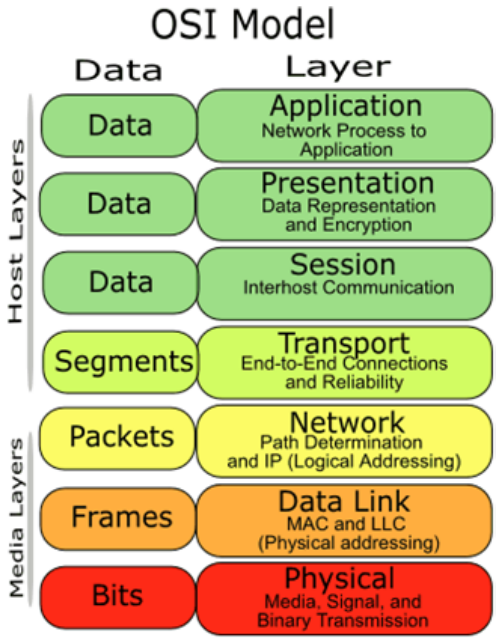


Figure 21 – OSI Model

- ***Layer 7: Applications:*** Where the user applications software lies. Such issues as file access and transfer, virtual terminal emulation, inter-process communication and the like are handled here.
- ***Layer 6: Presentation:*** Differences in data representation are dealt with at this level. For example, UNIX-style line endings (CR only) might be converted to MS-DOS style (CRLF), or EBCIDIC to ASCII character sets.
- ***Layer 5: Session:*** Communications between applications across a network is controlled at the session layer. Testing for out-of-sequence packets and handling two-way communication are handled here.
- ***Layer 4: Transport:*** Makes sure the lower three layers are doing their job correctly, and provides a transparent, logical data stream between the end user and the network service s/he is using. This is the lower layer that provides local user services.
- ***Layer 3: Network:*** This layer provides the functional and procedural means of transferring variable length data sequences from a source host on one network to a destination host on a different network. The Network Layer performs network routing functions, and might also perform fragmentation and reassembly, and report delivery errors. This is the lowest layer of the OSI model that can remain ignorant of the physical network.
- ***Layer 2: Data Link:*** The transmission of the data over the communication medium is the responsibility of this layer. The 0's and 1's that are used in the communication are grouped into logical encapsulation. This encapsulation is called frames. The data link layer provides error-free transfer of data frames from one node to another over the physical layer, allowing layers above it to assume virtually error-free transmission over the link. This layer is generally broken into two sub-layers: The Logical Link Control (LLC) on the upper half, which does the error checking, and the Medium Access Control (MAC) on the lower half, which deals with getting the data on and off the wire.
- ***Layer 1: Physical:*** The nuts and bolts layer. Here is where the cable, connector and signaling specifications are defined.

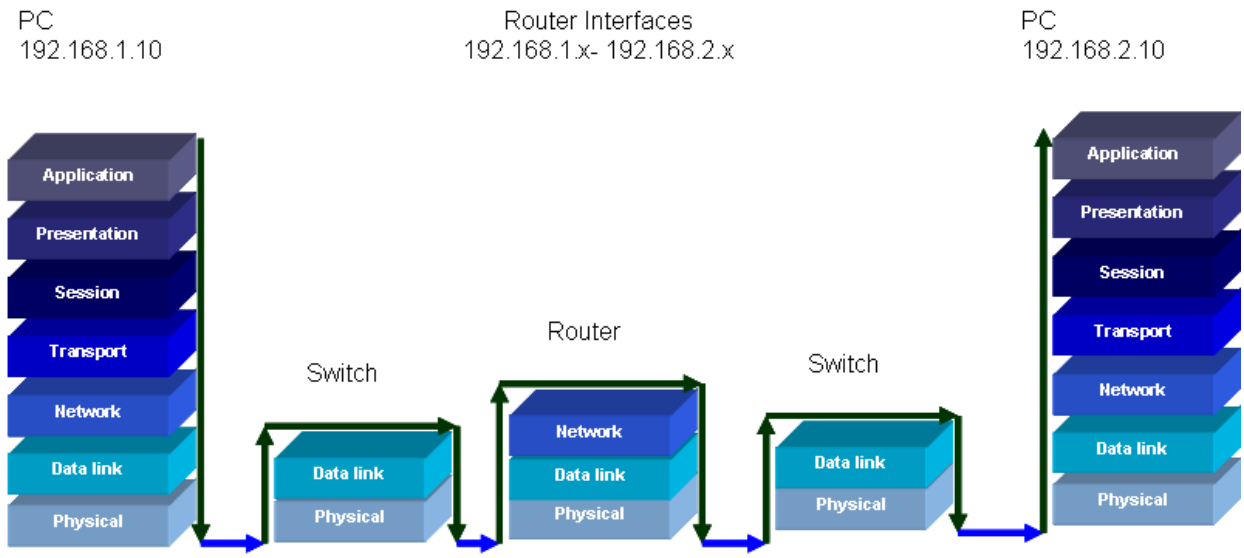


Figure 22 – Example of the OSI Model in Use

10. Multiplex Channel, SDH, PDH, SONET.

10.1 Multiplexing

Multiplexing is the sharing of a communications medium through local combining of signals at a common point. The reverse action of extracting the individual signals from the aggregate at the receiving end is called de-multiplexing. Three basic types of multiplexing are commonly employed: frequency-division multiplexing (FDM), time-division multiplexing (TDM) and code-division multiplexing (CDM).

10.1.1 Frequency Division Multiplexing

With FDM, multiple channels or multiple services are combined onto a single aggregate by frequency translating, or modulating, each of the individual signals onto a different carrier frequency for transmission. The individual channels are thus separated in the aggregate by their frequencies, i.e. each channel has its dedicated frequency slot. At the receiving end, the reverse action of extracting the individual signals is accomplished by filtering. While each user's information signal may be either analog or digital, the combined FDM signal is inherently an analog waveform. FDM is therefore primarily used with analog transmission systems.

10.1.2 Wave Division Multiplexing

With optical fiber systems, a special form of FDM called Wavelength Division Multiplexing (WDM) is increasingly being introduced to further exploit the huge capacity of optical fibers. Several transmission systems, each using a different wavelength or 'color', may be stacked onto the same fiber using WDM. In its simplest form, WDM uses different optical windows for the multiplexing, e.g. the windows centered around 1300 nm and 1550 nm wavelength. More sophisticated systems multiplex a number of optical channels (e.g. 4, 16, 32 or 64) within the same optical window centered round 1550 nm wavelength. As the spacing between the different wavelengths becomes very narrow in this case, the technology is called Dense Wavelength Division Multiplexing (DWDM).

As WDM actually creates 'virtual fibers' it may also be employed for the de-coupling of transmission systems from each other. Dedicated teleprotection links that operate quasi-isolated from other telecom services could be realized using WDM. For example, system 1 could consist of a protection relay with internal or external teleprotection function plus a fiber optic transmitter/receiver operating at wavelength $\lambda 1$. System 2 could be any other fiber-optic communication system operating at wavelength $\lambda 2$ and carrying other services such as data and voice. A failure or malfunction of System 2 should not adversely affect System 1, as the only common parts of the two systems are the optical fiber and the passive optical wave-division multiplexer / demultiplexer.

Although the isolation of the teleprotection from other services by means of WDM appears attractive from an operational point of view, it may not be easily justified for cost reasons.

10.1.3 Time Division Multiplexing

Time Division Multiplexing (TDM) may be conducted through the interleaving of time segments from different signals onto a single shared transmission path. With TDM, multiple channels share the common aggregate based on time. While TDM may be applied to either analog or digital signals, in practice it is applied almost always to digital signals. The digital signals may be interleaved bit-by-bit (bit interleaving), byte-by-byte (byte interleaving) or cell-based where data is broken up into “cells” consisting of a number of bytes. Most modern telecommunication systems employ some form of TDM for transmission over long distance routes. The multiplexed signal may be sent 'directly' (called 'baseband' transmission) over optical fibers, or it may be modulated onto a carrier signal for transmission over analog media, such as microwave radio or coaxial cables for example.

TDM can be split into various subclasses; however, the most commonly used subclass for protection traffic is fixed TDM. In fixed TDM - sometimes also called synchronous TDM - each channel has its assigned timeslot which sustains a fixed data rate and uses aggregate bandwidth irrespective of actual user data being transmitted or not. The number of channels is normally equal to the number of timeslots in a frame. Due to the fixed allocation of channels and timeslots, data can always be transmitted. Buffering and flow control are not required. Continuous data flow at a fixed bit rate without delay variations is ensured, a condition which is generally regarded as a prerequisite for protection signal transmission.

10.1.4 Code Division Multiplexing (Spread Spectrum)

In Code Division Multiplexing (CDM), several signals share a common medium (copper wires or radio waves) using the same frequency band simultaneously. Multiplexing of different channels is achieved by utilizing different pseudorandom binary sequence codes that modulate a carrier. The process of modulating the signal by the code sequence causes the power of the transmitted signal to be spread over a larger bandwidth. Systems based on CDM are therefore sometimes also referred to as 'Spread Spectrum' (SS) systems. The spreading of the spectrum enhances the noise immunity of such systems. CDM and in particular CDMA (code division multiple access) is mainly used with unlicensed spread spectrum radio where many simultaneous users have to share the same frequency band. CDM/SS techniques may also be used with wire-based systems to enhance the transmission capacity and noise immunity. Its application for inter-substation communication would however need to be further examined with respect to cost efficiency and transmission performance.

10.2 Digital Hierarchies

Digital transport systems form the backbone of modern telecommunication networks or Wide Area Networks (WAN). As the demand for information transmission increased and levels of traffic grew higher it became evident that larger number of channels needed to be bundled in order to avoid having to use excessively large number of individual physical links. Thus, it was necessary to define further levels of multiplexing which are structured in digital hierarchies.

10.2.1 PDH - Plesiochronous Digital Hierarchy

Digital telecommunication systems have historically been based on the Plesiochronous Digital Hierarchy (PDH). PDH systems accommodate "almost synchronous" channels in multiples of 64 kbps. The base rate of 64 kbps represents the digital equivalent of an analog telephone channel using traditional, uncompressed Pulse Code Modulation (PCM) speech coding techniques.

When multiplexing a number of digital signals with the same nominal bit rate they are likely to have been created by different pieces of equipment each generating a slightly different bit rate due to their independent internal clocks. A technique called “bit stuffing” is used for bringing the individual signals up to the same rate prior to multiplexing. Dummy bits or justification bits are inserted at the transmit side and discarded by the demultiplexer at the receiving end, leaving the original signal. The same problem with rate alignment occurs at every level of the multiplexing hierarchy. The process of multiplexing “almost synchronous” signals is called “plesiochronous”, from Greek. The use of plesiochronous operation throughout the hierarchy has led to the adoption of the term “Plesiochronous Digital Hierarchy”.

Plesiochronous operation does not allow extracting and inserting individual channels from the aggregate without prior demultiplexing and subsequent re-multiplexing, leaving towers of multiplexers. With the exception of vendor specific solutions, network management and performance monitoring throughout the hierarchy is not adequately supported with PDH systems either, because PDH systems have developed over time with insufficient provision for standardized management. These disadvantages - amongst others - have finally led to the definition of a new digital transmission hierarchy: the Synchronous Optical Network (SONET) in North America or the Synchronous Digital Hierarchy (SDH) in Europe.

There are basically two versions of the PDH systems in use today, one in Europe and one in North America. The European and American versions of the PDH system differ in the detail of their working, but the principles are the same. The North American version of PDH is called North American Digital Hierarchy (NADH). The specifications from the International Telecom Union (ITU) on digital hierarchy match the NADH only in theory and the first digital signal level. From there they deviate in signal rates, management capabilities, line coding, framing and everything else. However, both hierarchies use TDM. In this scheme, a circuit is divided into a continuous stream of time slots and multiple channels are multiplexed into the circuit. Traditionally, each channel was a digitized voice call, but video information and data may also occupy a channel. The basic channel is 64 kbps, which is the amount of bandwidth required to transmit a voice call that has been converted from analog to digital using a sampling rate of 8,000 times per second with the sample represented as an 8-bit value ($8 \times 8{,}000 = 64$ kbps).

Below are tables with the NADH and International digital hierarchy levels and transmission rates. DS stands for Digital Signal, followed by the level. For example DS-1 is digital signal level 1.

Table 3 North American Digital Hierarchy

Signal	Bit Rate	Capacity
DS-0	64 kbps	1 channel

DS-1	1.544 Mbps	24 DS-0 (24 channels)
DS-1C	3.512 Mbps	2 DS-1 (48 channels)
DS-2	6.312 Mbps	4 DS-1 (96 channels)
DS-3	44.736 Mbps	28 DS-1 (672 channels)
DS-4	274.176 Mbps	168 DS-1 (4032 channels)

Table 4 International Digital Hierarchy

Signal	Bit Rate	Capacity
E-0	64 kbps	1 channel
E-1	2.048 Mbps	32 E-0 (30 CH + 1 CH signaling + 1 CH overhead)
E-2	8.448 Mbps	4 E-1 + overhead
E-3	34.368 Mbps	16 E-1 + overhead
E-4	139.264 Mbps	64 E-1 + overhead

10.3 SONET (Synchronous Optical Network) and SDH (Synchronous Digital Hierarchy)

The rapid growth of digital networks and the convergence of telephone and high-speed data networks have enforced the development of new standards, which would facilitate the deployment of complex networks with new services and comprehensive network management options. The new standard appeared first as SONET (Synchronous Optical Network) in the United States.

SONET (Synchronous Optical Network) is a standard for optical telecommunications transport. It was formulated by the Exchange Carriers Standards Association (ECSA) for the American National Standards Institute (ANSI), which sets industry standards in the U.S. for telecommunications and other industries. The increased configuration flexibility and bandwidth availability of SONET provides significant advantages over the older PDH telecommunications system. These advantages include:

- Reduction in equipment requirements and an increase in network reliability
- Provision of overhead and payload bytes – the overhead bytes permit management of the payload bytes on an individual basis and facilitate centralized fault sectionalization
- Definition of a synchronous multiplexing format for carrying lower level digital signals (such as DS1, DS3) and a synchronous structure which greatly simplifies the interface to digital switches, digital cross-connect switches and add-drop multiplexers
- Availability of a set of generic standards which enable products from different vendors to be connected
- Definition of a flexible architecture capable of accommodating future applications, with a variety of transmission rates

In brief, SONET defines optical carrier (OC) levels and electrically equivalent synchronous transport signals (STSs) for the fiber-optic based transmission hierarchy.

10.3.1 Basic SONET Signal

SONET defines a technology for carrying many signals of different capacities through a synchronous, flexible, optical hierarchy. This is accomplished by means of a byte-interleaved multiplexing scheme. Byte-interleaving simplifies multiplexing, and offers end-to-end network management. The first step in the SONET multiplexing process involves the generation of the lowest level or base signal. In SONET, this base signal is referred to as Synchronous Transport Signal level-1, or simply STS-1, which operates at 51.84 Mb/s. Higher-level signals are integer multiples of STS-1, creating the family of STS-N signals in the table below. An STS-N signal is composed of N byte-interleaved STS-1 signals. This table also includes the optical counterpart for each STS-N signal, designated OC-N (Optical Carrier level-N).

Table 5 SONET Digital Hierarchy

Signal	Optical	Bit Rate	Capacity
STS-1	OC-1	51.840 Mbps	28 DS-1s or 1 DS-3
STS-3	OC-3	155.520 Mbps	84 DS-1s or 3 DS-3s
STS-12	OC-12	622.080 Mbps	336 DS-1s or 12 DS-3s
STS-48	OC-48	2488.320 Mbps	1344 DS-1s or 48 DS-3s
STS-192	OC-192	9953.280 Mbps	5376 DS-1s or 192 DS-3s
STS-768	OC-768	39813.12 Mbps	21504 DS-1s or 768 DS-3s

10.3.2 Synchronous Digital Hierarchy (SDH)

Synchronous Digital Hierarchy (SDH) is a standard for telecommunications transport formulated by the International Telecommunication Union (ITU), previously called the International Telegraph and Telephone Consultative Committee (CCITT). SDH was first introduced into the telecommunications network in 1992 and has been deployed at rapid rates since then. It's deployed at all levels of the network infrastructure, including the access network and the long distance trunk network. It's based on overlaying a synchronous multiplexed signal onto a light stream transmitted over fiber optic cable.

Table 6 Synchronous Digital Hierarchy

Signal	**Bit Rate**	**SDH Capacity**
STM-1	155.52 Mbps	63 E1 or 1 E4
STM-4	622.08 Mbps	252 E1 or 4 E4
STM-16	2488.32 Mbps	1008 E1 or 16 E4
STM-64	9953.28 Mbps	4032 E1 or 64 E4
STM-256	39813.12 Mbps	16128 E1 or 256 E4

In brief, SDH defines synchronous transport modules (STMs) for the fiber optic based transmission hierarchy.

SDH embraces most of SONET and is an international standard, but is often mistakenly regarded a European standard, because most of its suppliers carry only the European PDH bit rates specified

by European Telecommunication Standards Institute (ETSI). While there are commonalities between SDH and SONET, particularly at the higher rates, there are significant differences at the lower multiplexing levels, in order to accommodate the requirement of interworking the differing regional digital hierarchies. Through an appropriate choice of options, a subset of SDH is compatible with a subset of SONET; therefore, traffic interworking is possible. Interworking for alarms and performance management is however generally not possible between SDH and SONET systems.

Although SONET and SDH were conceived originally for optical fiber transmission, radio systems exist at rates compatible with both SONET and SDH.

10.3.3 SONET/SDH network topologies and network resilience

A synchronous network will be more reliable than PDH due to both the increased reliability of individual elements, and the more resilient structure of the whole network. SONET/SDH will allow development of network topologies which will be able to achieve 'network protection', that is to survive failures in the network by reconfiguring and maintaining service by alternate means. Network protection can be accomplished by the use of cross-connect functionality to achieve restoration, or through the use of self-healing ring architectures.

Two main types of synchronous ring architectures have been defined:

- The 2-fiber Unidirectional Path Switched Ring (UPSR - SONET) and 2-fiber Sub-Network Connection Protection ring (SNCP - SDH) - This is a dedicated path switched ring which sends traffic both ways around the ring, and uses a protection switch mechanism to select the alternate signal at the receive end upon failure detection.
- The 2 or 4 fiber Bidirectional Line Switched Ring (BLSR - SONET) and 2 or 4-fiber Multiplex Section Shared Protection Ring (MS-SPRing - SDH) - This is a shared switched ring which is able to provide 'shared' protection capacity which is reserved all the way around the ring. In the event of a failure, protection switches operate on both sides of the failure to route traffic through the reserved spare capacity.

Table 7 Logical Equivalence of the Terminology

SONET	SDH
2-fiber Unidirectional Path Switched Ring (UPSR)	2-fiber Sub-Network Connection Protection (SNCP)
2-fiber Bidirectional Line Switched Ring (BLSR)	2-fiber Multiplex Section Shared Protection ring (MS-SPRing)
4-fiber Bidirectional Line Switched Ring (BLSR)	4-fiber Multiplex Section Shared Protection ring (MS-SPRing)

Since ring operation on SONET and SDH has similar concepts, for ease of understanding, we will take a closer look at SONET ring operation

10.3.3.1 SONET GR-1400 2-Fiber Unidirectional Path Switched Ring (UPSR)

A path is the logical connection between points where the information to be transported over SONET is assembled and disassembled or enters and exits the ring. Information entering the ring is bridged at the path (circuit) level and transmitted on both fibers opposite directions around the ring, as depicted in Figure 23. This scheme uses one direction around the ring as the primary signal path and the other direction as the protected path. Switching is based on the health of the path at the circuit level where it exits the ring, as depicted in Figure 24.

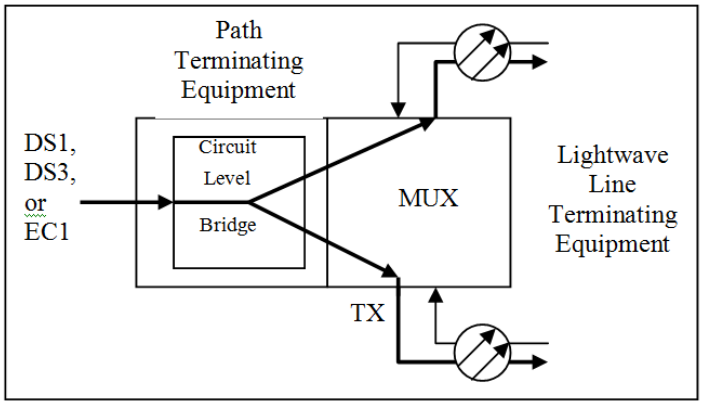


Figure 23 – Path Terminating Equipment Circuit Level

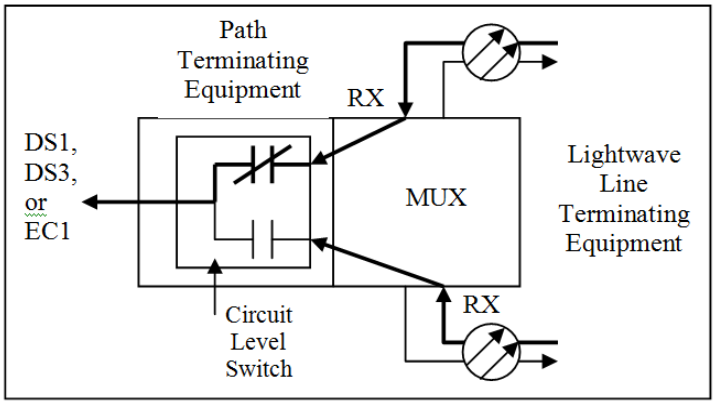


Figure 24 – Path Terminating Equipment Circuit Level Switch

Figure 25 depicts a signal entering a Unidirectional Path Switched Ring (UPSR) topology at node A and dropping out the signal at node B. The primary service path is depicted as the shortest route between the nodes. If a failure occurs between Node A and B, switching to the protection route is done at the individual path (circuit) level at Node B, as depicted in Figure 26.

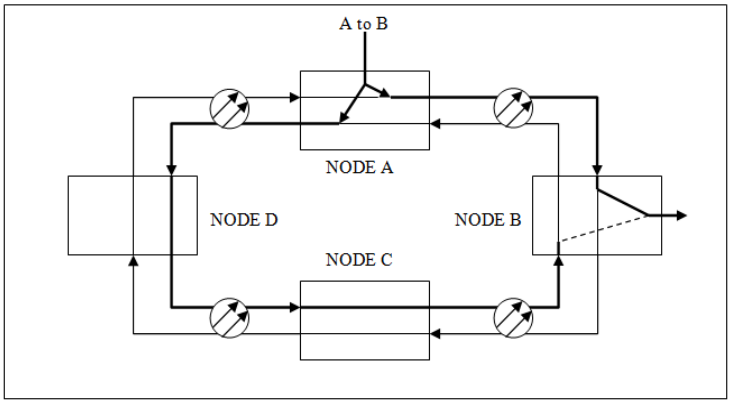


Figure 25 – 2-Fiber Unidirectional Path

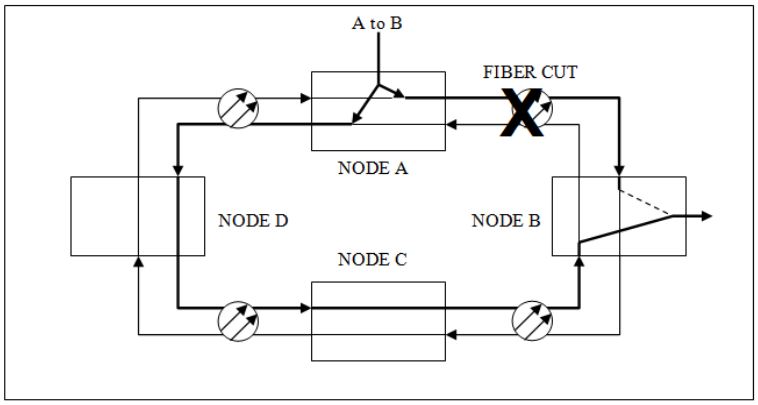


Figure 26 – Protected traffic flow in 2-Fiber UPSR

In summary, the Service and Protection routes are based on a per signal (VT1.5 or STS-1) basis, where if only one VT1.5 or STS-1 fails, the protection path for only that service is selected. All other service paths remain unchanged. The advantage of the UPSR is that the switch threshold is tied directly to the quality of an individual customer's circuit. The UPSR topology is ideal for "Hubbing" or "Central Office" applications where most traffic terminates at one location.

Since each circuit is bridged to transmit both directions around the ring, one time slot is consumed all the way around the ring. Therefore the capacity of a UPSR is independent of the number of nodes and is directly related to the line rate. For example, an OC-1 is equal to or less than twenty-eight VT1.5's or one STS-1. An OC-3 capacity is equal to or less than eighty-four VT1.5's or three STS-1's, and so on. UPSR typically employs non-revertive switching. Since information is sent both ways around the ring, it did not make sense to disrupt the network a second time once the failure was repaired.

10.3.3.1.1 Protective Relaying System Considerations with UPSR

When applying some protective relaying over this type of ring topology, precautions need to be taken. Because most protective relaying is bi-directional in nature, consideration must be given to

applications over a UPSR network. Since switching is determined at the individual path (circuit) level and switches at different nodes are independent from one another, it is possible for transmission from Node A to Node B to take a different route than transmission from Node B back to Node A, as depicted in Figure 27. This can result in an unequal delay in transmit and receive paths of a bi-directional system. Some current differential and phase comparison systems cannot compensate for unequal channel delays between transmit and receive paths. These systems were designed with fixed equal delay compensation and asymmetrical delays could result in false operations or failure to trip.

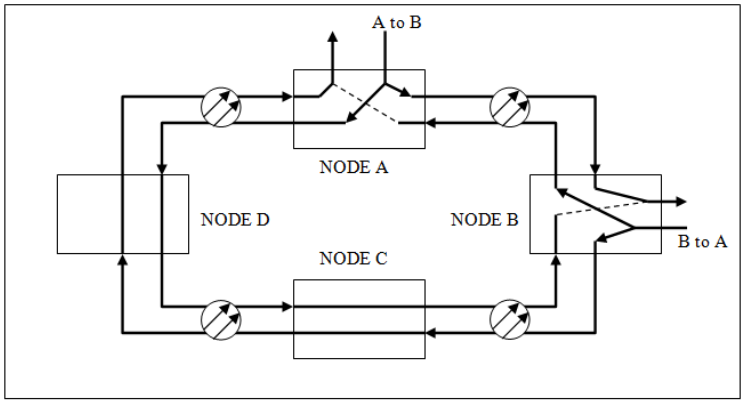


Figure 27 – Example of unequal channel delay

10.3.3.2 SONET GR-1230 2-Fiber Bi-directional Line Switched Ring (BLSR)

A SONET line layer is the connection or transmission span between any two nodes' optical line terminating equipment. The switching threshold is tied directly to the condition of the line. In a 2-fiber BLSR, half the bandwidth is reserved for Service and half the bandwidth is reserved for Protection. Both transmit and receive paths are mapped to take the same route in opposite directions and typically switched together thus eliminating any differential delay between transmit and receive paths. In a switched condition, delays around the ring may be greater in magnitude, but the transmit and receive delays are symmetrical.

Figure 28 depicts a signal between nodes A and B. The primary or Service path is typically the shortest route between the nodes. The traffic from A to B travels on Service fiber 1, while the traffic from B to A travels on Service fiber 2. As mentioned earlier, half the bandwidth of each fiber is reserved for protection. If a failure occurs between nodes A and B, both nodes adjacent to the failure detect the problem and switch their traffic route onto the reserved Protection bandwidth the opposite way around the ring, as depicted in Figure 29.

In a Bi-directional Line Switched Ring (BLSR), switching is typically revertive because all nodes around the ring share the protection bandwidth. If a second failure were to occur at a later time the protection bandwidth would be available for healing. The advantage of a BLSR is increased capacity for interoffice applications. Since information is not sent both ways around the ring like a UPSR, timeslot or channel reuse is possible in an add/drop fashion around the ring.

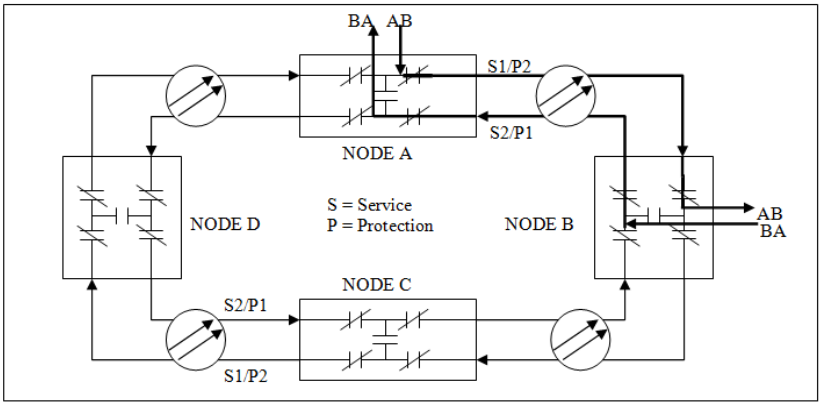


Figure 28 – 2-Fiber Bi-directional Line Switched Ring

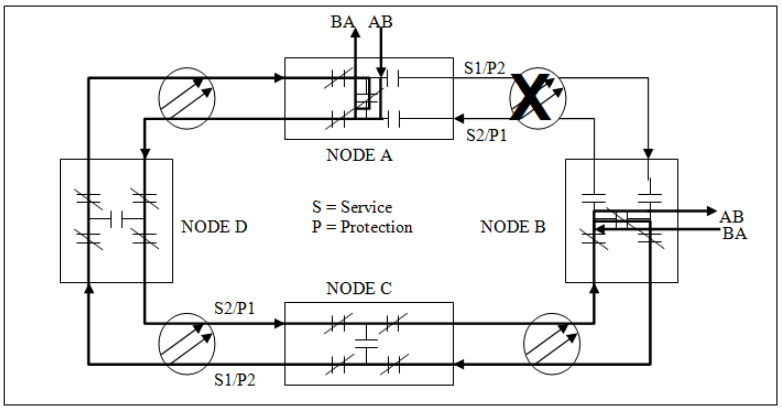


Figure 29 – Protected traffic flow in 2-Fiber BLSR

Table 8 depicts a typical channel plan for an OC-1 payload using half the bandwidth for Service and the other half reserved for Protection. Table 9 depicts the reassigned channel plan for a fiber break between Node B and Node C.

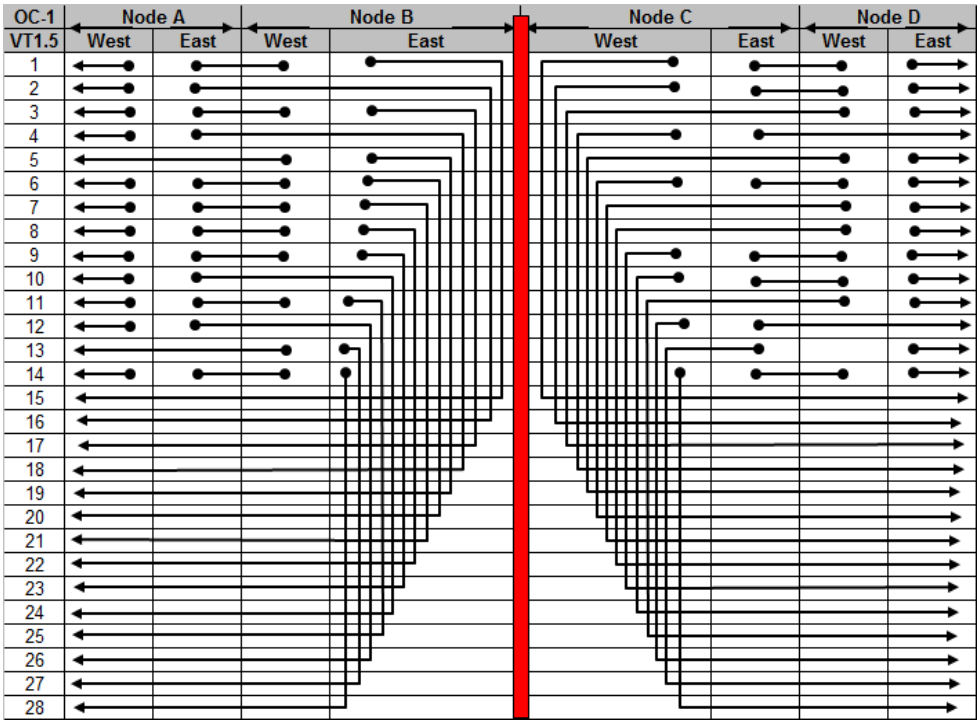
10.3.3.2.1 Protective Relaying System Considerations with BLSR

When protective relaying is applied over this type of ring topology, precautions need to be taken. Although unequal transmit and receive channel delays are no longer a concern, one still has to consider the longer delays experienced when traffic is switched the opposite way around a ring. Some current differential, phase comparison systems and blocking schemes are very delay sensitive. These systems were designed with fixed delay compensation and long delays could result in false operations or failure to trip. This could limit the size of the ring network.

Table 8 2-Fiber BLSR OC-1 Channel plan under normal conditions

OC-1	Node A		Node B		Node C		Node D	
VT1.5	West	East	West	East	West	East	West	East
1	←	→	→	←	←	→	→	→
2	←	→			←	→	→	→
3	←	→	→	←			→	→
4	←	→			←	→		
5	←		→	←			→	→
6	←	→	→	←	←	→	→	→
7	←	→	→	←			→	→
8	←	→	→	←			→	→
9	←	→	→	←	←	→	→	→
10	←	→			←	→	→	→
11	←	→	→	←			→	→
12	←	→			←	→		
13	←		→	←			→	→
14	←	→	→	←	←	→	→	→
15	Reserved for Protection							
16	Reserved for Protection							
17	Reserved for Protection							
18	Reserved for Protection							
19	Reserved for Protection							
20	Reserved for Protection							
21	Reserved for Protection							
22	Reserved for Protection							
23	Reserved for Protection							
24	Reserved for Protection							
25	Reserved for Protection							
26	Reserved for Protection							
27	Reserved for Protection							
28	Reserved for Protection							

Table 9 2-Fiber BLSR OC-1 Channel plan during fiber break between Nodes B and C



10.3.4 GR-1230 4-Fiber Bi-directional Line Switched Ring (BLSR)

A 4-fiber BLSR is similar to a 2-fiber one but it uses a second pair of fibers around the ring for Protection. Since half the bandwidth is no longer used for protection, a 4-fiber BLSR can handle twice the capacity. However, a 4-fiber BLSR also requires twice the optical line terminating equipment, which results in higher cost to implement. Just like a 2-fiber BLSR, both transmit and receive paths are mapped and switched together thus eliminating any differential delay between transmit and receive paths. In a switched condition, delays around the ring may be greater in magnitude but the transmit and receive delays are symmetrical.

10.3.5 SONET Delay Characteristics

In order to calculate the delay in a network the following SONET specifications need to be considered.

DS1 Synchronization Delay into SONET payload	< 100 µs
DS1 Desynchronization Delay out of SONET payload	< 100 µs
DS1 Pass-Through Delay	< 50 µs
Propagation Delay through Fiber	< 8 µs / mile or 12.8 µs / km
Propagation Delay through Radio	< 5 µs / mile or 8 µs / km

Since SONET standards only address DS1 as the smallest bandwidth low speed interface, an Engineer also needs to consider what type of multiplexer he uses for DS0 access onto the SONET transport.

10.3.6 SONET Restoration Characteristics

Engineers may be concerned about the restoration time of their network. Restoration time is the amount of time that transpires once a failure is detected and until valid data is being output again. During this time period communications is lost. Keep in mind that restoration times on networks will only have a major impact on a protective relaying traffic if the communication equipment outage occurs precisely when the system is communicating important information such as TRIP or BLOCK TRIP signals. The odds of simultaneity of occurrence are left to the Engineer to evaluate. In order to calculate the restoration time in a network the following SONET specifications need to be considered.

Time to sense a failure	< 10 ms
Switch time	< 50 ms

Again, since SONET standards only address DS1 as the smallest bandwidth low speed interface, the Engineer also needs to consider what type of DS1 multiplexer he uses for DS0 access onto the SONET transport. They should then look at the reframe time of the DS1 in order to calculate the total restoration delay. One should also consider any restoration times for the device being driven at the DS0 level. For example, some protective relays use channel addressing on switched digital networks to insure no miscommunications. These restoration times would need to be figured in the total equation.

10.4 SONET/SDH for power system protection

Since SONET/SDH networks provide a set of fixed bandwidth channels with a deterministic transmission characteristic, they are well suited for applications that rely on the transmission of a sustained fixed data rate and short signal transfer times, as needed by differential current protection for example. As SONET/SDH signals follow a fixed physical path through the network, SONET/SDH channels will exhibit a fixed transmission delay with low delay variations or "jitter" unless paths are re-routed automatically or manually due to network failures. Transmit and receive directions may however still experience different signal propagation times when the physical route does not follow the same path. Provisions to accommodate the non-equal signal transfer times have to be built into the protection relay in this case.

In conclusion, transport networks based on SONET/SDH technology can be designed to meet the stringent requirements of legacy and future protection systems regarding signal transfer times and error characteristics. Propagation velocity of the light pulses in optical fibers is around 200 km/ms, signal transfer delays between ports of an SONET/SDH node are typically well below 1 ms, and networks are designed to produce very low error rates , much less than 1 ppm (1 part per million or 10^{-6}),under normal operating conditions. Issues that are more critical to the operation of the protection scheme are related to network management and network security, e.g., the impact of path re-routing on transmission time variation and on circuit availability. These are however primarily matters of network planning and network operation.

10.4.1 PDH/SONET/SDH Networks

Transport Networks are used to transfer signal between different access points. These networks are based on permanent dedicated circuits multiplexed over higher capacity communication trunks.

PDH and SONET/SDH are the basic technologies used in transport networks. Both technologies are based on the Time Division Multiplexing technique. Thanks to this, they present a *deterministic and relatively low transmission delay*. Apart from changing signal transfer delays due to route switching, their use for most of the protection schemes do not pose any problem as the transmission delay is low in comparison with most of the protection requirements.

The use of a *fixed connection* established over a PDH or SONET/SDH network for the communication of two protection devices does not present any type of drawback as the incremental delay compared with a direct link is very low. On the other hand, as we have seen before, in order to achieve the availability level requested for this type of service we have to implement some type of recovery mechanism in the network that allows the use of an alternative path when the main path fails.

The BER of a digital connection established in a PDH/SONET/SDH network is normally very low and so it will not have any effect on the Security and Dependability of the protection scheme that uses this path. Nevertheless, the quality of the path can be affected by the synchronization of the network or may be adversely affected by a power system fault due to EMI (Electromagnetic Interference).

The implementation of a good network synchronization plan is very important to achieve the transmission quality levels expected in these types of networks. A poor synchronization scheme will lead to signal slips that produce error bursts that increment the BER of the digital path leading to a poor transmission quality or loss of signal. This effect can disturb the proper protection scheme operation. *It can be relevant for Current Differential Protection schemes since a slip can be seen as a sudden phase change in an analog signal.* SONET/SDH transport networks use a pointer mechanism to indicate the phase of the information inside the main information frame. Changes in phase lead to pointer adjustments that if mishandled can produce sudden phase changes in the transported signals that have a similar effect to the above mentioned slips.

The implementation of recovery or Self-Healing mechanism in a PDH network is based on proprietary solutions. A careful analysis of these algorithms should be carried out in order to find out if it is possible to control the routing of the alternative path and so limit its length. A sudden increment in the number of hops of a path will present a considerable increase in the total delay of the transport path. Uncontrolled changes in delay can disturb the proper operation of certain types of protection schemes such as Differential Current Protection. In any case it should be analyzed that any of the main or back-up paths do not present an End-to-End propagation delay greater than 5 to 8 ms or whatever the particular protection relay can tolerate.

Recovery mechanisms in SONET/SDH network are fully standardized. There are two basic mechanisms that could be applied to improve the overall availability of the transport Network, the SONET UPSR (SDH - SNCP) and the SONET BLSR (SDH – MS-SPRing)

The *UPSR* mechanism protects the end-to-end connection of the final users over the transport network. This method has proved to be very efficient in small ring configurations, but it presents a serious drawback for certain types of protection schemes such as Current Differential due to the fact that the back-up path can be configured with an asymmetrical layout that leads to an asymmetrical delay. This effect together with a possible sudden change in delay due to a different back-up path length will drive to erroneous protection actuation.

The *BLSR* is a straightforward method that protects the connection between two nodes by adding back-up links. In order to achieve a full coverage in the protection both links should use physically diverse routes. However, in a 2-fiber ring the amount of traffic that should be protected requires the same back-up capacity reserved in the network. It should also be noted that traffic has to travel up to the point of the failure before reversing its direction and traveling back around the ring in the opposite direction which results in additional delay, especially in larger rings. For example, if traffic was traveling between nodes 1 and 4 on a 10 node ring and there was a fiber failure between nodes 3 and 4, node 1's traffic would travel up to node 3 before reversing direction and traveling back through node 2 and node 1 again before heading around nodes 10 through 4.

PDH/SONET/SDH presents intrinsic service isolation and security. Due to the fact that these networks are based on the TDM technique and no signaling is available in a transport network, it is not possible for a user to attack another connection. It is recommended that security measures are considered at the control center, however security should be considered throughout the design.

10.5 SONET Synchronization

Synchronization is an important part of all SONET products. Synchronous networks constantly transmit data and use a separate clock signal to determine when to examine the incoming stream to extract a bit. Synchronous systems distribute timing information from an extremely accurate primary system clock. Each network element inherits its timing from the primary clock and can trace its lineage to the common shared clock. Synchronous networks may have several layers of accuracy, but the important feature is that each clock can trace timing to a single reference source. It is important to note that SONET uses a frequency clock running at a DS1 (1.544 Mb/s) line rate to synchronize the network and not a time of day clock, like IRIG-B, used in protective relaying for data correlation or time stamping of events.

The SONET Network Element (NE) is designed for high performance and reliable synchronization and can be used in a number of synchronization environments. Each SONET NE can be provisioned to free run from an internal oscillator, line timed from an incoming optical interface, or get external timing from the digital synchronization network via DS1 references. SONET NEs can support multiple synchronization reference configurations:

- External Timing from a Stratum 3 or better clock (typical central office installations are synchronized with DS1 timing references from a Stratum 1 Building Integrated Timing Supply (BITS) clock).
- Free running from the shelf's internal Stratum 3 Timing Signal Generator (TSG)
- Line/Loop Timing from incoming high speed OC-3, OC-12, OC-48, or OC-192 optical line signals.

10.5.1 Stratum Clock Hierarchy

SONET defines a timing hierarchy known as the Stratum Clock hierarchy. The table below shows the long-term accuracy requirements within the Stratum Clock hierarchy which ranges from Stratum 1 through 4.

Table 10 Stratum Clock Hierarchy

Stratum Hierarchy	Minimum Free Run Accuracy
1	$\pm$ 1.0 x 10^{-11}
2	$\pm$ 1.6 x 10^{-8}
3	$\pm$ 4.6 x 10^{-6}
4	$\pm$ 32 x 10^{-6}

Stratum 1 is defined as a completely autonomous source of timing, which has no other input, other than perhaps a yearly calibration. The usual source of Stratum 1 timing is an atomic standard (Cesium Beam or Hydrogen Maser) or reference oscillator (OCXO). The minimum adjustable range and maximum drift is defined as a fractional frequency offset f/f of 1 x 10-11 or less. At this minimum accuracy, a properly calibrated source will provide bit-stream timing that will not slip relative to an absolute or perfect standard more than once every 4 to 5 months. Atomic standards, such as Cesium clocks, have far better performance.

A Stratum 1 clock is an example of a Primary Reference Source (PRS) as defined in ANSI/T1.101. Alternatively, a PRS source can be a clock system employing direct control from Coordinated Universal Time (UTC) frequency and time services, such as Global Positioning System (GPS) navigational systems. The GPS System may be used to provide high accuracy, low cost timing of Stratum 1 quality.

Although Synchronous networks display accurate timing, some variations can occur between different network devices or between networks. This difference is known as phase variations. Phase variations are defined as Jitter or Wander. Jitter is defined as short-term phase variations above 10Hz. Wander is defined as long-term phase variations below 10Hz. In digital networks, Jitter and Wander are handled by buffers found in the interfaces within different network devices. One example is a Slip Buffer. The Slip Buffer is used to handle frequency differences between read and write operations. To prevent against write operations happening faster than read operations, read operations are handled at a slightly higher rate. On a periodic basis, read operations are paused, while a bit is stuffed into a stream to account for any timing differences between the read and write operations. This bit-stuffing scheme is referred to as a controlled slip (frame).

In terms of Wander, Bit Slips and Controlled Slips, the Stratum Clocking accuracy timing requirements are defined in the table below. The timing accuracy requirements increase as the Stratum hierarchy increases. The Stratum 1 Clock must meet the highest degree of accuracy.

Table 11 Stratum Clocking Accuracy Timing Requirements

Stratum Hierarchy	Wander (.12 microsecond increments)	Bit slips	Controlled (Frame Slips)
1	3.3 hours	18 hours	20.6 weeks
2	7.5 seconds	41 seconds	2.17 hours
3	26 ms	140 ms	27 seconds
4	4 ms	20 ms	3.9 seconds

10.5.2 Synchronization Status Messages (SSM)

SONET NE provides a standardized synchronization messaging feature to ensure the integrity of network synchronization during both normal and abnormal conditions. Through the use of synchronization messaging, the current quality and usability of the timing source can be conveyed from one SONET NE to the next. This capability allows line-timed SONET NEs shelves to automatically change their timing reference in order to always maintain the highest quality timing available and avoid loops. The capability also allows SONET NEs to inform a local BITS clock when the DS1 timing output has been degraded and should no longer be used as a reference. This synchronization messaging feature is based on the scheme developed in the ANSI T1X1 standards committee. The applications that are currently supported with the synchronization messaging feature can be divided into the following categories: DS1 timing output integrity and automatic synchronization reconfiguration.

The derived DS1 timing outputs are typically used as a synchronization reference to a BITS clock which provides the timing reference to an externally-timed SONET NE shelf. The synchronization reference is derived from the SONET transmission facility which is synchronized from an upstream timing reference. In this way, the timing from the BITS clock in one office (master) is distributed to the next office (slave) using the SONET transmission facilities between them as the synchronization vehicle. The BITS are typically capable of synchronizing to a Stratum 3 or better accuracy. SONET NEs are equipped with the embedded Timing Signal Generator (TSG) capable of synchronizing to a 4.6 ppm clock (Stratum 3) or better. The Stratum timing hierarchy requires that clocks of equal or better Stratum level be used to synchronize other clocks. In this way, the Stratum timing hierarchy is preserved under all failure conditions. Under non-failure conditions SONET NEs do not introduce their own internal timing source onto the SONET facility, but merely transfers the quality of its timing reference. A failure of all derived DS1 timing references to the BITS at the master office will cause the BITS to enter holdover mode, whose minimum accuracy is dependent on its internal clock. Since the BITS internal clock is of equal or better Stratum level than SONET NE the externally-timed SONET NE shelf will use this reference to synchronize all outgoing SONET transmission facilities. This preserves the required hierarchical structure of the timing network which must be maintained at all times.

11. Physical Communications Media- Electrical

11.1 Serial Communications RS-232

In telecommunications, RS-232 (Recommended Standard 232) is a standard for serial binary data signals connecting between a DTE (Data Terminal Equipment) and a DCE (Data Circuit-terminating Equipment). It is commonly used in computer serial ports.

The original DTEs were electromechanical teletypewriters and the original DCEs were (usually) modems. When electronic terminals (smart and dumb) began to be used, they were often designed to be interchangeable with teletypes, and so supported RS-232. The C revision of the standard was issued in 1969 in part to accommodate the electrical characteristics of these devices.

Later personal computers (and other devices) started to make use of the standard so that they could connect to existing equipment. For many years, an RS-232-compatible port was a standard feature for serial communications, such as modem connections, on many computers. It remained in widespread use into the late 1990s, and while it has largely been supplanted by other interface standards in computer products, it is still used to connect legacy peripherals, industrial equipment (such as based on PLCs), and console ports.

The standard has been renamed several times during its history as the sponsoring organization changed its name, and has been variously known as EIA RS 232, EIA 232, and most recently as TIA 232.

Many personal computers intended for office use ship with "legacy-free" motherboards without any RS-232 serial ports. Many motherboards and desktop systems provide these ports even though they may not be used, simply because it costs the manufacturer very little to include them. Small-form-factor systems and laptops, however, often do not include them in order to conserve space.

Network equipment, such as manageable switches and routers, usually has an RS-232 port for configuration of the device. It's a problem for some network administrators that most new laptops don't have an RS-232 port (though one can of course use a USB-to-serial converter, but often these do not support all handshaking fully). Various Peripheral Component Interconnect (PCI) and PCI Express cards provide RS-232 ports.

It is also possible to connect RS-232 devices via Ethernet and WLAN device drivers that act as network servers. Some manufacturers even have virtual serial port drivers available. This will be discussed later on this document.

RS-232 was recommended for short connections (15 meters or less), however the limit is actually defined by total capacitance and low capacitance cables allow reliable communications over longer distances exceeding 50 m. RS-232 interface cables are not usually constructed with twisted pair because of the unbalanced circuits.

11.1.1 Voltage levels

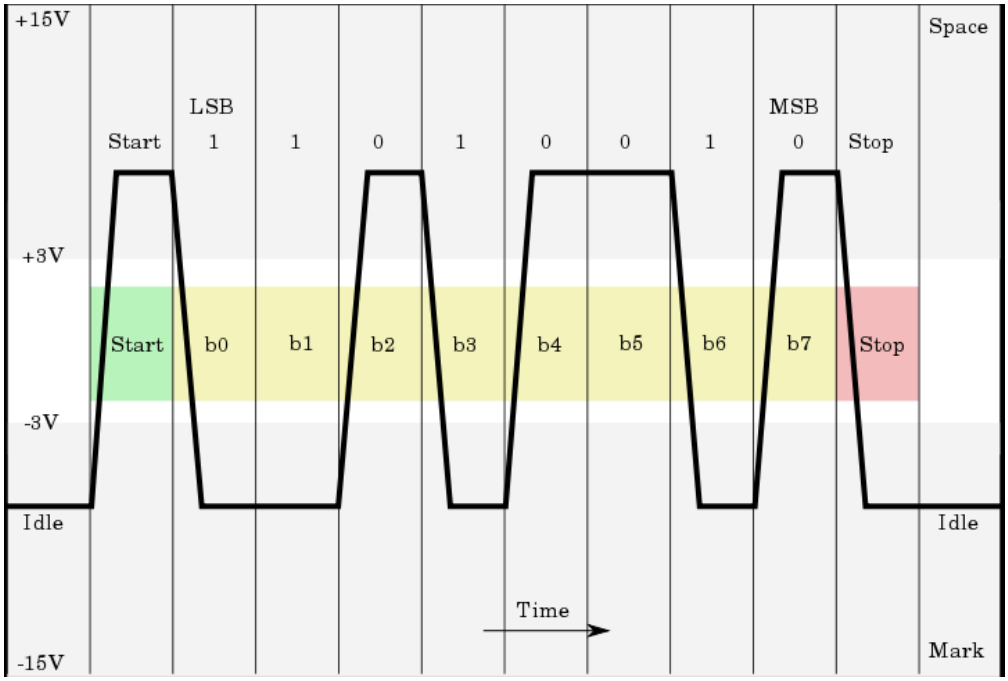


Figure 30 - Diagrammatic oscilloscope trace of voltage levels

Figure 30 shows a diagrammatic oscilloscope trace of voltage levels for an uppercase "K" ASCII character (0x4b) with 1 start bit, 8 data bits, 1 stop bit

The RS-232 standard defines the voltage levels that correspond to logical one and logical zero levels for the data transmission and the control signal lines. Valid signals are plus or minus 3 to 15 volts; the ±3 V range near zero volts is not a valid RS-232 level. The standard specifies a

maximum open-circuit voltage of 25 volts: signal levels of ±5 V, ±10 V, ±12 V, and ±15 V are all commonly seen depending on the power supplies available within a device. RS-232 drivers and receivers must be able to withstand indefinite short circuit to ground or to any voltage level up to ±25 volts. The slew rate, or how fast the signal changes between levels, is also controlled.

For data transmission lines (TxD, RxD and their secondary channel equivalents) logic one is defined as a negative voltage, the signal condition is called marking, and has the functional significance. Logic zero is positive and the signal condition is termed spacing. Control signals are logically inverted with respect to what one sees on the data transmission lines. When one of these signals is active, the voltage on the line will be between +3 to +15 volts. The inactive state for these signals is the opposite voltage condition, between −3 and −15 volts. Examples of control lines include request to send (RTS), clear to send (CTS), data terminal ready (DTR), and data set ready (DSR).

Because both ends of the RS-232 circuit depend on the ground pin being zero volts, problems will occur when connecting machinery and computers where the voltage between the ground pin on one end, and the ground pin on the other is not zero. This may also cause a hazardous ground loop. Use of a common ground limits RS-232 to applications with relatively short cables. If the two devices are far enough apart or on separate power systems, the local ground connections at either end of the cable will have differing voltages; this difference will reduce the noise margin of the signals. Balanced, differential, serial connections such as Universal Serial Bus (USB), RS-422 and RS-485 can tolerate larger ground voltage differences because of the differential signaling.

11.1.2 RS-232 Data Structure

The RS-232 standard describes a communication method where information is sent bit by bit on a physical channel. The information must be broken up in data words. The length of a data word is variable. On PC's a length between 5 and 8 bits can be selected. This length is the net information length of each word. For proper transfer additional bits are added for synchronization and error checking purposes. It is important that the transmitter and receiver use the same number of bits. Otherwise, the data word may be misinterpreted, or not recognized at all.

Data bits are sent with a predefined frequency, the baud rate. Both the transmitter and receiver must be programmed to use the same bit frequency. After the first bit is received, the receiver calculates at which moments the other data bits will be received. It will check the line voltage levels at those moments.

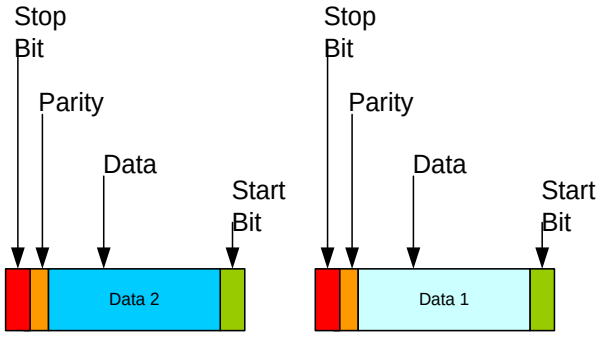


Figure 31 – Data Structure

11.1.2.1 Start bit

RS-232 defines an asynchronous type of communication. This means, that sending of a data word can start at any moment. If starting at any moment is possible, this can pose some problems for the receiver to know when the first bit is to be received is. To overcome this problem, each data word is started with an attention bit. This attention bit, also known as the start bit, is always identified by the space line level. Because the line is in mark state when idle, the start bit is easily recognized by the receiver.

11.1.2.2 Data bits

Directly following the start bit, the data bits are sent. A bit value 1 causes the line to go in mark state; the bit value 0 is represented by a space. The least significant bit is always the first bit sent.

11.1.2.3 Parity bit

For error detecting purposes, it is possible to add an extra bit to the data word automatically. The transmitter calculates the value of the bit depending on the information sent. The receiver performs the same calculation and checks if the actual parity bit value corresponds to the calculated value.

11.1.2.4 Stop bits

The stop bit identifying the end of a data frame can have different lengths. Actually, it is not a real bit but a minimum period of time the line must be idle (mark state) at the end of each word. On PC's this period can have three lengths: the time equal to 1, 1.5 or 2 bits. 1.5 bits is only used with data words of 5 bits length and 2 only for longer words. A stop bit length of 1 bit is possible for all data word sizes.

11.1.3 RS-232 Physical Properties

The RS-232 standard describes a communication method capable of communicating in different environments. This has had its impact on the maximum allowable voltages etc. on the pins. In the original definition, the technical possibilities of that time were taken into account. The maximum baud rate defined for example is 20 kbps. With current devices like the 16550A Universal Asynchronous Receiver / Transmitter (UART), maximum speeds of 1.5 Mbps are allowed.

11.1.4 Maximum cable lengths

Since the standard definitions are not always correctly applied, it is often necessary to consult documentation, test connections with a breakout box, or use trial and error to find a cable that works when interconnecting two devices. Connecting a fully-standard-compliant DCE device and DTE device would use a cable that connects identical pin numbers in each connector (a so-called "straight cable"). "Gender changers" are available to solve gender mismatches between cables and connectors. Connecting devices with different types of connectors requires a cable that connects

the corresponding pins. Cables with 9 pins on one end and 25 on the other are common, and manufacturers of equipment with RJ-45 connectors usually provide a cable with either a DB-25 or DE-9 connector (or sometimes interchangeable connectors so they can work with multiple devices).

Connecting two DTE devices together requires a null modem that acts as a DCE between the devices by swapping the corresponding signals. This can be done with a separate device and two cables, or using a "cross-over cable" wired to connect the transmit pin on one end to the receive pin on the other end and vice versa; connections may also need to be made to the flow control pins, depending on whether the particular devices being connected make use of those.

Cable length is one of the most discussed items in RS-232 world. The standard has a clear answer; the maximum cable length is 50 feet, or the cable length equal to a capacitance of 2500 pF. The latter rule is often forgotten. This means that using a cable with low capacitance allows you to span longer distances without going beyond the limitations of the standard. If, for example UTP CAT-5 cable, which has typical capacitance of 17 pF/ft, is used, the maximum allowed cable length is 147 feet.

The cable length mentioned in the standard allows maximum communication speed to occur. If speed is reduced by a factor 2 or 4, the maximum length increases dramatically. Keep in mind, that the RS-232 standard was originally developed for 20 kbps. By halving the maximum communication speed, the allowed cable length increases a factor ten!

Table 12 Cables Lengths

RS-232 cable length according to Texas Instruments	
Baud rate	Maximum cable length (ft)
19200	50
9600	500
4800	1000
2400	3000

You can usually ignore this "standard", since a cable can be as long as 10000 feet at baud rates up to 19200 if you use a high quality, well shielded cable. The external environment has a large effect on lengths for unshielded cables. In electrically noisy environments such as electrical substations, even very short cables can pick up stray signals. Table 12 offers some reasonable guidelines for 24 gauge wire under typical (low noise) conditions. You can greatly extend the cable length by using additional devices like optical isolators and signal boosters.

Optical isolators use Light Emitting Diodes (LEDs) and Photo Diodes to isolate each line in a serial cable including the signal ground. Any electrical noise affects all lines in the optically isolated cable equally - including the signal ground line. This causes the voltages on the signal lines relative to the signal ground line to reflect the true voltage of the signal and thus cancelling out the effect of any noise signals. Some electrical utilities have decided against use of optical isolators within their substations because of concern over transferred potential during ground

faults; these companies may instead use a fiber optic link with a port converter at each end of the link.

11.1.5 Error detection

One way of detecting errors is the frame detection mechanism which is used to test if the incoming bits were properly surrounded by a start and stop bit pair. For further error checking, a parity bit can be used. The use of this bit is however not mandatory. If the existence of wrong bits is rare (when communicating with an internal modem as opposed to a sonically-coupled telephone modem for example) or if a higher level protocol is used for error detection and correction in the application (Z-modem, RAS, etc) communication speed can be increased by not using the parity feature present on the UART.

Parity is a simple way to encode a data word to have a mechanism to detect an error in the information. The method used with serial communications adds one bit to each data word. The value of this bit depends on the value of the data word. It is necessary that both the transmitter and receiver use the same algorithm to calculate the value of the parity bit. Otherwise, the receiver may detect errors which are not present.

11.1.5.1 Even parity

Basically, the parity bit can be calculated in two ways. When even parity is used, the number of information bits sent will always contain an even number of logical 1's. If the number of high data bits is odd, a high value parity bit is added, otherwise a low bit will be used.

11.1.5.2 Odd parity

The odd parity system is quite similar to the even parity system, but in this situation, the number of high bits will always be odd.

11.1.6 Disadvantages of the parity system

The parity system using one bit for each data word is not capable of finding all errors. Only errors which cause an odd number of bits to flip will be detected. The second problem is that there is no way to know which bit is false. If necessary, a higher level protocol is necessary to inform the sender that this information must be resent. Therefore, on noisy lines, often other detection systems are used to assure that the sent information is received correctly. These systems mostly do not operate on single data words, but on groups of words. Known coding systems are:

Hamming coding:

- CRC16 cyclic redundancy check
- CCITT-16 cyclic redundancy check
- CRC-DNP cyclic redundancy check
- CRC32 cyclic redundancy check

Other serial interfaces similar to RS-232:

- RS-422 (a high-speed system similar to RS-232 but with differential signaling)
- RS-423 (a high-speed system similar to RS-422 but with unbalanced signaling)
- RS-449 (a functional and mechanical interface that used RS-422 and RS-423 signals - it never caught on like RS-232 and was withdrawn by the EIA)
- RS-485 (a descendant of RS-422 that can be used as a bus in multidrop configurations)
- MIL-STD-188 (a system like RS-232 but with better impedance and rise time control)
- EIA-530 (a high-speed system using RS-422 or RS-423 electrical properties in an EIA-232 pin out configuration, thus combining the best of both; supersedes RS-449)
- TIA-574 (standardizes the 9-pin D-sub miniature connector pin out for use with EIA-232 electrical signaling, as originated on the IBM PC/AT)

11.2 Serial Communications RS-485

EIA-485 (formerly RS-485 or RS-485) is an OSI model physical layer electrical specification of a two-wire, half-duplex, multipoint serial connection. (Note that although the signal is determined by the differential voltage between the two signal wires, a third wire is required to provide the signal reference. Often, the cable shield is used for the dual purpose of electrostatic noise shielding and providing the signal reference. In very noisy environments, a separate third wire may be used to provide the signal reference and the cable shield grounded appropriately to provide electrostatic shielding only, thus keeping the noise currents completely out of the signal path.) The standard specifies a differential form of signaling. The difference between the wires' voltages is what conveys the data. One polarity of voltage indicates a logic 1 level; the reverse polarity indicates logic 0. The difference of potential must be at least 0.2 volts for valid operation, but any applied voltages between +12 V and -7 volts will allow correct operation of the receiver.

EIA-485 only specifies electrical characteristics of the driver and the receiver. It does not specify or recommend any data protocol. But because multiple devices share the same transmit line, the protocol and applications employed should assure that only one device at a time attempts to transmit or should otherwise include data collision avoidance, detection, and arbitration. EIA-485 enables the configuration of inexpensive local networks and multidrop communications links. It offers high data transmission speeds (35 Mbit/s up to 10 m and 100 kbit/s at 1200 m). Since it uses a differential balanced line over twisted pair (like EIA-422), it can span relatively large distances (up to 4000 feet or just over 1200 meters).

In contrast to EIA-422, which has a single driver circuit which cannot be switched off, EIA-485 drivers need to be put in transmit mode explicitly by asserting a signal to the driver. This allows EIA-485 to implement linear topologies using only two lines and between the ribbon cable. The equipment located along a set of EIA-485 wires is interchangeably called nodes, stations and devices.

The recommended arrangement of the wires is as a connected series of point-to-point (multidropped) nodes, a line or bus, not a star, ring, or multiply-connected network. Ideally, the two ends of the cable will have a termination resistor connected across the two wires to prevent signal reflection at the open ends. Without termination resistors, reflections of fast driver edges can

cause multiple data edges that can cause data corruption. Termination resistors also reduce electrical noise sensitivity due to the lower impedance, and bias resistors (see below) are required. The value of each termination resistor should be equal to the cable impedance (typically, 120 ohms for twisted pairs). Star and ring topologies are not recommended because of signal reflections or excessively low or high termination impedance.

EIA-485, like EIA-422 can be made full-duplex by using four wires, however, since EIA-485 is a multi-point specification, this is not necessary in many cases. EIA-485 and EIA-422 can interoperate with certain restrictions.

RS-485 can be used to communicate with remote devices at distances up to 4000 ft (1200 m) at speeds of up to 100 kbit/s at this distance. Converters between RS-232 and RS-485, USB and RS-485, Ethernet and RS-485 are available to allow your PC to communicate with remote devices. By using "Repeaters" and "Multi-Repeaters" very large RS-485 networks can be formed. The Application Guidelines for TIA/EIA-485-A has one diagram called "Star Configuration. Not recommended." Using an RS-485 "Multi-Repeater" can allow for "Star Configurations" with "Home Runs" (or multi-drop) connections similar to Ethernet Hub/Star implementations (with greater distances). Hub/Star systems (with "Multi-Repeaters") allow for very maintainable systems, without violating any of the RS-485 specifications. Repeaters can also be used to extend the distance and/or number of nodes on a network. It can and is being done.

11.2.1 Uses of EIA-485

EIA-485 is often used with common UARTs to implement low-speed data communications in commercial aircraft cabins. For example, some passenger control units use it. It requires minimal wiring, and can share the wiring among several seats. It therefore reduces the system weight.

EIA-485 also sees use in programmable logic controllers and on factory floors in order to implement proprietary data communications with Distributed I/O equipment or IEDs. Since it is differential, it resists electromagnetic interference from motors and welding equipment. It is used in large sound systems, as found at music events and theatre productions, for remotely controlling high-end sound-processing equipment from a standard computer running special software. The EIA-485 link is typically implemented over standard XLR cables more usually used for microphones, and so can be run between stage and control desk without laying special cables. It is also is used in building automation as the simple bus wiring and long cable length is ideal for joining remote devices as well as to control theatrical and disco lighting where it is known as DMX.

11.2.2 Differential signals with RS-485

[5] One of the main problems with RS-232 is the lack of immunity for noise on the signal lines. The transmitter and receiver compare the voltages of the data- and handshake lines with one common zero line. During power system disturbances for example, shifts in the ground level can have disastrous effects. Therefore the trigger level of the RS-232 interface is set relatively high at ±3 Volt. Noise is easily picked up and limits both the maximum distance and communication speed.

With RS-485 on the contrary there is no such thing as a common zero as a signal reference. Several volts difference in the ground level of the RS-485 transmitter and receiver does not cause any problems. The RS-485 signals are floating and each signal is transmitted over a Sig+ line and a Sig- line. The RS-485 receiver compares the *voltage difference* between both lines, instead of the *absolute voltage level* on a signal line. This works well and prevents the existence of ground loops, a common source of communication problems. The best results are achieved if the Sig+ and Sig- lines are twisted. The image in Figure 32 explains why.

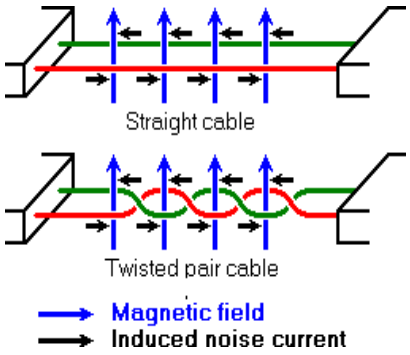


Figure 32 – Noise in Straight and Twisted Pair Cables

In Figure 32, noise is generated by magnetic fields from the environment. The picture shows the magnetic field lines and the noise current in the RS-485 data lines that is the result of that magnetic field. In the straight cable, all noise current is flowing in the same direction, practically generating a looping current just like in an ordinary transformer. When the cable is twisted, we see that in some parts of the signal lines the direction of the noise current is the opposite from the current in other parts of the cable.

Because of this, the resulting noise current is many factors lower than with an ordinary straight cable. Shielding – a common method to prevent noise in RS-232 lines – tries to keep hostile electromagnetic fields away from the signal lines. Properly applied shielding can effectively drain electrostatically-coupled noise currents to ground, but has almost no effect on low-frequency magnetically-induced noise voltages. A tightly twisted signal pair connected to a differential input receiver provides a high degree of immunity to magnetically-induced noise voltage. A twisted pair in RS-485 communication however adds immunity which is a much better way to fight noise. The magnetic fields are allowed to pass, but do no harm. The voltage induced in each twist cancels the voltage the adjacent twist such that almost no net voltage is presented to the input of the receiver. If high noise immunity is needed, often a combination of twisting and shielding is used as for example in STP, shielded twisted pair and FTP, foiled twisted pair networking cables – the twisting of the signal pairs providing the magnetic shielding and the foil or braided shield grounded at one or both ends providing the electrostatic shielding. Differential signals and twisting allows RS-485 to communicate over much longer communication distances than achievable with RS-232. With RS-485 communication distances of 1200 m are possible.

Table 13 Characteristics of RS-485 compared to RS-232, and RS422

Characteristics of RS-232, RS422, and RS-485

	RS-232	RS422	RS-485
Differential	No	Yes	yes
Max number of drivers Max number of receivers	1 1	1 10	32 32
Modes of operation	Half duplex full duplex	half duplex	half duplex
Network topology	point-to-point	multidrop	multipoint
Max distance (acc. standard)	15 m	1200 m	1200 m
Max speed at 12 m Max speed at 1200 m	20 kbps (1 kbps)	10 Mbps 100 kbps	35 Mbps 100 kbps

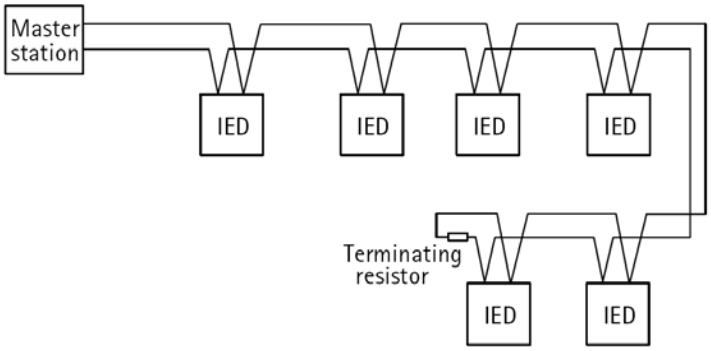
Differential signal lines also allow higher bit rates than possible with non-differential connections. Therefore RS-485 can overcome the practical communication speed limit of RS-232. Currently RS-485 drivers are produced that can achieve a bit rate of 35 Mbps.

Interesting is that RS-232 is the only interface capable of full duplex communication. This is, because on the other interfaces the communication channel is shared by multiple receivers and – in the case of RS-485 – by multiple senders. RS-232 has a separate communication line for transmitting and receiving which – with a well written protocol – allows higher effective data rates at the same bit rate than the other interfaces. The request and acknowledge data needed in most protocols does not consume bandwidth on the primary data channel of RS-232.

11.2.3 Network topology with RS-485

Network topology is probably the reason why RS-485 is now the favorite of the three mentioned interfaces in data acquisition and control applications. RS-485 is the only one of the interfaces capable of internetworking multiple transmitters and receivers in the same network. When using the default RS-485 receivers with an input resistance of 12 kΩ it is possible to connect up to 32 devices to the network. Currently available high-resistance RS-485 inputs allow this number to be expanded to 256. RS-485 repeaters are also available which make it possible to increase the number of nodes to several thousands, spanning multiple kilometers. And that with an interface which does not require intelligent network hardware: the implementation on the software side is not much more difficult than with RS-232. It is the reason why RS-485 is so popular with computers, PLCs, micro controllers and intelligent sensors in scientific and technical applications.

The general network topology of RS-485 consists of N nodes connected in a multipoint RS-485 network. For higher speeds and longer lines, termination resistances are necessary on both ends of the line to eliminate reflections. Use 100 Ω resistors on both ends. The RS-485 network must be designed as one line with multiple drops, not as a star. Although total cable length maybe shorter in a star configuration, adequate termination is not possible anymore and signal quality may degrade significantly.



Note: A Terminating Resistor is built into the Master Station

Figure 33 – RS-485 Network Topology

11.2.4 RS-485 functionality

And now the most important question, how does RS-485 function in practice? Default, all the senders on the RS-485 bus are in tri-state with high impedance. In higher level protocols, one of the nodes is defined as a master, which sends queries or commands over the RS-485 bus. All other nodes receive these data. Depending of the information in the sent data, zero or more nodes on the line respond to the master. In this situation, almost 100% of bandwidth is used.

There are other implementations of RS-485 networks where every node can start a data session on its own. This is comparable with the way Ethernet networks function. Because there is opportunity of data collision with this implementation, theory tells us that in this case only 37% of the bandwidth will be effectively used. With such an implementation of a RS-485 network it is necessary that there is error detection implemented in the higher level protocol to detect the data corruption and resend the information at a later time.

There is no need for the senders to explicitly turn the RS-485 driver on or off. RS-485 drivers automatically return to their high impedance tri-state within a few microseconds after the data has been sent. Therefore it is not needed to have delays between the data packets on the RS-485 bus.

RS-485 is used as the electrical layer for many well known interface standards, including Profibus and Modbus. Therefore RS-485 will be in use for many years in the future.

11.3 Electrical Interfaces

11.3.1 Metallic media (coax and twisted pair)

Metallic media are the oldest and most commonly used form of electronic communication media. The large installed base of metallic systems and relative ease of interface make it attractive to adapt digital communications to metallic transport. Metallic media has been enhanced to serve the needs of digital communications. Consequently, metallic transport is not likely to become obsolete any time soon.

Metallic media in the communication world are roughly divided between twisted pair (or "copper") systems and co-axial cable systems. Twisted pair has been the primary standard and has the largest installed base. Signals are routed point to point on twisted pairs of 18 to 32 gauge copper wire in multiple pair cables.

Modem manufacturers have recently announced 33.6 kbps V.34 modems and 56 kbps pulse code modulated (PCM) modems. Although speed has improved for some circuits, buffering, retransmit, error correction, and unpredictable speed during noisy circuit conditions limit relay applications. Integrated Services Digital Network (ISDN) and Digital Subscriber Line (DSL) technologies, originally designed for the telecommunications industry, show promise for relay applications due to increased speed and lower delay. However, unwanted induction and conduction on the metallic media will continue to be issues to deal with in the substation environment.

Coax has been more commonly used with high frequency and bandwidth broadcast systems like cable TV (CATV). Transporting data over cable is currently a popular topic due to the demand for Internet bandwidth. Developing adequate bandwidth from the user to the hub is a challenge; currently hybrid fiber coax (HFC) designs offer the largest bandwidth. Since coax can transport several gigabits of data over thousands of feet relatively shielded from interference, it may be useful in this role for protection systems.

11.3.2 Digital Electrical Interfaces

Several electrical communication interface standards exist to permit the interconnection of equipment from different manufacturers. These interfaces can be asynchronous or synchronous.

Asynchronous data transmission does not utilize a master clock, therefore each terminal generates its own timing. Asynchronous communications is primarily used for slower speed data, and is not as efficient as synchronous data transmission. As framing, or start, and stop bits are required for every data byte.

Synchronous communications requires a common clock source, generally provided by the Data Communications Equipment (DCE), to which the Data Terminal Equipment (DTE) synchronizes. While synchronous communications systems require more precise clock circuitry, they allow faster data transfer rates then asynchronous methods, as the start and stop bits are not required to mark the beginning and end of each data byte.

A DTE device can be described as any digital device that transmits, or receives data, and requires communications equipment for the data transfer.

A DCE device can be described as a digital device that is connected to a communications line for the purpose of transfer data, without regard its content. Ex: modem.

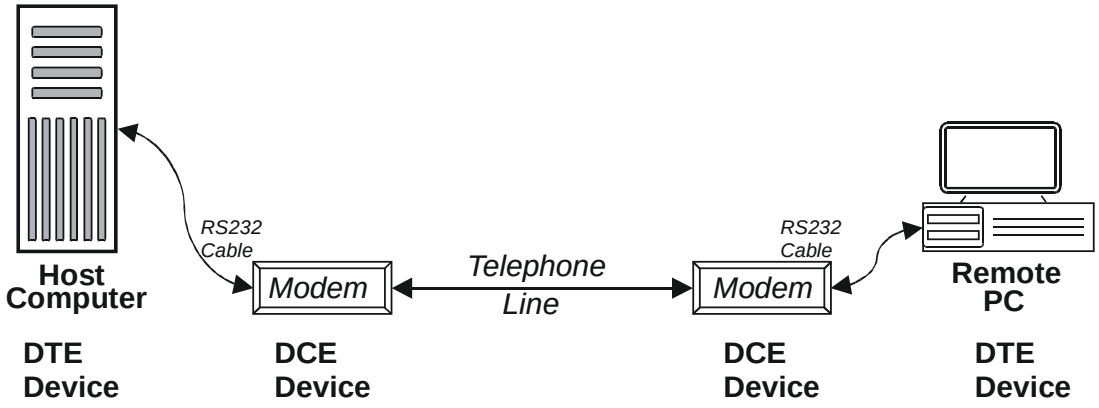


Figure 34 – DTE and DCE devices

Signal names are in reference to the terminal DTE device. For example, TX data is an output from the DTE device, transmitted to the DCE device. DTE devices usually use a male plug connector, while DCE devices usually use a female connector. There are many styles of the connectors.

11.3.3 RS-232 Electrical Interface

The RS-232 standard was designed to allow DTE devices to be connected directly to DCE devices, with a straight – through cable. The RS-232 connector is usually, a nine pin DE9 connector, or a twenty five pin, DB25, connector. (Note, the DE9 connector is commonly referred to as DB9 and it is understood in the context of personal computer communication connectors that the name DB9 is actually referring to the smaller E-size housing.)

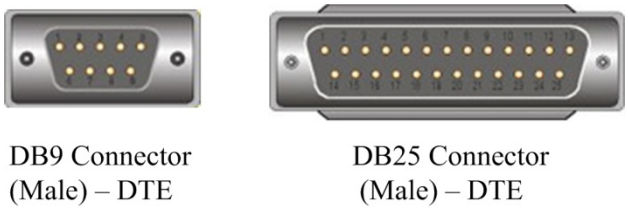


Figure 35 – RS-232 Typical Connectors

RS-232 is an unbalanced interface that uses signals with reference to ground; this makes the interface susceptible to ground potential differences. Isolated DC power supplies, and interface circuits are often used to overcome this problem. RS-232 data is typically sent at irregular intervals with variable time between characters, this requires either hardware, or software flow control to prevent the receiver data buffers from being overrun. The RS-232-C standard specifies a maximum bit rate of 20,000 bps. Besides lower bit rates, maximum cables lengths are typically limited to 50 feet. (See also *Section 11.1.3 RS-232 Physical Properties* earlier in this document.)

11.3.4 RS449 Electrical Interface

Developed to overcome RS-232 speed, and distance limitations, RS449 can support data rates of 100 Kbps at 4,000 feet, or 10 Mbps at 40 feet. The EIA RS449 standard specifies the functional

and mechanical characteristics of the RS449 interconnection between the data terminal equipment (DTE) in the data communications equipment (DCE) complying to EIA electrical interface standards RS 422, for balanced signals, and RS 423, for unbalanced signals.

Male

Female

Pin	Signal	Abbr.	DTE	DCE	Pin	Signal	Abbr.	DTE	DCE
1	**Shield**				20	Receive	RC		
2	Signal Rate	S	Out	In	21	Unassigned			
3	Unassigned				**22**	**Send Data**	SD+	Out	In
4	**Send Data**	SD-	Out	In	**23**	**Send**	ST+	In	Out
5	**Send**	ST-	In	Out	**24**	**Receive**	RD+	In	Out
6	**Receive**	RD-	In	Out	25	Request To	RS+	Out	In
7	Request To	RS-	Out	In	**26**	**Receive**	RT+	In	Out
8	**Receive**	RT-	In	Out	27	Clear To	CS+	In	Out
9	Clear To	CS-	In	Out	28	Terminal In	IS	Out	In
10	Local	LL	Out	In	29	Data Mode	DM+	In	Out
11	Data Mode	DM-	In	Out	30	Terminal	TR+	Out	In
12	Terminal	TR-	Out	In	31	Receiver	RR+	In	Out
13	Receiver	RR-	In	Out	32	Select	SS	In	Out
14	Remote	RL	Out	In	33	Signal	SQ	In	Out
15	Incoming	IC	In	Out	34	New Signal	NS	Out	In
16	Signal	SF/SR+	In/Out	Out/In	35	Terminal	TT+	Out	In
17	Terminal	TT-	Out	In	36	Standby	SB	In	Out
18	Test Mode	TM-	In	Out	37	Send	SC		
19	Signal	SG							

Figure 36 – RS449 Pinouts

Note: signals in bold are commonly used in the majority of applications

RS449 is a high-speed digital interface - unlike RS-232, which uses signals with reference to ground. RS449 receivers look for the difference between two wires. By twisting the two wires and making a "twisted pair" any stray noise picked up on one wire will be picked up on the other, because both wires pick up the same noise the RS449 differential interface just shifts in voltage level with reference to ground, but does not change with respect to each other. The receivers are only looking at the difference in voltage level of each wire to the other not to ground. The biggest problem faced is how the cables are made and routed.

The differential signals for RS449 are labeled as either "A and B" or "+ and -". In the case of RS449 wire A or + does not connect to B or -. Wire A always connects to A and B connects to B or + to + and - to -. If the wires get crossed (A to B or + to -), the signal gets inverted and the communication won’t work - be sure to check the polarities.

RS-449 interfaces are commonly found on communications equipment where high throughput and/or long distances are required. The interface also offers good noise immunity enabling reliable communications in environments where there are high levels of EMI.

11.3.5 V.35 Electrical Interface

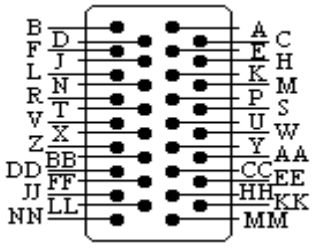
While not very popular, the V.35 is a specification for a connector type, pin allocation and signal level used for synchronous communications interfaces. V.35 is a partially balanced, partially single-ended interface specification. While the data leads and clock leads are balanced, the handshake leads are single-ended. Most commonly used for 56kbps and 64kbps data rates.

V.35 uses differential interfaces for the clock and data signals, which are the only signals requiring high switching speeds for high-speed communications. Throughput of up to 10Mbps is typical, dependent on the equipment and cable used. The other signals are unbalanced (single wire) and normally incur a minimum of state changes. Separate clock lines are used for receiving and transmitting data.

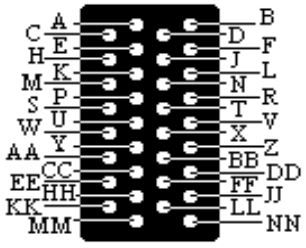
V.35 interfaces are common in some parts of the world primarily due to its adoption by telephone companies and their equipment suppliers. Commonly used bit-rates are 64Kbps, 128Kbps, and 256Kbps etc.

Maximum cable length depends on required speed and cable capacitance. The extremes specified are 2000ft/600m to 4000ft/1200m @ 100kbps, 300ft/90m at 10Mbps. Sync applications only.

Table 14 V.35 Connector Pinning



M/34 Male



M/34 Female

Pin	Signal	Abbr.	DTE	DCE
A	Chassis Ground		-	-
B	Signal Ground		-	-
C	Request To Send	RTS	Out	In
D	Clear To Send	CTS	In	Out
E	Data Set Ready	DSR	In	Out
F	Data Carrier Detect	DCD	In	Out
H	Data Terminal Ready	DTR	Out	In
J	Local Loopback	LL	In	Out
K	Local Test		Out	In
L	Unassigned			

Pin	Signal	Abbr.	DTE	DCE
M	Unassigned			
N	Unassigned			
P	Send Data A	TxD-	Out	In
R	Receive Data A	RxD-	In	Out
S	Send Data B	TxD+	Out	In
T	Receive Data B	RxD+	In	Out
U	Terminal Timing A		Out	In
V	Receive Timing A		In	Out
W	Terminal Timing B		Out	In
X	Receive Timing B		In	Out
Y	Send Timing A		In	Out
Z	Unassigned			
AA	Send Timing B		In	Out
BB	Unassigned			
CC	Unassigned			
DD	Unassigned			
EE	Unassigned			
FF	Unassigned			
HH	Unassigned			
JJ	Unassigned			
KK	Unassigned			
LL	Unassigned			
MM	Unassigned			
NN	Unassigned			

11.3.6 G.703 Electrical Interface

G.703 is a standard originally described voice over digital networks. Voice to digital conversion according to PCM requires a bandwidth of 64 kbps (+/- 100 ppm), resulting in the basic unit for G.703. By multiplication this results in e.g. T1 (1544 kbps) and E1 (2048 kbps). G.703 is the electrical and functional description.

Table 15 Some Definitions

G.704	Framing
G.706	CRC-4 procedure
G.732	Fault handling

G.703 can be transported over balanced (120 ohm TP) and unbalanced (dual 75 ohm coax) wires. The balanced version with a speed of 64kbps, is split in three different ways of transmission: co-directional (4-wire), central-directional (6/8 wire) and contra-directional (8-wire).

11.3.6.1 Co-Directional

This is a 4-wire version. Each direction (transmit, receive) consists of 2 wires twisted together, providing a balanced signal.

The data and timing are sent in the same direction over the same wires. This makes the data and timing signals co-directional.

Table 16 Some Electrical Characteristics

Mark	1.0 Vdc
Space	0 Vdc +/- 0.10 Vdc
Pulse width	3.9 µsec

The bit coding is done in three steps.
Step1: A binary 1 is replaced by 1100 and a binary 0 by 1010.
Step2: Conversion into a three-level signal (alternate mark inversion or AMI) by alternating the polarity of consecutive blocks.
Step3: Conversion to Violated AMI. Every 8th block of the polarity is alternated. The violated block marks the last bit in an octet.

11.3.6.2 Central –Directional

This is a rarely used version. The clock signals are supplied on different wires from a centralized clock. The centralized could be an atomic-clock. The reason for eight or six wire version is the possibility to send a clock signal balanced in both directions at the same time, or in each direction separate. The first has six wires (two clock, four data), the second has eight wires (four clock, four data).

Table 17 Some Electrical Characteristics

Mark	1.0 Vdc
Space	0 Vdc +/- 0.10 Vdc
Pulse width	15.6 µsec

The modulation technique used is alternate mark inversion (AMI).

11.3.6.3 Contra-Directional

This is always an 8-wire version. There are, of course, the transmit and receive pair and two pairs for the clock signals. All clock signals are sent to the DTE. This means they are all originated by the DCE.

Table 18 Some Electrical Characteristics

Mark	1.0 Vdc
Space	0 Vdc +/- 0.10 Vdc
Pulse width	15.6 µsec

The modulation technique used is AMI.

11.3.6.4 Speeds higher than 64kbps

All other speeds use a different coding scheme and different pulse width, also the mark and space voltages may differ. A quick overview for the most common used:

Table 19 Some Electrical Characteristics for T1

Cabling	co-directional
Mark	3.0 Vdc
Space	0 Vdc +/- 0.30 Vdc
Pulse width	647 nsec
Encoding	AMI (bipolar) or B8ZS
Speed	1544 kbps +/- 50 ppm

Table 20 Some Electrical Characteristics for E1

Cabling	Coaxial or one symmetrical pair (4 wires) for each direction
Mark	Balanced: 3.0 Vdc Unbalanced: 2.37 Vdc
Space	Balanced: 0 Vdc +/- 0.237 Vdc Unbalanced: 0 Vdc +/- 0.3 Vdc
Pulse width	488 nsec
Encoding	AMI or High Density Bipolar of order 3 (HDB3)
Speed	2048 kbps +/- 50 ppm

For a more detailed description see the corresponding documents about the E-series and T-series.

Table 21 Pinning Specifications

Signal	RJ45 Description	DTE RJ45	BNC Description	DTE BNC
RxA	Receive Input Negative	1	Receive Input	Tip
RxB	Receive Input Positive	2	Receive Ground	Ring
TxA	Transmit Output Negative	4	Transmit Output	Tip
TxB	Transmit Output Positive	5	Transmit Ground	Ring
S1	Transmit Ground	3		
S2	Receive Ground	6		

11.3.7 RS530 Electrical Interface

The RS530 interface is a generic connector specification. It's not an actual interface. The connector pinning can be used to support RS422, RS423, V.35 and X.21. The purpose is to replace the large RS449 Sub-D37 connector.

RS530 uses a differential signaling on a DB25 connector. The interface is used for HIGH SPEED synchronous protocols. Using differential signaling allows for higher speeds over long cabling.

This standard is applicable for use at data signaling rates in the range from 20,000 to a nominal upper limit of 2,000,000 bits per second.

Table 22 RS530 Pinning Specifications

Pin	Name	Dir	Description	Circuit	Paired with
1		—	Shield		18
2	TxD	→	Transmitted Data	BA	14
3	RxD	←	Received Data	BB	16
4	RTS	→	Request To Send	CA	19
5	CTS	←	Clear To Send	CB	13
6	DSR	←	Data Set Ready	CC	22
7	SGND	—	Signal Ground	Ground	21
8	DCD	←	Data Carrier Detect	CF	10
9		←	Rtrn Receive Sig. Elmnt Timing	DD	17
10		←	Rtrn DCD	CF	8
11		→	Rtrn Transmit Sig. Elmnt Timing	DA	24
12		←	Rtrn Transmit Sig. Elmnt Timing	DB	15
13		←	Rtrn CTS	CB	5
14		→	Rtrn TxD	BA	2
15		←	Transmit Signal Element Timing	DB	12

Pin	Name	Dir	Description	Circuit	Paired with
16		←	Rtrn RxD	BB	3
17		←	Receive Signal Element Timing	DD	9
18	LL	→	Local Loopback	LL	1
19		→	Rtrn RTS	CA	4
20	DTR	→	Data Terminal Ready	CD	23
21	RL	→	Remote Loopback	RL	7
22		←	Rtrn DSR	CC	6
23		→	Rtrn DTR	CD	20
24		→	Transmit Signal Element timing	DA	11
25		←	Test Mode	TM	

11.3.8 Electrical Interface Comparison

Table 23 Electrical Interface Comparison Table

Interface	Data Rate	Distance	Isolation	Connector	Comments
RS449 / V.11	64Kbps to 2Mbps	1000m at low bit rates	Balanced	DB-37	Serial Only
X.21 / V.11	64Kbps to 2Mbps	1000m at low bit rates	Balanced	DB-15	
V.35; V.11 & V.28	64Kbps to 2Mbps	400m @ 48Kbps 15m @ 2Mbps	Balanced Data & Clock only	M/34	Considered Obsolete
G.703	64Kbps to 2Mbps	300m	Balanced	DB-15	Transformer Isolation Octet Timing Codirectional Contradirectional Timing

11.3.9 Serial Communications RS-422

American national standard ANSI/TIA/EIA-422-B (formerly RS-422) and its international equivalent ITU-T Recommendation V.11 (also known as X.27), are technical standards that specify the "electrical characteristics of the balanced voltage digital interface circuit"[6]. It provides for data transmission, using balanced or differential signaling, with unidirectional/non-reversible, terminated or non-terminated transmission lines, point to point, or multi-drop. In contrast to RS-485 (which is multi-point instead of multi-drop) EIA-422/V.11 does not allow multiple drivers but only multiple receivers.

Several key advantages offered by this standard include the differential receiver, a differential driver and data rates as high as 10 Mb at 12 meters (40 ft). The specification itself does not set an upper limit on data rate, but rather shows how signal rate degrades with cable length. The figure plotting this stops at 10 Mbit/s.

EIA-422 only specifies the electrical signaling characteristics of a single balanced signal. Protocols and pin assignments are defined in other specifications. The mechanical connections for this interface are specified by EIA-530 (DB-25 connector) or EIA-449 (DC-37 connector), however devices exist which have 4 screw-posts to implement the “transmit” and “receive” pair only. The maximum cable length is 1200 m. Maximum data rates are 10 Mbit/s at 12 m or 100 kbit/s at 1200 m. EIA-422 cannot implement a truly multi-point communications network (such as with EIA-485), however one driver can be connected to up to ten receivers.

When used in relation to communications wiring, RS-422 wiring refers to cable made of 2 sets of twisted pair, often with each pair being shielded, and a ground wire. While a double pair cable may be practical for many RS-422 applications, the RS-422 specification only defines one signal path and does not assign any function to it. Any complete cable assembly (i.e. with connectors) should be labeled with the specification that defined the signal function and mechanical layout of the connector, such as RS-449.

Table 24 Some Electrical Characteristics for RS422

Physical Media	Twisted Pair
Network Topology	Point-to-point, Multi-dropped
Maximum Devices	10 (1 driver & 10 receivers)
Maximum Distance	1200 meters (4000 feet)
Mode of Operation	Differential
Maximum Baud Rate	10Mbps - 100Kbps
Voltage Levels	-6V to +6V (maximum Voltage)
Mark(1)	Negative Voltages
Space(0)	Positive voltages
Available Signals	Tx+, Tx-, Rx+, Rx- (Full Duplex)
Connector types	Not specified, Commonly Screw terminals

12. Physical Communication Media- Fiber Optic

12.1 Introduction

The use of optical fiber media has dramatically increased in the last fifteen years. This is due to multi vendor availability, much lower purchase and installation costs, dielectric characteristics, increased bandwidth potentials, and communications speed. Optical fibers are available as part of the overhead ground wire, in a self supported dielectric conductor, as a messenger conductor, or designed for underground environment. Utilities are using a variety of installation options to build a very reliable communications backbone with minimum common mode failures. Fiber optics is especially attractive when utilizing available bandwidth to combine communications needs of the electric utility, e.g., telecommunications, SCADA, video, data, voice, switching. With currently

available fusion and mechanical splices, approximately 100 km (60 miles) of single mode 1550nm optical fiber with 0.20 - 0.40 decibels per kilometer (dB/km) attenuation can be used without a repeater, and slightly less distance with lower cost 1330nm fiber.

A fiber optic pair available for exclusive use by the relays provides optimal performance for digital communications. Dedicated fiber gives a fast and error-free point-to-point connection. The main drawback is that a fiber cut will cause channel interruption for a long period of time, and many utilities lack expertise and equipment for replacing and splicing a damaged fiber cable. Of course, the installation and material costs for a dedicated fiber compared to conventional communication channels limits its availability for relaying.

Two optical fiber categories with distinctive operational attributes are multimode and single-mode fibers. The distance of the communication link generally dictates whether to use multi-mode or single-mode fiber.

Typical losses per km are:

Multimode step index	3.0 dB @ 850 nm
Multimode graded index	1 – 2 dB @ 1330 nm
Single mode step index	0.35 dB @ 1330 nm and 0.2 dB @ 1550 nm

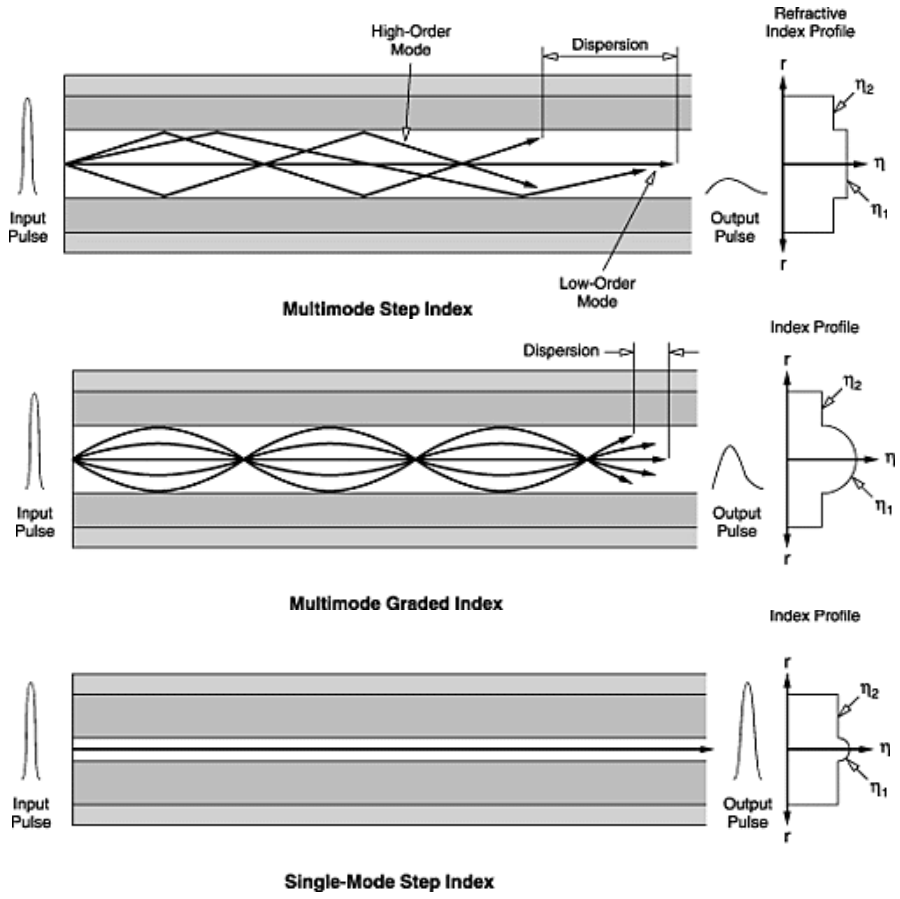


Figure 37 – Optical Fibers

As shown above, two basic types of multimode fibers exist. The simpler and older type is a "step index" fiber that has higher losses than the "graded index" fiber. Multi-mode is used for shorter distances, up to about 16 km (10 miles). All inter-substation fiber optic connections are generally made with multimode mode fiber due to the lower cost. A typical example of an inter-substation connection is the C37.94 relay-to-multiplexer fiber interface that is limited to 2 km (1.25 miles).

For longer distances, single mode fiber is used, with LED or laser optical transmitters. Laser provides longer reach but is more expensive. The longest distances, 100 km (60 miles) or longer, are achieved with single mode, 1550 nm fiber and laser optical transmitter. Relays and teleprotection devices often have a number of interfaces to choose from. To determine the required relay interface, an estimate should be made based on the actual installation, fiber loss and specified system gain, for example:

Table 25 Optical Budget

Optical Transmitter Power	- 17 dBm
Connector loss (2 dB per connector x 2)	- 4 dB
Splice loss (0.4 dB/splice x 4)	- 1.2 dB
Fiber loss 1310 nm single-mode (0.25 dB x 10 km)	- 2.5 dB
Receive signal Level	- 24.7 dBm
Receiver Sensitivity	- 40.0 dBm
System Margin	15.3 dB (≥ 3 dB recommended)

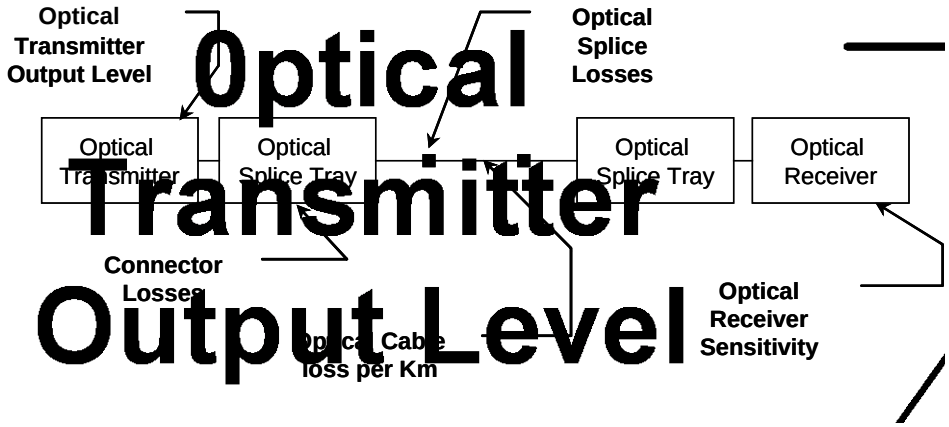


Figure 38 – Losses in dedicated fiber applications

Note that some relay designs will not accept too high received signal level as this may over-drive the receiver circuitry. As the relay is not able to read the received signal, it will alarm for loss-of-channel. This might happen if a communications interface with high output level is used on a short fiber with too little attenuation, or during back-to-back bench testing. The remedy is to add

an attenuator in the fiber circuit, or, if bench-testing, attenuate the circuit temporarily by loosening the fiber connector.

12.2 Fiber Optic Connectors

In the development of fiber optic technology over the last 30 years, many companies and individuals have invented the "better mousetrap" - a fiber optic connector that was lower loss, lower cost, easier to terminate or solved some other perceived problem. In all, about 100 fiber optic connectors have been introduced to the marketplace, but only a few represent the majority of the market.

12.3 Design

Most fiber optic connectors are plugs or so-called male connectors with a protruding ferrule that holds the fibers and aligns two fibers for mating. They use a mating adapter to mate the two connectors that fits the securing mechanism of the connectors (bayonet, screw-on or snap-in.) The ferrule design is also useful as it can be used to connect directly to active devices like LEDs, vertical-cavity surface-emitting lasers (VCSELs) and detectors. The follow sections provide information on the most popular fiber optic connector used in Ethernet networks for protection and control applications.

12.3.1 ST

ST (an AT&T Trademark) is probably still the most popular connector for multimode networks (ca. 2005), like most buildings and campuses. It has a bayonet mount and a long cylindrical 2.5 mm ceramic (usually) or polymer ferrule to hold the fiber. Most ferrules are ceramic, but some are metal or plastic. A mating adapter is used to mate two connectors (shown below.) And because STs are spring-loaded, you have to make sure they are seated properly. If you have high loss, reconnect them to see if it makes a difference.

The ST/SC/FC/FDDI/ESON connectors have the same ferrule size - 2.5 mm or about 0.1 inch - so they can be mixed and matched to each other using hybrid mating adapters. This makes it convenient to test, since you can have a set of multimode reference test cables with ST or SC connectors and adapt to all these connectors.

Figure 39 - ST Connector

12.3.2 SC

SC is a snap-in connector also with a 2.5 mm ferrule that is widely used for its excellent performance. It was the connector standardized in TIA-568-A, but was not widely used at first because it was twice as expensive as a ST. Now it's only a bit more expensive and much more common. It's a snap-in connector that latches with a simple push-pull motion. It is also available in a duplex configuration.

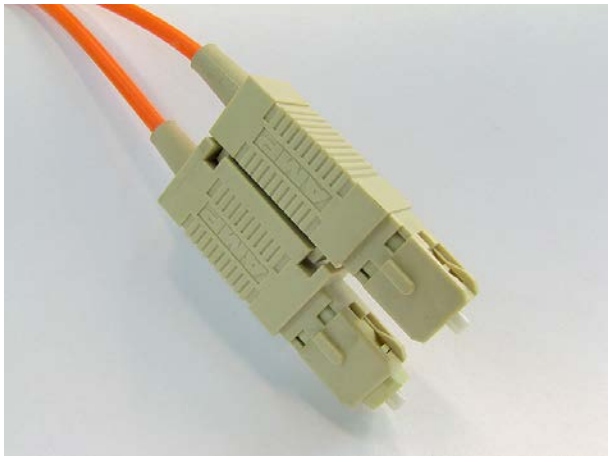


Figure 40 - SC Connector

12.3.3 FC

FC was one of the most popular single-mode connectors for many years. It also uses a 2.5 mm ferrule, but some of the early ones use ceramic inside stainless steel ferrules. It screws on firmly, but you must make sure you have the key aligned in the slot properly before tightening. It's been mostly replaced by SCs and LCs.

Figure 41 - FC Connector

12.3.4 LC

LC is a small form factor connector that uses a 1.25 mm ferrule, half the size of the SC. Otherwise, it's a standard ceramic ferrule connector, easily terminated with any adhesive. Good performance, highly favored for single-mode.

The LC, MU and LX-5 use the same ferrule but cross-mating adapters are not easy to find.

Figure 42 - LC Connector

12.3.5 MT-RJ

MT-RJ (*Mechanical Transfer Registered Jack*) uses a form factor and latch similar to the RJ-45 connectors. Two separate fibers are included in one unified connector. It is easier to terminate and install than ST or SC connectors. The smaller size allows twice the port density on a face plate than ST or SC connectors do. There are two variations: pinned and no-pin. The pinned variety, which has two small stainless steel guide pins on the face of the connector, is used in patch panels to mate with the no-pin connectors on MT-RJ patch cords.

Figure 43 - MT-RJ Connector

Dedicated fiber application for relaying is very straight-forward, but there might be a need to make sure that the fibers for the connection between the relay and the optical splice tray have the correct connectors ahead of time. The most common fiber connector is ST but some relays might require FC-PC connectors. An ST connector will then not work and if the splice tray uses ST connectors a special cable with FC-PC in one end and ST in the other is required. This modification is not easily done at site as special tools are needed to cut and fuse the fiber to the connector.

13. Physical Communications Media- Microwave and Wireless

13.1 Microwave

In the power system industry "microwave" refers to a type of communications used for transmitting and receiving signals from one location to another. Microwave communications transmits and receives signals through the air with the use of radios and antennas. The frequency range of the radio signals used in microwave communications is between 300MHz and 300GHz. Specific frequencies within the microwave range are regulated and assigned to various users by governing organizations around the world (e.g. Federal Communications Commission (FCC) in the United States, Radio Society of Great Britain (RSGB) in Great Britain, etc.).

One of the advantages of microwave over lower frequency radios is that it has a large bandwidth, which means it has a greater number of frequencies available to be allocated for individual users. Also, because the wavelength of microwave frequencies is very short, it is possible to use highly directional antennas that are relatively small in size – this makes it more practical than lower frequency communications, which have longer wavelengths and require large antennas. However, microwave is restricted to relatively short "line of sight" communication paths. Therefore, repeater stations are required to transmit and receive signals that have mountains or other obstacles between the sending and receiving locations. Additional advantages of microwave include:

- Microwave supports a wide variety of network requirements, such as voice, data, and video.
- Leasing costs for telephone lines are eliminated
- Except for tower locations, microwave is not restricted by "Right of Way" requirements.
- Microwave system expansion and service are under the control of the utility.

- Unlike power line carrier, the microwave path is not affected during transmission line faults.

Microwave communications is used throughout a power system to control and operate high voltage equipment located at remote locations. Some of the common uses include; transfer trip, telemetry (line loading), remote operation of high voltage equipment (power circuit breakers, transformer tap changers, etc.), telephone communications, as well as remote status and indication of power system equipment (alarms, open/close indication).

Microwave communications is achieved utilizing either analog or digital multiplexing techniques. Analog microwave is quickly being replaced with digital equipment, which offers greater channel capacity. Analog microwave systems use frequency division multiplexing (FDM) to achieve high channel capacity. A standard telephone channel (300 to 3400 Hz) is allocated a 4 kHz bandwidth. Twelve channels will require 48 kHz bandwidth, and is referred to as a "Group", and are frequency division multiplexed to the 60 kHz, to 108 kHz range. Five such groups will require 240 kHz. Of bandwidth, and further frequency division multiplexed a frequency spectrum of 312 kHz to 552 kHz, and is referred to as a Super Group. As shown in Figure 44 the frequency division process continues until the available microwave bandwidth is consumed.

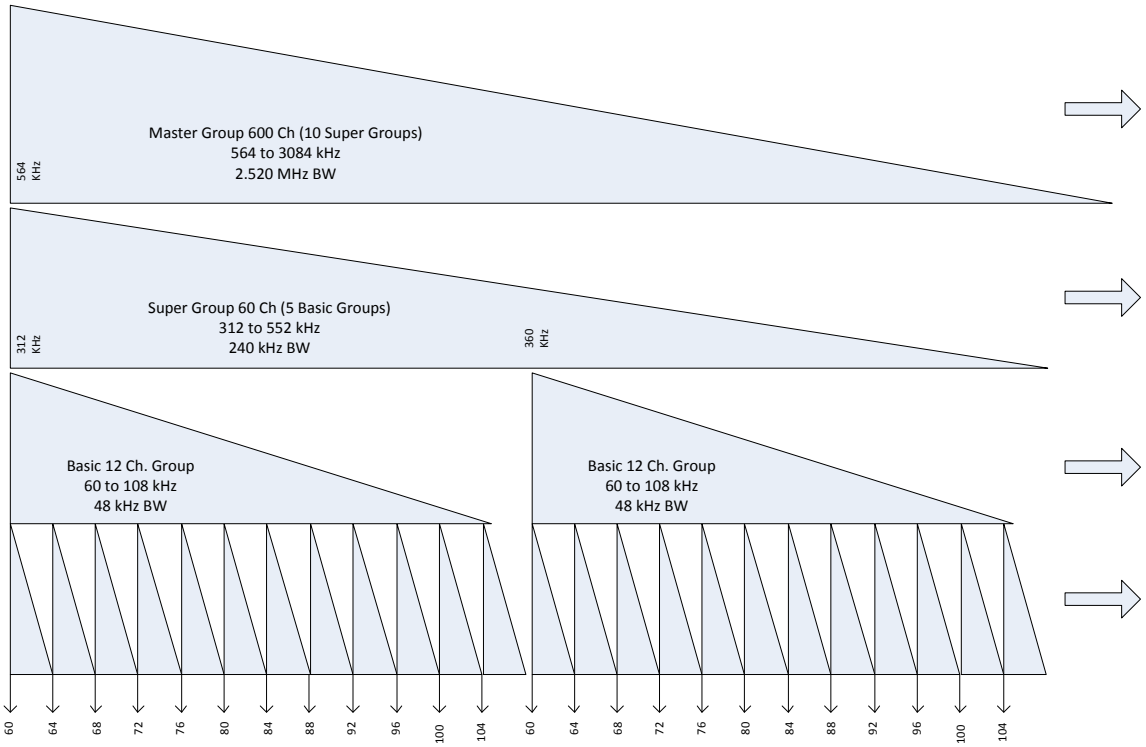


Figure 44 – Analog Microwave FDM Carrier System

Terrestrial digital microwave signals are electromagnetic waves in the radio frequency spectrum above 890 MHz and below 20 GHz. Microwave is frequently applied to span or skip natural land and water barriers and man-made barriers. Microwave systems are point to point with a maximum distance of 50 to 100 km (30 to 60 miles) before the need to regenerate or repeat signals.

In digital microwave systems the data modems, required in an analog system, are replaced by digital channel banks. These channel banks can be combined to form a multiplexed system as shown in Figure 45. The channel banks convert analog voice, and data inputs into a digital format using Pulse Code Modulation (PCM). The digital channel bank combines 24 voice channels into a standard 1.544 Mbps DS-1 signal. The DS-1 level is further multiplexed into DS-3 before transmitted over the radio link.

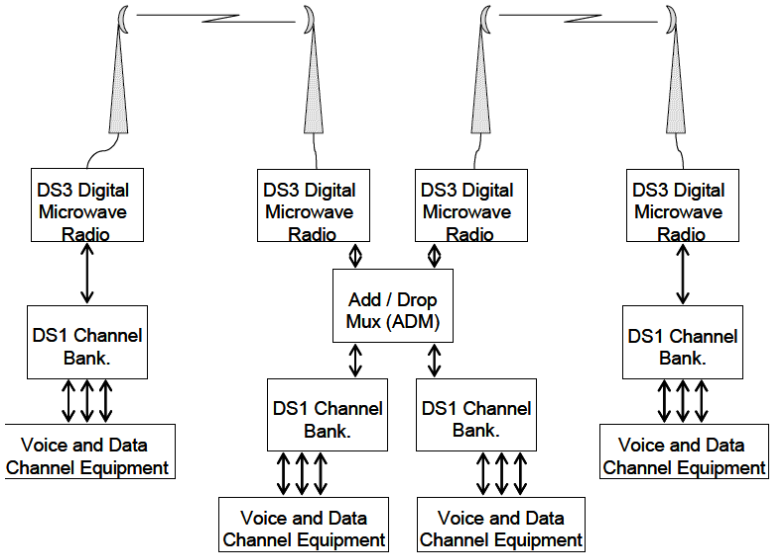


Figure 45 - Typical digital microwave system

13.1.1 Microwave losses

Good microwave system design should properly coordinate frequencies, provide for signal degradation due to multipath fading and atmospheric and weather conditions, use proper power and antenna for the application, and where possible make use of original analog microwave path licenses with "grandfathered" regulatory and environmental rules.

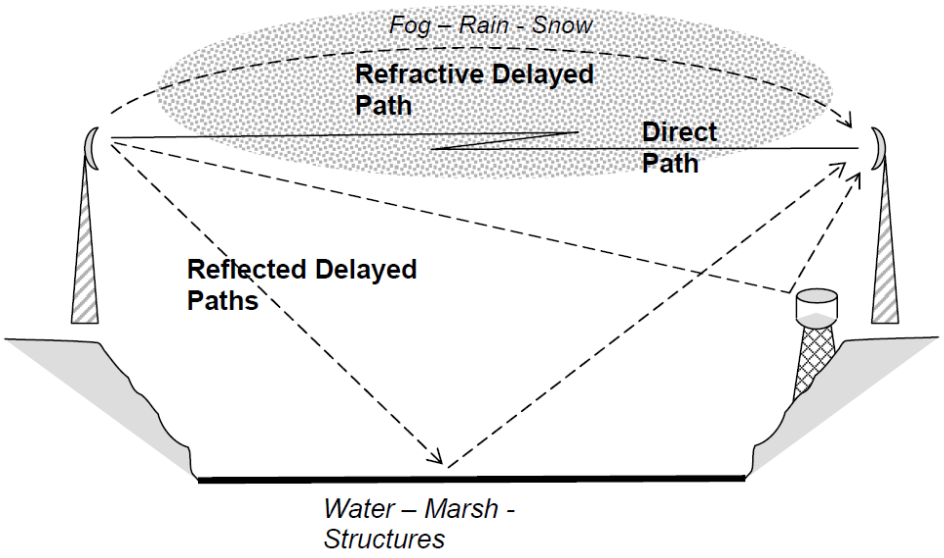


Figure 46 - Microwave propagation and multi-path delay impairment

The microwave signal is vulnerable to losses in free space as the signal travels from the transmitter to the receiver antennas. These losses occur from weather conditions, and obstructions, in and around the signal path.

To compensate for signal fading, two different methods can be used; space diversity or frequency diversity. Space diversity is the more common method and is obtained by adding a second receiving antenna at another height on the tower. Since signal cancellation is unlikely to occur simultaneously on both antennas, space diversity enhances system reliability. Frequency diversity requires two transmitters and two receivers, running simultaneously. Since a cancellation is unlikely to occur at two different frequencies simultaneously, system reliability is enhanced. Due to the additional equipment and bandwidth required, frequency diversity is used only by government agencies.

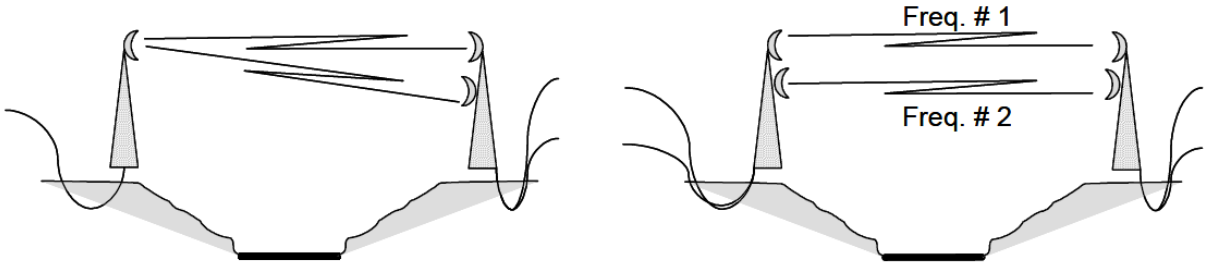


Figure 47 - Space diversity (left) and Frequency diversity (right)

13.1.2 Digital Microwave Channel Performance

Digital microwave, due to its complex digital coding schemes, offers better performance, i.e., improved signal to noise ratios and lower dollar equipment costs, is now the preferred terrestrial

transmission method, and will continue to dominate the microwave market segment in the future. Digital microwave operates in the 2, 4, 6, or 11 GHz bands.

Channel delays on digital microwave are very short, typically 500 to 600 us, making them suitable for high speed relaying. The switching time allowed by SONET standards is 100 ms. After a signal fade, antenna switch, or lightning strike, the receivers must re-synchronize to the signal before they can demodulate and process the information. A concern for relaying is fading during inclement weather conditions as this is when power system faults are most likely to occur.

13.2 Wireless (other than microwave)

13.2.1 Spread Spectrum Radio

The use of Spread Spectrum radios has become a popular low-cost alternative to more traditional modes of communication. The radios operate in one of the 900 MHz, 2.4 GHz, or 5.7 GHz range RF bands set aside for unlicensed radio. They are used for communications for small SCADA applications, or relay data acquisition. They can be used for communication for relaying pilot schemes as well. They have the advantage of not requiring any right-of-way or physical conductor for the communications. The remote radios operate on low power levels and do not require licenses. They do require line-of-sight paths and reasonably short distances for adequate signal strength.

13.2.2 Cellular Telephone

A similar alternative to the Spread spectrum radio is the use of cellular telephone for similar applications. They would have an advantage where obtaining radio line of sight or locating towers for antennas are not feasible. The cellular option is valid as long as acceptable wireless phone signal strength is available [7].

13.3 Digital Radio

Digital radio is increasingly used by the electric utility industry for a large variety of general and emerging specialized applications. A number of different radio systems exist, e.g., VHF and UHF, trunked, cellular, and multiple-address system (MAS) which are primarily for portable mobile applications.

VHF (30-172 MHz) and UHF (450-512 MHz) radio has not been used for general protection applications due to possible unavailability along with propagation limitations. Consequently applications have generally been limited to direct transfer trip for low speed less critical applications.

Trunked radio in the 800 MHz, band, primarily designed for shared voice communications, is not used as protection channel because of variable user congestion and lack of security.

Cellular mobile radio operates in the 800-900 MHz range (824-849 MHz Rx / 869-894 MHz Tx) and is a shared channel technology. When a user desires to use a communication path, a signal is sent to a central controller that responds telling the user what channel to use. This channel

assignment may stay the same throughout the data transfer or may switch at any time. Noise, adjacent channel interference, changes in channel speed, overall speed, channel switching during data transfer, power limitations, and lack of security make this type of channel undesirable for protective relaying.

With the availability of personal digital service (PCS) digital cellular technology comes devices designed for data transport. As the time division multiple access (TDMA) and the code division multiple access (CDMA) products mature, protection concerns, such as real time communications requirements may be met allowing limited relay applications. Future CDMA is of particular interest due to its secure spread spectrum technology and its power line applications in digital power line carrier.

14. TCP/IP

The **Internet Protocol Suite** (commonly known as **TCP/IP**) is the set of communications protocols used for the Internet and other similar networks. It is named from two of the most important protocols in it: the Transmission Control Protocol (TCP) and the Internet Protocol (IP), which was the first two networking protocols defined in this standard. Today's IP networking represents a synthesis of several developments that began to evolve in the 1960s and 1970s, namely the Internet and LANs (Local Area Networks), which emerged in the mid- to late-1980s, together with the advent of the World Wide Web in the early 1990s.

The Internet Protocol Suite, like many protocol suites, may be viewed as a set of layers. Each layer solves a set of problems involving the transmission of data, and provides a well-defined service to the upper layer protocols based on using services from some lower layers. Upper layers are logically closer to the user and deal with more abstract data, relying on lower layer protocols to translate data into forms that can eventually be physically transmitted.

The TCP/IP model consists of four layers. From lowest to highest, these are the Link Layer, the Internet Layer, the Transport Layer, and the Application Layer.

14.1 History

The Internet Protocol Suite resulted from research and development conducted by the Defense Advanced Research Projects Agency (DARPA) in the early 1970s. After initiating the pioneering ARPANET in 1969, DARPA started work on a number of other data transmission technologies. In 1972, Robert E. Kahn joined the DARPA Information Processing Technology Office, where he worked on both satellite packet networks and ground-based radio packet networks, and recognized the value of being able to communicate across both. In the spring of 1973, Vinton Cerf, the developer of the existing ARPANET Network Control Program (NCP) protocol, joined Kahn to work on open-architecture interconnection models with the goal of designing the next protocol generation for the ARPANET.

By the summer of 1973, Kahn and Cerf had worked out a fundamental reformulation where the differences between network protocols were hidden by using a common internetwork protocol. In this reformulation, instead of the network being responsible for reliability, as in the ARPANET,

the hosts became responsible. Cerf credits Hubert Zimmerman and Louis Pouzin, designer of the CYCLADES network, with important influences on this design.

The design of the network included the recognition that it should provide only the functions of efficiently transmitting and routing traffic between end nodes and that all other intelligence should be located at the edge of the network, in the end nodes. Using a simple design, it became possible to connect almost any network to the ARPANET, irrespective of their local characteristics, thereby solving Kahn's initial problem. One popular saying has it that TCP/IP, the eventual product of Cerf and Kahn's work, will run over "two tin cans and a string."

A computer called a *router* (a name changed from *gateway* to avoid confusion with other types of *gateway*s) is provided with an interface to each network, and forwards packets back and forth between them. Requirements for routers are defined in (Request for Comments 1812).

The idea was worked out in more detailed form by Cerf's networking research group at Stanford in the years1973–74, resulting in the first TCP specification (RFC 675). (The early networking work at Xerox PARC, which produced the PARC Universal Packet protocol suite, much of which existed around the same period of time, was also a significant technical influence; people moved between the two.)

DARPA then contracted with BBN Technologies, Stanford University, and the University College London to develop operational versions of the protocol on different hardware platforms. Four versions were developed: TCP v1, TCP v2, a split into TCP v3 and IP v3 in the spring of 1978, and then stability with TCP/IP v4 — the standard protocol still in use on the Internet today.

In 1975, a two-network TCP/IP communications test was performed between Stanford and University College London (UCL). In November, 1977, a three-network TCP/IP test was conducted between sites in the US, UK, and Norway. Several other TCP/IP prototypes were developed at multiple research centers between 1978 and 1983. The migration of the ARPANET to TCP/IP was officially completed on January 1, 1983, when the new protocols were permanently activated.

In March 1982, the US Department of Defense declared TCP/IP as the standard for all military computer networking. In 1985, the Internet Architecture Board held a three day workshop on TCP/IP for the computer industry, attended by 250 vendor representatives, promoting the protocol and leading to its increasing commercial use.

14.2 TCP/IP Layers

The TCP/IP suite uses encapsulation to provide abstraction of protocols and services. Such encapsulation usually is aligned with the division of the protocol suite into layers of general functionality. In general, an application (the highest level of the model) uses a set of protocols to send its data down the layers, being further encapsulated at each level.

This may be illustrated by an example network scenario, in which two Internet host computers communicate across local network boundaries constituted by their internetworking gateways (routers).

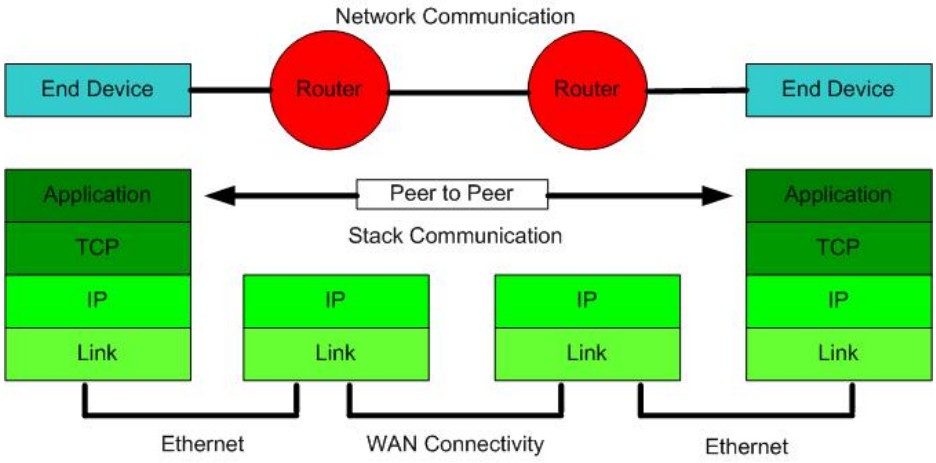


Figure 48 – TCP / IP Layers

The functional groups of protocols and methods are the Application Layer, the Transport Layer, the Internet Layer, and the Link Layer. It should be noted that this model was not intended to be a rigid reference model into which new protocols have to fit in order to be accepted as a standard.

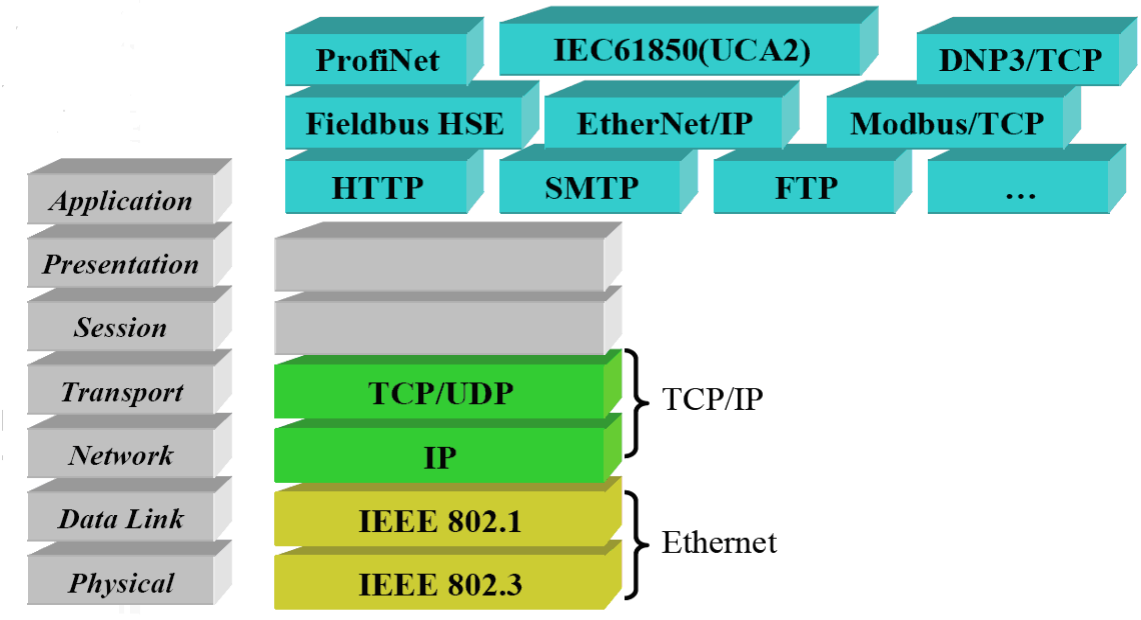


Figure 49 – Location of TCP/IP and Communication Protocols within the OSI model Stack

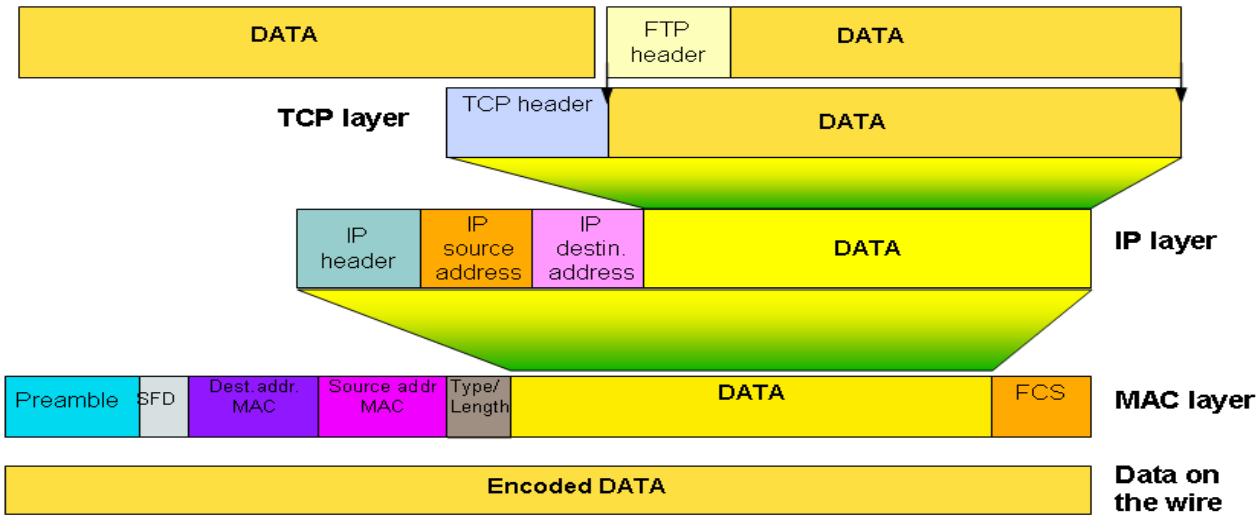


Figure 50 – Example of Ethernet Frame Hierarchy

The following table provides some examples of the protocols grouped in their respective layers.

Table 26 Protocol Grouping by Layers

Application	DNS, TFTP, TLS/SSL, FTP, Gopher, HTTP, IMAP, IRC, NNTP, POP3, SIP, SMTP,SMPP, SNMP, SSH, Telnet, Echo, RTP, PNRP, rlogin, ENRP
	Routing protocols like BGP and RIP, which run over TCP/UDP, may also be considered part of the Internet Layer.
Transport	TCP, UDP, DCCP, SCTP, IL, RUDP, RSVP
Internet	IP (IPv4, IPv6), ICMP, IGMP, and ICMPv6
	OSPF for IPv4 was initially considered IP layer protocol since it runs per IP-subnet, but has been placed on the Link since RFC 2740.
Link	ARP, RARP, OSPF (IPv4/IPv6), IS-IS, NDP

14.3 IP Addressing

An **Internet Protocol** (**IP**) **address** is a numerical label that is assigned to devices participating in a computer network utilizing the Internet Protocol for communication between its nodes. An IP address serves two principal functions in networking: host or network interface identification and location addressing. The role of the IP address has also been characterized as follows: "A name indicates what we seek. An address indicates where it is. A route indicates how to get there."

The original designers of TCP/IP defined an IP address as a 32-bit number and this system, known as Internet Protocol Version 4 or IPv4, is still in use today. However, due to the enormous growth of the Internet and the resulting depletion of available addresses, a new addressing system (IPv6), using 128 bits for the address, was developed in 1995 and last standardized by RFC 2460 in 1998. Although IP addresses are stored as binary numbers, they are usually displayed in decimal

notations, such as 208.77.188.166 (for IPv4), and hexadecimal as in 2001:db8:0:1234:0:567:1:1 (for IPv6).

IP Address Numbering Overview is included within the Ethernet section of this paper.

14.4 Static and dynamic IP addresses

When a computer is configured to use the same IP address each time it powers up, this is known as a Static IP address. In contrast, in situations when the computer's IP address is assigned automatically, it is known as a Dynamic IP address.

14.4.1 Method of assignment

Static IP addresses are manually assigned to a computer by an administrator. The exact procedure varies according to platform. This contrasts with dynamic IP addresses, which are assigned either by the computer interface or host software itself, as in Zeroconf, or assigned by a server using Dynamic Host Configuration Protocol (DHCP). Even though IP addresses assigned using DHCP may stay the same for long periods of time, they can generally change. In some cases, a network administrator may implement dynamically assigned static IP addresses. In this case, a DHCP server is used, but it is specifically configured to always assign the same IP address to a particular computer. This allows static IP addresses to be configured centrally, without having to specifically configure each computer on the network in a manual procedure.

In the absence or failure of static or stateful address configurations, an operating system may assign an IP address to a network interface using state-less autoconfiguration methods, such as Zeroconf.

14.4.2 Uses of dynamic addressing

Dynamic IP addresses are most frequently assigned on LANs and broadband networks by Dynamic Host Configuration Protocol (DHCP) servers. They are used because it avoids the administrative burden of assigning specific static addresses to each device on a network. It also allows many devices to share limited address space on a network if only some of them will be online at a particular time. In most current desktop operating systems, dynamic IP configuration is enabled by default so that a user does not need to manually enter any settings to connect to a network with a DHCP server. DHCP is not the only technology used to assigning dynamic IP addresses. Dialup and some broadband networks use dynamic address features of the Point-to-Point Protocol.

14.4.2.1 Sticky dynamic IP address

A sticky dynamic IP address or sticky IP is an informal term used by cable and DSL Internet access subscribers to describe a dynamically assigned IP address that does not change often. The addresses are usually assigned with the DHCP protocol. Since the modems are usually powered-on for extended periods of time, the address leases are usually set to long periods and simply renewed

upon expiration. If a modem is turned off and powered up again before the next expiration of the address lease, it will most likely receive the same IP address.

15. Ethernet

Ethernet is a type of network cabling and signaling specifications (OSI Model layers 1 [physical] and 2 [data link]) originally developed by Xerox in the late 1970s. In 1980, Digital Equipment Corp. (DEC), Intel, and Xerox (the origin of the term DIX, as in DEC/Intel/Xerox) began joint promotion of this baseband, Carrier Sense, Multiple Access / Collision Detection (CSMA/CD) computer communications network over coaxial cabling, and published the "Blue Book Standard" for Ethernet Version 1. This standard was later enhanced, and in 1985 Ethernet II was released.

The IEEE's (Institute of Electrical and Electronics Engineers') Project 802 then (after considerable debate) used Ethernet Version 2 as the basis for the 802.3 CSMA/CD network standards. The IEEE 802.3 standard is generally interchangeable with Ethernet II, with the greatest difference being the construction of the network packet header.

As electronics and networking have grown, the Ethernet standard has developed to include the new technologies, but the basic mechanics of operation of every Ethernet network stems from Mr. Metcalfe's original design at the Xerox Corporation's Palo Alto Research Center. The original Ethernet design described communication over a single cable shared by all devices on the network. The beauty of Ethernet is that once a device is connected to the network via the single cable, it will establish communication with other attached devices. This allows the network to expand to accommodate new devices without requiring any modification to those devices already on the network [26].

In the early days, Ethernet networks were set up in what is called a multi-drop network based on Metcalfe's original "Ether" trunk, where devices "tapped" into the information highway. Ethernet network topologies have since evolved into star networks that include hubs, switches, and routers. A hub is a passive device that passes or buses all the information on the network to every connected device. An Ethernet switch is an intelligent hub; like the hub, it passes the data to all connected devices but includes the capability to decode parts of those messages and uses this decoded information to direct the traffic to the appropriate address. Switches also introduced a major improvement over the hubs, that is, the ability to virtually eliminate collisions by managing the data via store-and-forward methods that act in a deterministic fashion. The process is prescribed in the Ethernet Carrier Sense Multiple Access with Collision Detection (CSMA/CD) protocol. Finally, routers are similar to switches, except they add the function of routing traffic from a LAN to another LAN, thus creating a Wide Area Network (WAN).

The original speed of Metcalfe's Ethernet was 2.94 Megabit per second, which very quickly was increased to 10 Megabit per second, pushed to 100 Megabit per second, 1 Gigabit per second, and most recently to 10 Gigabit per second. Driven by Moore's Law and manufacturing economies of scale, the price of Ethernet technology is continually falling.

15.1 Ethernet Brief History

Today Ethernet is the predominant networking technology used in office and home environments.

Because Ethernet networks are inexpensive and fairly well understood, their use is quickly becoming popular for industrial and utility applications including substation automation networks.

Despite the fact that Ethernet networks were not developed specifically for operation in substations and other harsh environments, Ethernet is so popular in other applications that it is easier and simpler to utilize and enhance Ethernet than to create something new. New Ethernet equipment has been designed to operate reliably in extreme harsh environment.

Only 15 years ago, most Human Machine Interfaces (HMIs) operated on dedicated mainframe computers with terminals rather than the legion of personal computers that is used today. Early personal computer HMIs used custom operating systems dedicated to HMI operation. While dedicated systems are more stable and reliable, today's systems often cost from 10 to 1 percent of the expense of dedicated single-purpose systems.

Both industrial and utility networking experts are moving forward accepting the limitations of Ethernet networks and solving the problems associated with Ethernet networks. Advances in computing power and network technology allow us to take advantage of the popularity and availability of Ethernet networking equipment and solutions [8].

15.2 The OSI Model - Ethernet

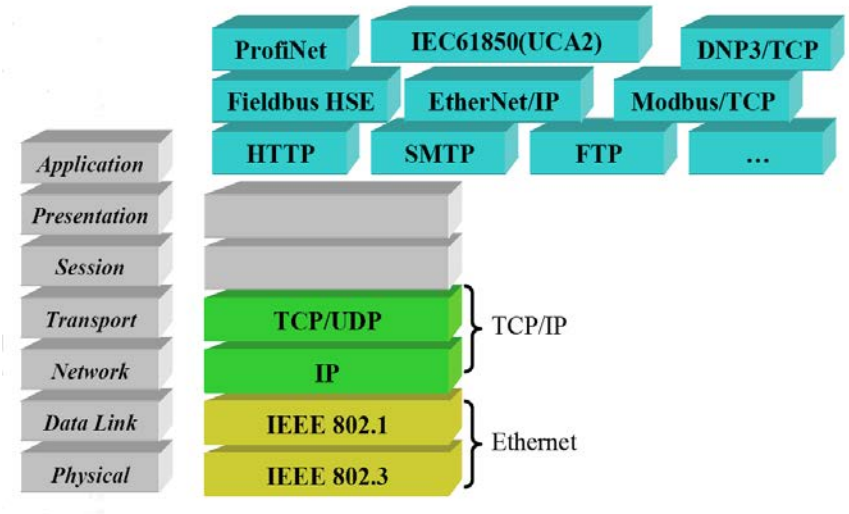


Figure 51 – OSI Model Ethernet

If we apply the OSI Model to an Ethernet system, they become as shown in the Figure 51, which can be described as follows:

- ***Layer 7 (Application Layer):*** The application layer refers communication services to applications. Examples: Telnet, FTP, TFTP and SNMP
- ***Layer 6 (Presentation Layer):*** This layer's main purpose is defining data formats, such as ASCII text, EBCDIC text, binary, BCD, and JPEG.
- ***Layer 5 (Session Layer):*** The session layer defines how to start, control, and end conversations (called sessions).
- ***Layer 4 (Transport Layer):*** Transport layer functionalities would include either reliable or unreliable transmission, flow control and error recovery could be implemented in this layer as well. Examples: UDP and TCP.
- ***Layer 3 (Network):*** This layer defines end-to-end delivery of packets. To accomplish this, the network layer defines logical addressing so that any endpoint can be identified. It defines how routing works also defines how to fragment packets into smaller packets to accommodate media with smaller maximum transmission unit sizes. Examples: IP, IPX, AppleTalk.
- ***Layer 2 (Data link):*** Data link protocols define delivery across an individual link. These protocols are necessarily concerned with the type of media in question. Examples: IEEE 802.3/802.2, HDLC, Frame Relay, PPP and ATM.
- ***Layer 1 (Physical):*** Physical layer deals with the physical characteristics of the transmission medium including connectors, pins, use of pins, electrical currents, encoding, and light modulation. Examples: Ethernet 802.3, 802.4 Token Bus and 802.5

15.3 The Ethernet Packet

See the information below which describes the structure of the Ethernet Packet that can be used to illustrate the structure and possible size of each packet. The Ethernet packet preamble is normally generated by the chipset. Software is responsible for the destination address, source address, type and data. The chips normally will append the frame check sequence.

62 bits	***Preamble:*** **A series of alternating 1's and 0's used by the ethernet receiver to acquire bit synchronization. This is generated by the chip.**
2 bits	***Start of Frame:*** **Two consecutive 1 bits used to acquire byte alignment. This is generated by the chip.**
6 bytes	***Destination Ethernet Address:*** **Address of the intended receiver. The broadcast address is all 1's**
6 bytes	***Source Ethernet Address:*** **The unique Ethernet address of the sending station**
2 bytes	***Length or Type of field:*** **For IEEE 802.3 this is the number of bytes of data. For Ethernet I & II, this is the type of packet. Types of codes are > 1500 to allow both to coexist. The type code for IP packets is 0x800.**
46 bytes To 1500 bytes	***Data:*** **Short packets must be padded to 46 bytes**
4 bytes	***Frame Check Sequence:*** **The FCS is a 32 bit CRC calculated using the AUTODIN II Polynomial. This field is normally generated by the chip**

Figure 52 – The Ethernet Packet

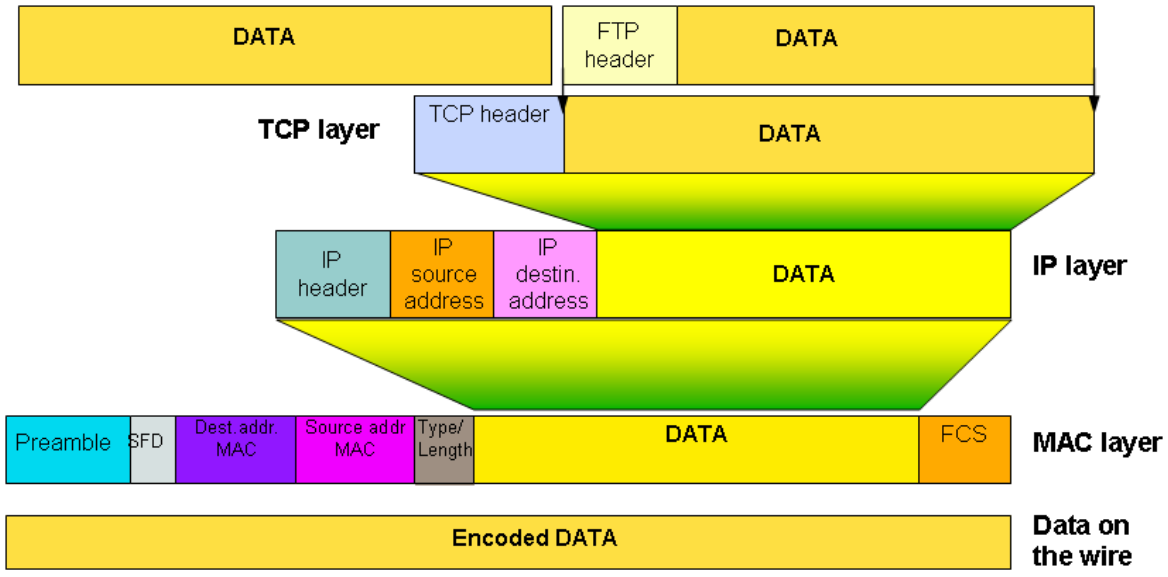


Figure 53 – Example of Ethernet Packet in Actual Orientation

For example:

The shortest packet is: 6 + 6 + 2 + 46 + 4 = 64 bytes

The longest packet is: 6 + 6 + 2 + 1500 + 4 = 1518 bytes

15.4 An Introduction to IP- Internet Protocol

15.4.1 What is IP?

The Internet Protocol (IP) is the method or protocol by which data is sent from one computer to another on the Internet. Each computer or IP capable device (known as a host) on the Internet has at least one IP Address that uniquely identifies it from all other computers on the Internet. When you send or receive data (for example, an e-mail or a Web page URL), the message gets divided into little chunks called packets. Each of these packets contains both the sender's IP address and the receiver's IP address. Any packet is sent first to a gateway device (Router) that understands a small part of the Internet. The gateway reads the destination address and forwards the packet to an adjacent gateway that in turn reads the destination address and so forth across the Internet until one gateway recognizes the packet as belonging to a computer within its immediate neighborhood or domain. That gateway then forwards the packet directly to the computer whose address is specified.

IP is a connectionless protocol, which means that there is no continuing connection between the end points that are communicating. Each packet that travels through the Internet is treated as an independent unit of data without any relation to any other unit of data. (The reason the packets do get put in the right order is because of TCP, the connection-oriented protocol that keeps track of the packet sequence in a message.) In the Open Systems Interconnection (OSI) communication model, IP is in layer 3, the Networking Layer.

The most widely used version of IP today is Internet Protocol Version 4 (IPv4). However, IP Version 6 (IPv6) is well on its way to be implemented. IPv6 provides for much longer addresses and therefore for the possibility of many more Internet users. IPv6 includes the capabilities of IPv4 and any server that can support IPv6 packets can also support IPv4 packets.

15.4.2 Ethernet and IP- how do they work?

There are 2 concepts to keep in mind when talking about Ethernet and IP:

- Ethernet is a communications transport protocol that operates at layers 1 and 2 of the OSI model
- IP is an umbrella of communications protocols that operate at layer 3 and above on the OSI model and that fall under 2 specific categories- UDP and TCP- with another internal control protocol called ICMP

15.4.2.1 TCP- Transmission Control Protocol

TCP (Transmission Control Protocol) is a set of rules (protocol) used along with the Internet Protocol (IP) to send data in the form of message units between computers over the Internet. While IP takes care of handling the actual delivery of the data, TCP takes care of keeping track of the individual units of data (called packets) that a message is divided into for efficient routing through the Internet.

TCP is known as a connection-oriented protocol, which means that a connection is established and maintained until such time as the message or messages to be exchanged by the application programs at each end have been exchanged. TCP is responsible for ensuring that a message is divided into the packets that IP manages and for reassembling the packets back into the complete message at the other end. In the Open Systems Interconnection (OSI) communication model, TCP is in layer 4, the Transport Layer.

15.4.2.2 UDP- User Datagram Protocol

User Datagram Protocol (UDP) is a communications protocol that offers a limited amount of service when messages are exchanged between computers in a network that uses the Internet Protocol (IP). UDP is an alternative to the Transmission Control Protocol (TCP) and, together with IP, is sometimes referred to as UDP/IP. Like the Transmission Control Protocol, UDP uses the Internet Protocol to actually get a data unit (called a datagram) from one computer to another. Unlike TCP, however, UDP does not provide the service of dividing a message into packets (datagrams) and reassembling it at the other end. Specifically, UDP doesn't provide sequencing of the packets that the data arrives in. This means that the application program that uses UDP must be able to make sure that the entire message has arrived and is in the right order. Network applications that want to save processing time because they have very small data units to exchange (and therefore very little message reassembling to do) may prefer UDP to TCP. The Trivial File Transfer Protocol (TFTP) uses UDP instead of TCP.

UDP provides two services not provided by the IP layer. It provides port numbers to help distinguish different user requests and, optionally, a checksum capability to verify that the data arrived intact.

In the Open Systems Interconnection (OSI) communication model, UDP, like TCP, is in layer 4, the Transport Layer.

15.4.2.3 ICMP- Internet Control Message Protocol

ICMP (Internet Control Message Protocol) is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the IP software and are not directly apparent to the application user.

It is good to think of ICMP as the health monitor of the Internet. PING (Packet InterNet Groper) is a type of ICMP message that is used to determine if a device is reachable by IP or not. There are many other types of ICMP messages such as TraceRT, WhoIS, Finger and many more.

15.5 Ethernet OSI Layer 1- Physical Layer

15.5.1 Physical cabling

Ethernet cabling falls into two categories; 4 pair twisted pair cabling that follows what is called a Category, or CAT, standard and fiber optic glass based cable.

15.5.1.1 Twisted pair cabling-

A type of cable that consists of two independently insulated wires twisted around one another. The use of two wires twisted together helps to reduce crosstalk and electromagnetic induction. While twisted-pair cable is used by older telephone networks and is the least expensive type of local-area network (LAN) cable, most networks contain some twisted-pair cabling at some point along the network.

15.5.1.2 Unshielded Twisted Pair (UTP) Cable

Twisted pair cabling comes in two varieties: shielded and unshielded. Unshielded twisted pair (UTP) is the most popular and is generally the best option for school networks (See Figure 54).

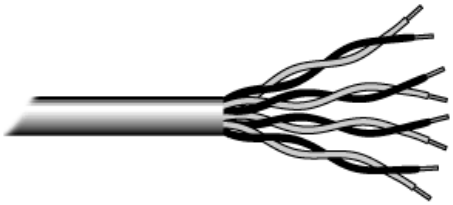


Figure 54 – Unshielded twisted pair

The quality of UTP may vary from telephone-grade wire to extremely high-speed cable. The cable has four pairs of wires inside the jacket. Each pair is twisted with a different number of twists per inch to help eliminate interference from adjacent pairs and other electrical devices. The tighter the twisting of the cable, the higher the supported transmission rate and the greater the cost per foot. The EIA/TIA (Electronic Industry Association/Telecommunication Industry Association) has established standards of UTP and rated six categories of wire (additional categories are emerging).

Table 27 Categories of Unshielded Twisted Pair

Category	Speed	Use
1	1 Mbps	Voice Only (Telephone Wire)
2	4 Mbps	LocalTalk & Telephone (Rarely used)
3	16 Mbps	10BaseT Ethernet

4	20 Mbps	Token Ring (Rarely used)
5	100 Mbps (2 pair) 1,000 Mbps (4 pair)	100BaseT Ethernet Gigabit Ethernet
5e	1,000 Mbps	Gigabit Ethernet
6	10,000 Mbps	Gigabit Ethernet

15.5.1.3 Unshielded Twisted Pair Connector

The standard connector for unshielded twisted pair cabling is an RJ-45 connector. This is a plastic connector that looks like a large telephone-style connector (See Figure 55). A slot allows the RJ-45 to be inserted only one way. RJ stands for Registered Jack, implying that the connector follows a standard borrowed from the telephone industry. This standard designates which wire goes with each pin inside the connector.

Figure 55 – RJ-45 Connector

15.5.1.4 Shielded Twisted Pair (STP) Cable

Although UTP cable is the least expensive cable, it may be susceptible to radio and electrical frequency interference (it should not be too close to electric motors, fluorescent lights, etc.). If you must place cable in environments with lots of potential interference, or if you must place cable in extremely sensitive environments that may be susceptible to the electrical current in the UTP, shielded twisted pair may be the solution. Shielded cables can also help to extend the maximum distance of the cables.

- Shielded twisted pair cable is available in three different configurations:
- Each pair of wires is individually shielded with foil.
- There is a foil or braid shield inside the jacket covering all wires (as a group).
- There is a shield around each individual pair, as well as around the entire group of wires (referred to as double shield twisted pair).

The following is the pin-out description for Ethernet cables for both UTP and STP:

15.5.1.5 RJ-45 pinout

1. Data 1+
2. Data 1-
3. Data 2+

4. Not Assigned
5. Not Assigned
6. Data 2-
7. Signal Common (0 V) for Data 1
8. Signal Common (0 V) for Data 2

15.6 Ethernet OSI Layer 2

15.6.1 Ethernet Layer 2 Structure

Ethernet Layer 2 communications is actually broken up into 2 sections, the Data Link Layer and the MAC (Media Access Control) Layer.

15.6.1.1 Data Link Layer

The **Data Link Layer** is Layer 2 of the seven-layer OSI model. It corresponds to or is part of the link layer of the TCP/IP reference model. The Data Link Layer is the protocol layer which transfers data between adjacent network nodes in a wide area network or between nodes on the same local area network segment. The Data Link Layer provides the functional and procedural means to transfer data between network entities and might provide the means to detect and possibly correct errors that may occur in the Physical Layer. Examples of data link protocols are Ethernet for local area networks (multi-node), the Point-to-Point Protocol (PPP), High-Level Data Link Control (HDLC) and Advanced Data Communication Control Protocol (ADCCP) for point-to-point (dual-node) connections.

The Data Link Layer is concerned with local delivery of frames between devices on the same LAN. Data Link frames, as these protocol data units are called, do not cross the boundaries of a local network. Inter-network routing and global addressing are higher layer functions, allowing Data Link protocols to focus on local delivery, addressing, and media arbitration. In this way, the Data Link layer is analogous to a neighborhood traffic cop; it endeavors to arbitrate between parties contending for access to a medium.

15.6.1.2 Media Access Control (MAC) Layer

The **Media Access Control** (**MAC**) data communication protocol sub-layer, also known as the Medium Access Control, is a sub-layer of the Data Link Layer specified in the seven-layer OSI model (layer 2). It provides addressing and channel access control mechanisms that make it possible for several network hosts to communicate within a multi-point network, typically a local area network (LAN). The hardware that implements the MAC is referred to as a **Medium Access Controller**.

The MAC sub-layer acts as an interface between the Logical Link Control (LLC) sub-layer and the network's physical layer. The MAC layer emulates a full-duplex logical communication channel in a multi-point network. This channel may provide unicast, multicast or broadcast communication service.

15.6.1.3 What is a MAC Address?

A MAC address is the hardware address for any Ethernet device. The address is broken into 2 parts:

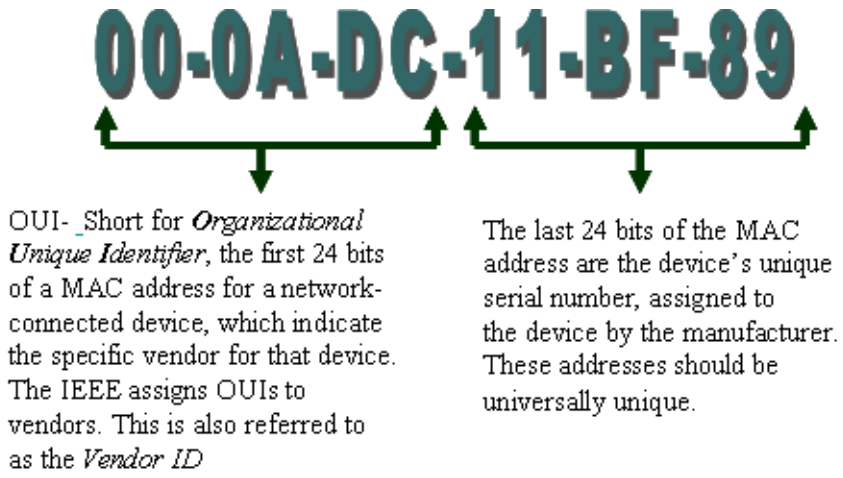


Figure 56 – MAC Address Format

MAC Address types:

00-0A-DC-11-22-33	This is an example of an address that is embedded within an Ethernet device. It is used in primarily unicast communication
FF-FF-FF-FF-FF-FF	The well Known format for Layer 2 Broadcast. FF in HEX format is 255. Switches flood (send out on all ports) broadcasts
01-00-5E-xx-xx-xx	This Organizational Unique Identifier (OUI) is the well known format for a Multicast MAC address. Switches handle multicasts the same as Broadcasts. Extra functionality such as Internet Group Management Protocol (IGMP) Snooping is added to help switches better handle multicasts.

15.6.2 Ether Layer 2 Protocols and Functions

15.6.2.1 VLANs- separating a physical network into logical parts

A **Virtual LAN**, commonly known as a **VLAN**, is a logical grouping of hosts with a common set of requirements that communicate as if they were attached to the same Broadcast domain, regardless of their physical location. A VLAN has the same attributes as a physical LAN, but it allows for end stations to be grouped together even if they are located across multiple Ethernet network switches. Network reconfiguration can be done through software instead of physically relocating devices.

The protocol most commonly used today in configuring virtual LANs is IEEE 802.1Q. The IEEE committee defined this method of multiplexing Virtual Local Area Networks (VLANs) in an effort

to provide multi-vendor VLAN support. Prior to the introduction of the 802.1Q standard, several proprietary protocols existed, such as Cisco's ISL and Cabletron's SecureFast protocol.

IEEE 802.1Q tagging performs "explicit tagging" - the frame itself is tagged with VLAN information. 802.1Q uses an internal field for tagging, and therefore does modify the Ethernet frame. This internal tagging is what allows IEEE 802.1Q to work on both access and trunk links: frames are standard Ethernet, and therefore can be handled by commodity hardware.

The IEEE 802.1Q header contains a 4-byte tag header containing a 2-byte tag protocol identifier (TPID) and 2-byte tag control information (TCI). The TPID has a fixed value of 0x8100 that indicates that the frame carries the 802.1Q/802.1p tag information. The TCI contains the following elements:

- Three-bit user priority
- One-bit canonical format indicator (CFI)
- Twelve-bit VLAN identifier (VID)-Uniquely identifies the VLAN to which the frame belongs – numbers from 1-4095
    - A VLAN tag number of 0 is not standard, but can be used for what is called a Priority tag. This will be addressed later.

Early network designers often configured VLANs with the aim of reducing the size of the collision domain in a large single Ethernet segment and thus improving performance. When Ethernet switches made this a non-issue (because each switch port is a collision domain), attention turned to reducing the size of the broadcast domain at the MAC layer. Virtual networks can also serve to restrict access to network resources without regard to physical topology of the network.

Virtual LANs operate at Layer 2 (the data link layer) of the OSI model. Administrators often configure a VLAN to map directly to an IP network, or subnet, which gives the appearance of involving Layer 3 (the network layer). In the context of VLANs, the term "trunk" denotes a network link carrying multiple VLANs, which are identified by labels (or "tags") inserted into their packets. Such trunks must run between "tagged ports" of VLAN-aware devices, so they are often switch-to-switch or switch-to-router links rather than links to end devices.

15.6.2.2 Redundancy Protocols

Ethernet switches in the network can be used to provide protocol redundancy and maintaining Ethernet network health. Layer 2 Redundancy protocols do two things: Identify all the possible paths amongst the networking devices and place the redundant extra paths in a blocking state to remove network loops. If these redundant paths are not removed, loops in an Ethernet network will be formed that will cause flooding due to data duplication and recirculation. This will choke a network in a short period of time. In the event a network segment fails, the protocol activates the appropriate ports that are in a blocking state to re-establish connectivity. The object being to fix the issue before the process even knows there is a problem.

Ethernet networks have redundancy protocols that are supported by identified Ethernet standards. These are supported in Layer 2 and Layer 3 of the OSI model. First we will look at Layer 2:

Standard Layer 2 Network Redundancy Protocols:

- **Spanning Tree** - There are several flavors of Spanning Tree.
    - STP (Spanning Tree Protocol) - Standardized in 1996 as IEEE 802.1D, it is the first and slowest of the Spanning Tree protocols. Average failover time for STP started at 30 seconds and went up. Much too slow for any industrial Process. Next came…
    - RSTP (Rapid Spanning Tree Protocol) – Currently standardized as IEEE802.1D 2004, it is an evolutionary leap for STP. It is more rapid, with failover times from about 250 msec to up to 12 seconds, so it was better than STP. Still an issue with the speed of failover for Industrial processes.
    - MSTP (Multiple Spanning Tree Protocol) - Originally standardized as IEEE 802.1S and then incorporated into IEEE 802.1Q 2003, it allows multiple instances of Spanning Tree Protocol per Virtual LAN. This means that in a single physical network, there can be multiple virtual network groupings, each with their own instance of Spanning Tree Protocol.
    - There are proprietary implementations of Spanning Tree that are optimized for use in Industrial Networks. They are based upon standard RSTP, but are not designated as a standard STP protocol.
- **LACP (Link Aggregation Control Protocol) -** This protocol allows the user to configure multiple Ethernet ports between Ethernet switches into a Single virtual “Link”. This allows load sharing of information between the links and is extremely fast in moving data between a failed port and an adjacent port if there is a link failure.

The amount of interconnections among the network elements dictates the amount of failures the network can take and still maintain the process. Refer to Figures 57 to 59 which show examples of these protocols.

15.6.2.3 Rapid Spanning Tree

Spanning Tree is a redundant topology in that it provides network redundancy instead of just path redundancy while preventing loops in a network. For Ethernet to function properly, only one active path can exist between devices. To provide redundancy, Spanning Tree relies on having multiple paths or connections to different switches and configures some of these paths into standby (Blocked) state. If a network segment becomes unreachable, spanning tree reconfigures and re-establishes link by activating the "Blocked" links.

All switches in the LAN gather information about each other through an exchange of data messages called BPDU's or Bridge Protocol Data Units. The exchange of messages causes the following:

- The election of a "Root" switch for stability.
- The election of a designated switch.
- The removal of loops by placing redundant switch ports in a backup state.

The "Root" switch is considered to be the "logical" center of the Spanning tree network. All paths that are not needed to reach the "Root" switch from anywhere in the network are placed in backup

mode. BPDU's contain information about the transmitting switch it came from and its ports including:

- Unique switch Identifier or MAC address.
- Switch priority
- Port priority
- Port cost.

Spanning Tree uses this information to elect the "Root" switch and "Root" port for the switched network.

The switches send configuration BPDU's to configure the spanning tree topology. All switches connected to the LAN receive the transmitted BPDU. The BPDU's are not forwarded by the switch, but the information contained in the BPDU can be used by the receiving switch to transmit a new BPDU.

The resulting action of this communication is:

- One switch is identified as the Root.
- The shortest distance to the root is determined for each switch.
- A designated switch or switch closest to the Root is selected.
- An active port from each switch is selected and the others are blocking.

If all the switches are enabled with default settings, the switch with the lowest MAC address becomes the root by default. However, due to traffic patterns, number of forwarding ports or just simply physical location, this may not be the best way to select the root switch. By increasing the priority (lowering the actual numerical value of the priority number) of the ideal switch so that it becomes the root, you are forcing spanning tree to recalculate and form a new topology. The same can be said for which port is active and which port stays in standby. By increasing the priority (lowering the actual numerical value of the priority number) of the ideal port so that it becomes active, you are forcing spanning tree to recalculate and form a new topology.

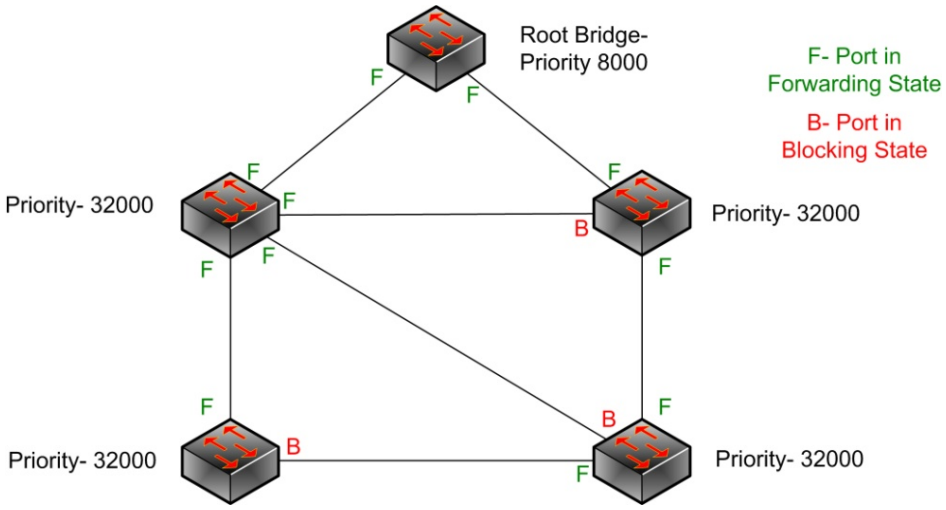


Figure 57 – Example of a Spanning Tree Ethernet Network

Spanning Tree networks can support either ring or mesh topologies. A ring topology is basically a ring of Ethernet Switches connected together in a ring fashion. A mesh topology requires the use of a couple of Ethernet switches up at the top with switches below that have a connection to both the upper switches. Mesh networks use more fiber than ring networks, but can typically survive more network hits intact. Figure 58 shows a typical Mesh network while Figure 59 shows a Ring network example.

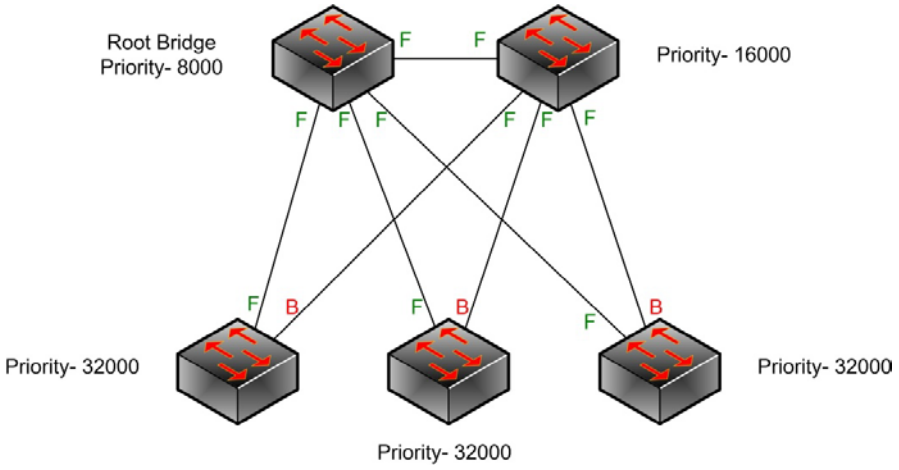


Figure 58 – Spanning Tree in a Mesh Network

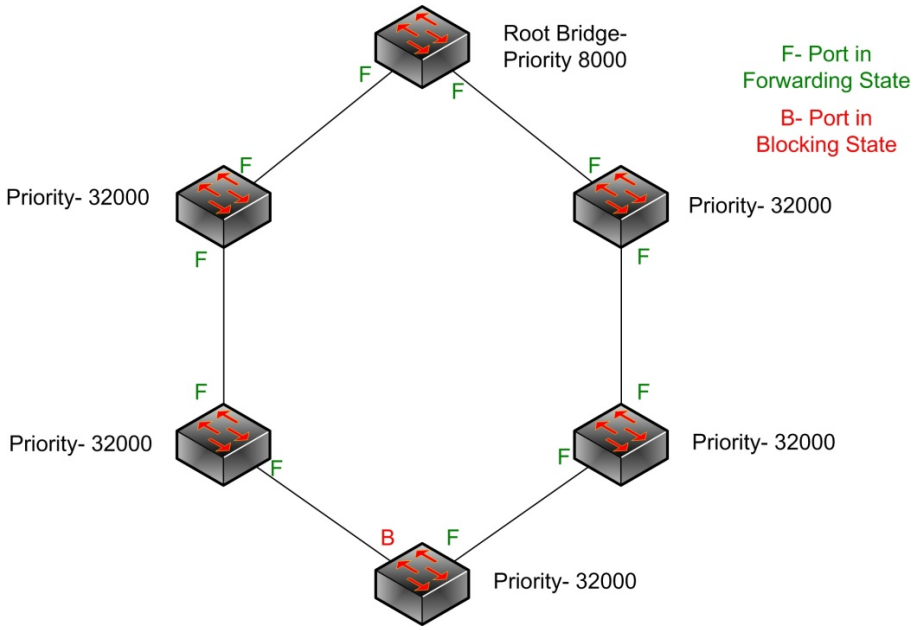


Figure 59 – Spanning Tree in a Ring

15.6.2.4 Link Aggregation Control Protocol (LACP)

Link Aggregation Control Protocol (LACP) (IEEE 802.1ad) provides redundancy without the use of Spanning Tree. It enables users to be able to bundle groups of ports between switches to form 1 virtual link with the bandwidth of the member links. LACP provides several functions:

- Higher bandwidth
- Enhanced Bandwidth Granularity
- Load sharing across the member links to balance bandwidth across the member links
- Fault tolerance provided by offloading data to working member links when a member link fails

LACP is a method of providing needed extra bandwidth between Ethernet switches that have extra non-utilized ports without buying a switch or switches with higher bandwidth ports. For example, moving from 100Mbps switching to Gigabit Ethernet switches.

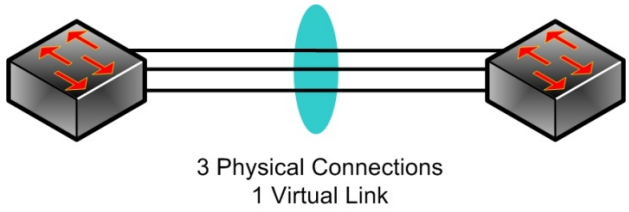


Figure 60 – Example of an LACP based Ethernet connection between switches

15.6.2.5 Class of Service (CoS) and Quality of Service (QoS) - One backs up the other…

Class of Service (CoS)-not to be confused with Quality of Service (QoS) - is a form of priority queuing that has been used in a number of communication and networking protocols. It is a way of classifying and prioritizing packets based on application type (voice, video, file transfers, transaction processing), the type of user (CEO, secretary), or other settings.

CoS is a queuing discipline while QoS covers a wider range of techniques to manage bandwidth and network resources. CoS classifies packets by examining packet parameters or CoS markings and places packets in queues of different priorities based on predefined criteria. QoS has to do with guaranteeing certain levels of network performance to meet service contracts or to support real-time traffic. With QoS, some method is used to reserve bandwidth across a network in advance of sending packets. In other words, QoS is the level of importance assigned to a type of traffic, CoS is the method employed to enforce it across the network.

The typical Ethernet switch supports 2 different types of Class of Service functions. The first, operating at layer 2 of the OSI model, is 802.1p. 802.1p is part of the 802.1Q VLAN tag structure utilizing the three priority tag bits of the tag. There is also a tag called a priority tag. It is a VLAN tag with a VLAN ID of 0 with the priority bits set. This is not standard but is widely supported on many managed Ethernet switches.

The second type of CoS is a layer three OSI function called Differentiated Service Control Point (DSCP). It uses the Type of Service (ToS) bits that are part of the Layer Three portion of the Ethernet frame. Many managed Ethernet switches are able to look at the ToS bits and then assign the frame to a priority queue on the switch port.

15.7 Ethernet OSI Layer 3- IP Layer Routers and Router redundancy

15.7.1 Introduction

As Ethernet networks expand, the use of a single IP subnet is not enough. In order to facilitate communication between IP Subnets, you need to use a Layer 3 network device, namely, a router. Routers can provide data movement in 2 ways: Statically via routes that are mapped by hand (Static Routing) or dynamically via designated routing protocols (Dynamic Routing).

Definition of a router: A device which provides a path from a node on one network or subnet to a node on another network

Definition of routing: the process of determining the end-to-end path between the sender and the receiver of a packet. There are 2 types:

- Source routing- the source node determines the route and includes it in special fields in the data frame. Source route bridging in Token Ring uses source.
- Hop-by-hop- The route between source and destination is determined along the way, hop by hop. Most routing protocols are hop-by-hop based.

The routing protocols most used are Routing Information Protocol (RIP), Routing Information Protocol Version 2 (RIPII) and Open Shortest Path First – Routing protocol (OSPF) for standard protocols.

Static routing can be useful for small routing areas, but does not provide fast failover because it requires user interaction to program and alternate the route manually. Dynamic routing is required where a hand off failover is required or the routing environment is large. Routing protocols are inherently slower on failover than layer 2 protocols.

Routers support several types of protocols to communication like OSPF and that have a communications redundancy built in as long as the physical network architecture remains in place.

There is also a router physical redundancy protocol. If one router fails, its designated backup is placed into service seamlessly as if the original never left. This is called VRRP, Virtual Router Redundancy Protocol. VRRP is the way for routers to perform physical redundancy to each other. If one router dies or is unable to function in the appropriate manner, its designated backup will take over the former router's function. They maintain this relationship through the use of HELLO packets and regular updates to make sure that both routers have all the same information. The use of VRRP would be a function to incorporate into an IEC61850 design if there is a requirement to attach to a corporate network and there is a requirement to maintain some sort of segregation between the substation IEC61850 network and the corporate environment. Figure 61 shows an example of VRRP.

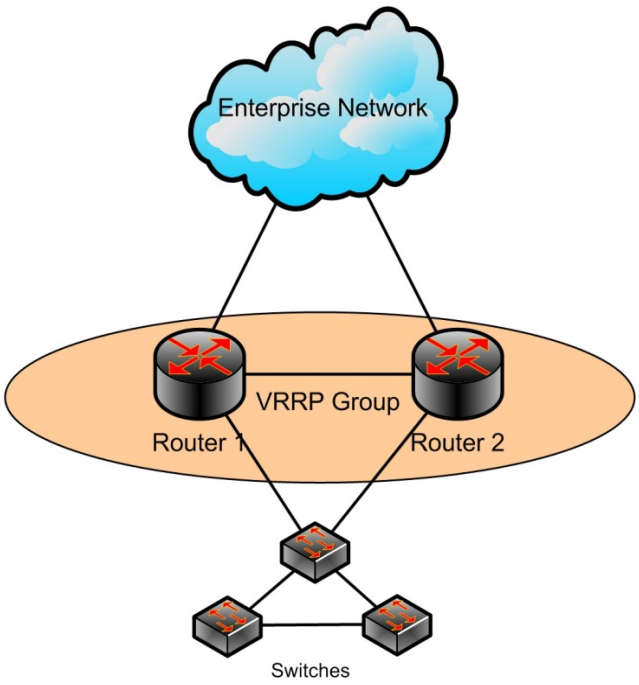


Figure 61 – VRRP Example

15.7.2 IP Addressing and Subnetting

An Internet Protocol (IP) address is a numerical label that is assigned to devices participating in a computer network utilizing the Internet Protocol for communication between its nodes. An IP address serves two principal functions in networking: host or network interface identification and location addressing. The role of the IP address has also been characterized as follows: *"A name indicates what we seek. An address indicates where it is. A route indicates how to get there."*

The original designers of TCP/IP defined an IP address as a 32-bit number and this system, known as Internet Protocol Version 4 or IPv4, is still in use today. However, due to the enormous growth of the Internet and the resulting depletion of available addresses, a new addressing system (IPv6), using 128 bits for the address, was developed in 1995 and last standardized by RFC 2460 in 1998. Although IP addresses are stored as binary numbers, they are usually displayed in human-readable notations, such as 208.77.188.166 (for IPv4), and 2001:db8:0:1234:0:567:1:1 (for IPv6).

The Internet Protocol also has the task of routing data packets between networks, and IP addresses specify the locations of the source and destination nodes in the topology of the routing system. For this purpose, some of the bits in an IP address are used to designate a subnetwork. The number of these bits is indicated in CIDR notation, appended to the IP address, e.g., *208.77.188.166/24*.

15.7.3 IPv4 Subnetting

In the early stages of development of the Internet Protocol, network administrators interpreted an IP address in two parts, network number portion and host number portion. The highest order octet (most significant eight bits) in an address was designated the *network number* and the rest of the bits were called the *rest field* or *host identifier* and were used for host numbering within a network. This method soon proved inadequate as additional networks developed that were independent from the existing networks already designated by a network number. In 1981, the Internet addressing specification was revised with the introduction of classful network architecture.

Classful network design allowed for a larger number of individual network assignments. The first three bits of the most significant octet of an IP address was defined as the *class* of the address. Three classes (*A*, *B*, and *C*) were defined for universal unicast addressing. Depending on the class derived, the network identification was based on octet boundary segments of the entire address. Each class used successively additional octets in the network identifier, thus reducing the possible number of hosts in the higher order classes (*B* and *C*). The following table gives an overview of this now obsolete system.

This is how the IP Address classes are divided up:

Table 28 IP Address Classification

Class	Range
A	1.0.0.0 to 127.255.255.255
B	128.0.0.0 to 191.255.255.255
C	192.0.0.0 to 223.255.255.255
D	224.0.0.0 to 239.255.255.255
E	240.0.0.0 to 255.255.255.255

15.8 Ethernet Network Types and Orientations

[9] Ethernet allows for a wide variety of network topologies providing different levels of redundancy, availability, performance and of course cost. There are three basic network architectures (Cascading, Ring, and Star) that are commonly implemented with Ethernet Switches with numerous variations and hybrids of the three. Each of the three basic architectures offers various performance vs. cost trade-offs.

15.8.1 Cascade

Each switch is connected to the previous switch or next switch in the cascade via one of its ports. These ports are sometimes referred to as uplink ports and are often operating at a higher speed than the ports connected to the IED's. The maximum number of switches, N, which can be cascaded depends on the worst case delay (latency) which can be tolerated by the system.

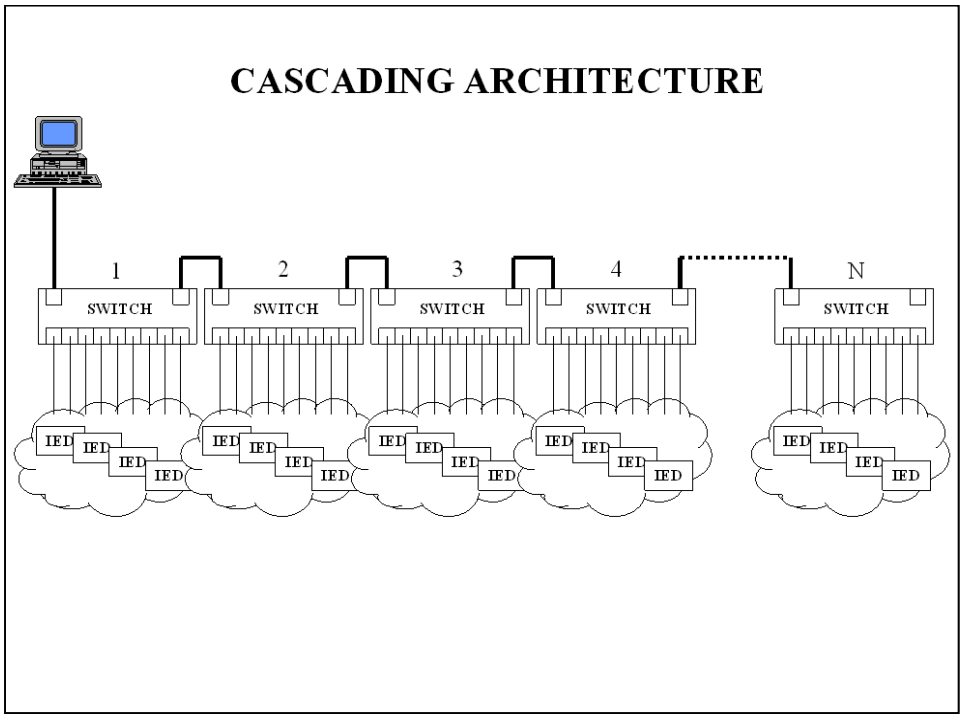


Figure 62 – Cascade topology in the substation [9]

15.8.2 Star Topology

The star topology is based on a “backbone” switch with all of the other switches uplinking to it.

Advantages:

- Lowest Latency - allows for lowest number of ‘hops’ between any two switches connected to the backbone switch N.

Disadvantages:

- No Redundancy – if the backbone switch fails all switches are isolated or if one of the uplink connections fails then all IED’s connected to that switch are lost.

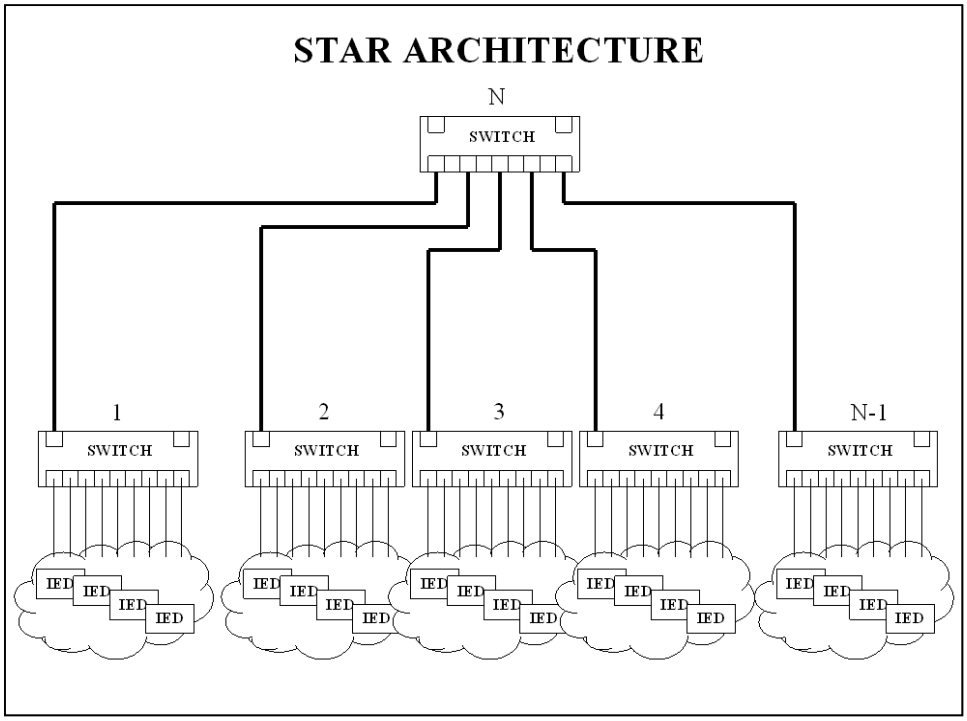


Figure 63 – Ethernet star topology in the substation [9]

15.8.3 Ring

The ring architecture provides some level of redundancy as compared to the star or cascade topologies due to the redundant path.

Theoretically, messages could circulate indefinitely in a loop and eventually eat up all of the available bandwidth. However, ‘managed’ switches take into consideration the potential for traffic loops and implement an algorithm called Spanning Tree Protocol (STP) which is defined in the IEEE 802.1D standard. Spanning Tree allows switches to detect loops and internally block messages from circulating in the loop. As a result managed switches with Spanning Tree actually

logically break the ring by blocking messages internally. This results in the equivalent of a cascading architecture with the advantage that if one the links should break the managed switches in the network will reconfigure to span out via two paths.

Advantages:

- Rings offer redundancy in the form of immunity to physical breaks in the network.
- IEEE 802.1w Rapid Spanning Tree Protocol allows sub-second network reconfiguration.
- Cost effective cabling/wiring allowed. Similar to Cascaded architecture.

Disadvantages:

- Latency – worst case delays across the cascading backbone have to be considered if the application is very time sensitive (similar to Cascading)
- All switches should be Managed Switches. This is not necessarily a disadvantage per se but simply an added complexity. Although, the advantages of Managed Switches often far outweigh the added complexity.

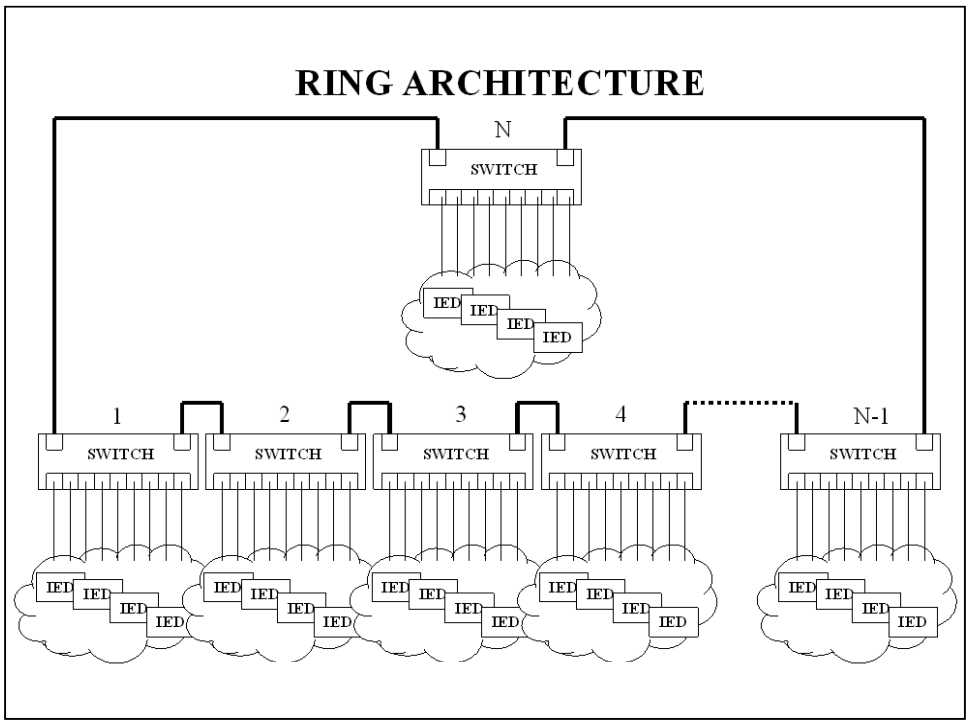


Figure 64 – Ethernet ring topology in the substation [9]

15.8.4 Hybrid Architecture

The Hybrid architecture combines star and ring topologies, as shown in the Figure 65. This architecture can withstand any one of the fault types shown in the Figure 65 and not lose communications between any of the IED's on the network. In this way, a high level of availability (i.e. uptime) is achieved.

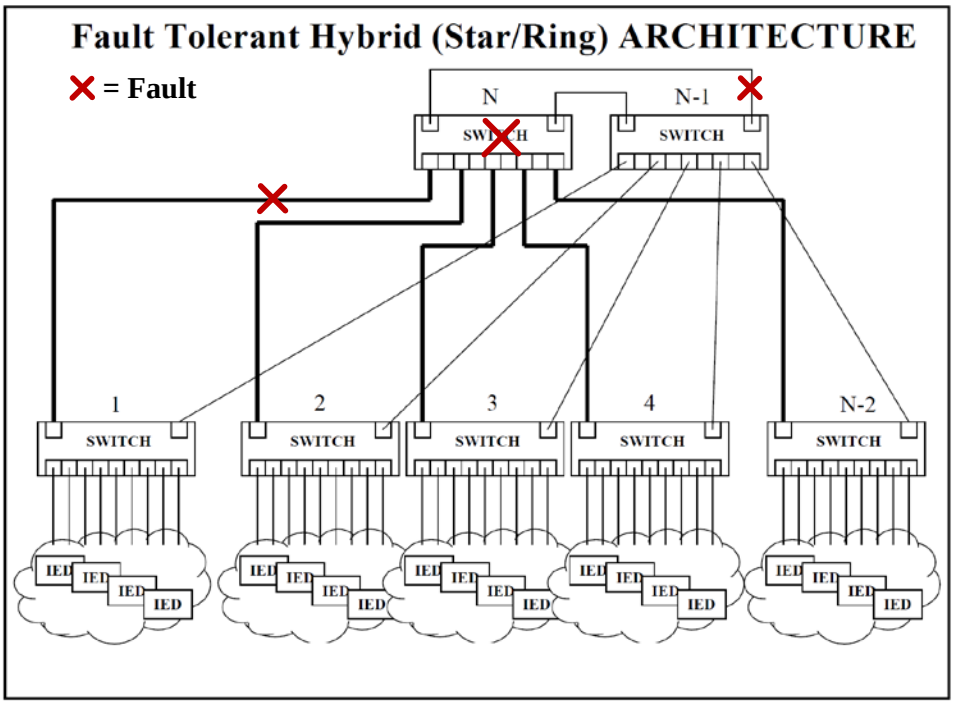


Figure 65 – Star/ring hybrid topology tolerant to link and core node faults [9]

15.8.5 Mesh Topology

A Mesh is a topology where devices are interconnected via many redundant paths, therefore increasing availability but also increasing complexity. In a mesh topology if any cable or node fails, there are many other ways for two nodes to communicate. Mesh topology is indeed present at the IP layer implicating routing but also it can be implemented at the Ethernet level through the use of a Spanning Tree as already described in *Section 15.6.2 Ether Layer 2 Protocols and Functions*.

Mesh topologies are commonly used in Wide Area Networks and in Wireless Sensor Networks.

Advantages:

- High levels of redundancy and availability /survivability
- Flexible architecture - The network can be expanded without disruption to other nodes

Disadvantages:

- Increasing complexity
- Difficult to manage and troubleshoot

15.8.6 Scalability

Scalability is the capability of the network to increase several orders of magnitude in performance and capacity in order to fulfill future network requirements. The scalability concerns the network's architecture, structure, technology and manageability but not necessarily the equipment.

In the power environment, many applications and services are not already implemented and therefore the scalability is one of the important parameters to be taken into account during the design stage.

The following gives some guidelines as to the scalability of the system:

- Architecture – A proper mix of layer 2 and layer 3 must be used to build the network architecture in order to control the performance and the security of the system in a scalable manner.
- Topology – Topology is generally a limiting factor to network growth. A pure topology as described previously (star, cascade or ring) cannot be scaled in a convenient manner. Scalability in the power environment implicates the use of a hybrid topology.
- MAC Addressing space – For large flat networks the size of the MAC address table can become very large. In order to keep the network scalable it is necessary to split the large Ethernet structures into multiple sub-networks separated through layer 3 (refer to Architecture here above).
- VLAN planning – The separation of the different categories of services into identified VLANs from the early design stage prevents the network from growing up to saturation.
- Manageability – Manageability is the aptitude to scale up and keep operating at a large scale without downtime or a large effort for administration. The architectural control described previously and avoiding too much complexity at each Ethernet level provides a scalable manageability.
- Protection mechanisms – Protection mechanism has also clear limitations relative to scalability. The protection strategy of the Ethernet structure must employ the different mechanisms (ring protection, Spanning Tree, layer 3 resilience) in a coordinated manner and combined to provide appropriately scalable resilience.

15.9 Comparing Serial with Ethernet Communications

Comparing the characteristics of serial vs. Ethernet communications, the following are the most important reasons why one must consider using one versus the other:

15.9.1.1 Reliability of Data Communication

The Ethernet is a secure and proven way of data communication with error connection handled by the hardware and the TCP world standard communication protocol. The primary limiting factor for shared-bus topologies like serial links is that of high input/output (I/O) and limited distance. Reliability is a problem with shared buses, as a failure in any single pin or connection will cause the whole interface to fail. Shared buses lack the expansion and I/O

capabilities to enable individual servers and storage racks to grow into multiple servers separated by distance.

15.9.1.2 Speed of Data Communication

Over Ethernet data is moving with a minimum speed of 1 Mbps with absolute error correction. Over an RS-232 the speed is at best one tenth of the Ethernet's minimum speed, with minimum or no error correction.

15.9.1.3 Safety of Data Communication

With the Ethernet port a socket is opened by the OS and no other application can get access to the data that is being transmitted, so no one can manipulate, change, or destroy the communication channel. Ethernet is a guarantee that the data is moved between the host and the IED without other applications running on the same PC to manipulate that data. With RS-232 the data can be manipulated and copied by other applications running the same PC.

15.9.1.4 Ethernet Has Better and Faster Recovery

Ethernet networks utilize redundant links and recovery protocols as protection techniques against link failures.

15.9.1.5 Standardized Cable and Connection

For the Ethernet network the engineer is using world class unshielded twisted pair (UTP) cables and plugs; however, in the serial world there is no standard of the cables.

15.9.1.6 Distance of Data Communication and Noise Immunity

When using Ethernet technology the data can be error free at high speed of 1 Mbps minimum over distances up to 50m. When using the RS-232 for speeds of 110kbps the theoretical distance for error free communication is relatively very short. This means that in the majority of cases the distance alone between the IED and the PC is a key factor to choose Ethernet over serial communications. Furthermore in noisy environments the Ethernet cable is proven to work while the RS-232 or RS-485 non standard cables offer no guarantee that noise will not corrupt data.

15.10 Ethernet in Substation Environment

[10] If Ethernet switches and serial servers are used in substation automation applications, they should comply with either IEC 61850-3 or IEEE P1613 standards for EMI immunity and environmental requirements to ensure reliable operation of networking equipment in substation environments.

For applications where the Ethernet network will be involved in critical protection functions, the Ethernet switches should comply with the ***Class 2*** device definition given in IEEE P1613 (i.e. error free communications during the application EMI immunity type tests).

Managed Ethernet switches with advanced Layer 2 and Layer 3 features such as the ones listed below, should be used to ensure real-time deterministic performance:

- IEEE 802.3 Full-Duplex operation (no collisions)
- IEEE 802.1p Priority Queuing
- IEEE 802.1Q VLAN
- IEEE 802.1w Rapid Spanning Tree
- IGMP Snooping / Multicast Filtering

A variety of flexible network architectures offering different levels of performance, cost and redundancy are achievable using managed Ethernet switches.

The following are a few reasons why migrating to Ethernet is the way of the future in substation automation:

- Enables Peer-to-Peer Communications
- Allow for Multiple Masters
- Client – Server vs. Master – Slave
- Higher data transfer
- Higher bandwidth

15.11 Enabling Peer-to-Peer Communications

Ethernet as a media has been mentioned a number of times and installing Ethernet-based LANs in substations is a growing trend. Peer-to-peer protection and control systems implemented over Ethernet address the available bandwidth problem that can occur with other peer-to-peer protocols. Any discussion of Ethernet in substations must include Generic Object Oriented Substation Events (GOOSE) messaging, part of the UCA 2.0/IEC 61850 protocol, a peer-to-peer protocol virtually dependent upon Ethernet. Peer-to-peer communication allows two or more IEDs (such as protection and control relays) to share information.

GOOSE messages are broadcast over the network on an exception basis. An IED will experience an event and then broadcast a predefined message over the network. Other devices on the network are programmed to listen to the entire message, a portion of it, or ignore the message altogether. To ensure the message gets received, the sending device will repeat the message's broadcast a number of times with exponentially increasing time delays between broadcasts.

Since GOOSE only sends data when needed, it reduces network traffic. However, GOOSE doesn't provide explicit knowledge of the message's presence (or absence) to its recipients. The user should also be aware that the UCA 2.0 and IEC implementations of GOOSE are somewhat different, though the IEC implementation appears to be destined as the preferred implementation. PeerComm is interoperable with both the UCA 2.0 and the IEC versions of GOOSE messaging.

In summary, peer-to-peer networks of relays and controls have the potential to provide extremely fast system reconfiguration, enhanced protection and improved reliability, which are not possible with any serial type of communications. Typical applications being deployed include high-speed loop schemes, distributed source transfer schemes and bus differential protection. They are undoubtedly an exciting part of our power system's future.

15.12 Multiple Master Access to IEDs

As previously mentioned, the availability now of TCP protocols enables Modbus or DNP TCP devices to immediately and easily connect and communicate over existing Ethernet and fiber networks. This creates the opportunity to transfer information from/to anywhere within the Enterprise Network.

Unlike the serial versions of the legacy protocols, their TCP versions will allow multiple masters to poll the same slave device simultaneously. This is allowed because, over Ethernet using TCP/IP, multiple messages can be sent, buffered and delivered without the requirement of token passing or total bus control – which is often the case with many RS-485 and RS422 protocols.

15.13 Transfer Rate vs. Media Type

The maximum total transfer rate between Masters and IEDs will depend on the type of media and the network interface card at each end.

Several choices have been specified for unshielded twisted pair (UTP) media: Category 3, 4, 5, 5E, or optical fiber cables which can also be classified as single mode or multimode. The differences are cable cost and transmission rate capability as well as covering distance.

In order to understand standard Ethernet code, one must understand what each digit means. Following is a guide:

Table 29 Guide to Ethernet Coding

10	At the beginning means the network operates at 10Mbps.
BASE	Means the type of signaling used is baseband.
2 or 5	At the end indicates the maximum cable length in meters.
T	At the end stands for twisted-pair cable.
X	At the end stands for full duplex-capable cable.
FL	At the end stands for fiber optic cable.

For example: 100BASE-TX indicates a Fast Ethernet connection (100 Mbps) that uses a twisted pair cable capable of full-duplex transmissions.

An important part of designing and installing an Ethernet network is selecting the appropriate Ethernet medium. There are four major types of media in use today:

- Thick wire for 10BASE5 networks

- Thin coax for 10BASE2 networks
- Unshielded twisted pair (UTP) for 10BASE-T networks
- Fiber optic for 10BASE-FL

The most popular wiring schemes are 10BASE-T and 100BASE-TX, which use unshielded twisted pair (UTP) cable. Cat 5 cable is the highest, most expensive grade, offering support for transmission rates of up to 100 Mbps. Cat 4 and Cat 3 cable are less expensive, but cannot support the same data throughput speeds; Cat 4 cable can support speeds of up to 20 Mbps; Cat 3 up to 16 Mbps.

The 100BASE-T4 standard allows for support of 100 Mbps Ethernet over Cat 3 cables, but at the expense of adding another pair of wires (4 pair instead of the 2 pair used for 10BASE-T).

For specialized applications fiber-optic is the best option, but it is more expensive. Because it does not conduct electricity, fiber-optic cable can also be useful in areas where heavy electromagnetic interference is present, therefore is highly recommended in substations and industrial environment or between buildings to insulate networking equipment from electrical damage possible from ground potential rise caused by lightning.

The Ethernet standard allows for fiber-optic cable segments several kilometers long, making fiber-optic Ethernet perfect for connecting nodes and buildings that are otherwise not reachable with copper media.

Many client/server networks suffer from too many clients trying to access the same server, which creates a bottleneck where the server attaches to the LAN. Fast Ethernet, in combination with switched Ethernet, can create an optimal cost-effective solution for avoiding slow networks since most 10/100Mbps components cost about the same as 10Mbps-only devices.

When integrating 100BASE-T into a 10BASE-T network, the only change required from a wiring standpoint is that the corporate premise distributed wiring system must now include Category 5 (CAT5) rated twisted pair cable in the areas running 100BASE-T. Once rewiring is completed, gigabit speeds can also be deployed even more widely throughout the network using standard CAT5 cabling.

The Fast Ethernet specification calls for two types of transmission schemes over various wire media. The first is 100BASE-TX, which, from a cabling perspective, is very similar to 10BASE-T. It uses CAT5-rated twisted pair copper cable to connect various hubs, switches and end-nodes. It also uses an RJ45 jack just like 10BASE-T and the wiring at the connector is identical. These similarities make 100BASE-TX easier to install and therefore the most popular form of the Fast Ethernet specification.

The second variation is 100Base-FX which is used primarily to connect hubs and switches together either between wiring closets or between buildings. 100BASE-FX uses multimode fiber-optic cable to transport Fast Ethernet traffic.

Gigabit Ethernet specification calls for three types of transmission schemes over various wire media. Gigabit Ethernet was originally designed as a switched technology and used fiber for uplinks and connections between buildings. Because of this, in June 1998 the IEEE approved the Gigabit Ethernet standard over fiber: 1000BASE-LX and 1000BASE-SX.

The next Gigabit Ethernet standardization to come was 1000BASE-T, which is Gigabit Ethernet over copper. This standard allows one gigabit per second (Gbps) speeds to be transmitted over CAT5 cable and has made Gigabit Ethernet migration easier and more cost-effective than ever before.

16. High availability Ethernet protocols

One of the main advantages of Ethernet is its ability to deliver information with a minimal delay overhead. However, its main drawback is its lack of reliability: a sender does not know whether a recipient received a packet or not. To overcome the reliability issue, higher level protocols (i.e. TCP) are added, but they dramatically slow down the overall transmission delay and increase the complexity of the protocol stack. Critical power system applications, such as protection functions (e.g. busbar protection) require a short transmission delay between the sensor/actuator and protection device as well as a reliable communication protocol to ensure, for example, that a trip signal has been received by a breaker.

IEC62439 defines a set of Ethernet-based protocols providing high availability property, i.e. ensure the packet delivery even in the case of one element failing in the communication infrastructure. The purpose of this section is to give a brief introduction to the protocols defined by the IEC62439 standard as well as an overview highlighting their main differences.

16.1 Media Redundancy Protocol (MRP)

The Media Redundancy Protocol (MRP) specifies a recovery protocol based on a ring topology. It is designed to react deterministically on a single failure of an inter-link switch or switch in the network.

A MRP ring network is made of multiple nodes: one of the nodes acts as a media redundancy manager (MRM) while the other ones act as media redundancy client (MRC). A MRM observes and controls the ring topology in order to react on network faults by sending frames on one ring port and receiving them on its other ring port (and vice-versa in the other direction). The MRC nodes react on received reconfiguration frames from the MRM and can detect and signal link changes on their ring ports.

16.2 Parallel Redundancy Protocol (PRP)

The Parallel Redundancy Protocol (PRP) implements redundancy at the device level, through doubly attached nodes operating according to PRP rules. A double attached node is connected to two independent LANs of similar topology, named LAN_A and LAN_B, which operate in parallel. A source node sends the same frame over both LANs and a destination node receives it from both LANs within a certain time, consumes the first frame and discards the duplicate. The

two LANs are identical in protocol at the Media Access Control - Logical Link Control (MAC-LLC) level, but they can differ in performance and topology. Transmission delays may also be different, especially if one of the networks reconfigures itself, e.g. using RSTP, to overcome an internal failure. The two LANs follow configuration rules that allow the network management protocols such as Address Resolution Protocol (ARP) to operate correctly. The two LANs have no connection between them and are assumed to be fail-independent.

16.3 High-availability Seamless Redundancy (HSR)

The High-availability Seamless Redundancy protocol retains the PRP property of zero recovery time in case of a network element failure applicable to any topology, in particular rings and rings of rings. As in PRP, a node has two ports operated in parallel; it is a Doubly Attached Node with HSR protocol (DANH). A simple HSR network consists of doubly attached switching nodes, each having two ring ports, interconnected by full-duplex links. A sender node sends simultaneously the same packet in both directions on the ring, while the recipient accepts the first packet and rejects the second. In case of a multicast traffic, the packets are eliminated by the originator ensuring therefore that each node on the ring received the message (refer to Figure 66).

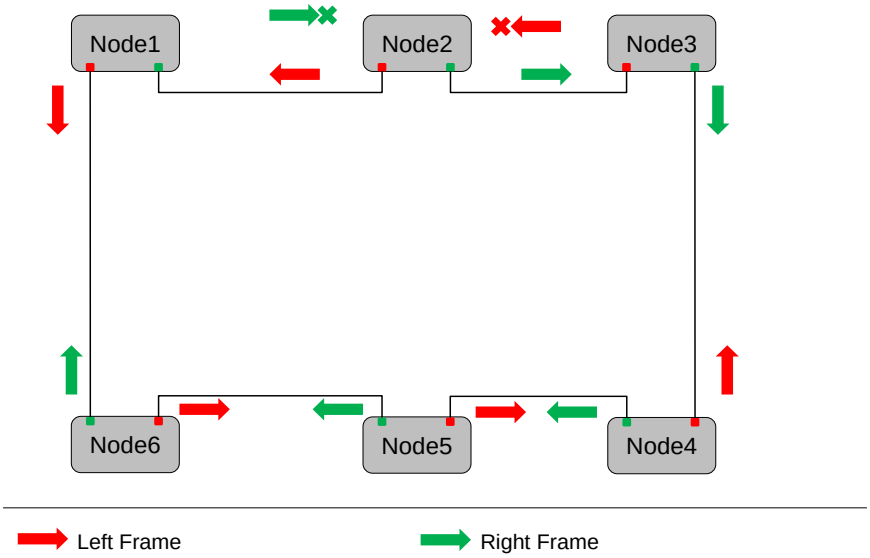


Figure 66 – HSR example for a ring multicast traffic.

16.4 Cross-network Redundancy Protocol (CRP)

The Cross-network Redundancy Protocol (CRP) specifies a redundancy protocol that is based on the duplication of the network. The redundancy protocol is executed within the end nodes, as opposed to a redundancy protocol built in the switches. There is no central “redundancy manager”; instead each node operates autonomously. The cross-network connection capability enables single attached end nodes to be connected on either of the two networks.

DiagnosticFrames are used to exercise communication paths and to assess the network health. A DiagnosticFrame contains a summary of the reporting node's view of the network health and status, including its own port. Annunciation frames are sent to announce the existence of the node. Each Doubly-attached Nodes (DANC) sends a pair of DiagnosticFrames periodically on both of its ports. Each DANC that receives one DiagnosticFrame on one port expects the other message of the pair on the other port. (On a single LAN, the node receives both messages on both ports.) If a node receives no message or if it does not receive the second DiagnosticFrame on the other port before receiving several more DiagnosticFrames on the same port, it records a fault for the corresponding node.

16.5 Beacon Redundancy Protocol (BRP)

The Beacon Redundancy Protocol (BRP) network topology can be described as two interconnected top switches, each heading an underlying topology of star, line, or ring. Beacon end nodes are connected to the top switches. The BRP stack contains two identical ISO/IEC 8802-3 (IEEE 802.3) ports connected to the network. These ports interface with the MAC sub-layer compliant with ISO/IEC 8802-3 (IEEE 802.3). Though there are two physical ports, a BRP end node uses only a single MAC address. The link redundancy entity continuously monitors the status of leaf links between both ports and corresponding ports on the switches. When a failure of the leaf link between the end node active port and the corresponding port on the switch is detected, the link redundancy entity shall reconfigure end node ports, provided the inactive port was not in the fault mode as well. After reconfiguration, all traffic flows through the newly activated port. Some messages may be lost during the failure detection and reconfiguration process, and their recovery is supported by upper layer protocols which also deal with messages lost due to other network errors.

16.6 Distributed Redundant Protocol (DRP)

The Distributed Redundant Protocol (DRP) provides a framework for describing the operational behavior of the switches in a ring topology to detect a single network failure (such as an inter-switch link failure or a ring switch failure) and recover from it within a deterministic recovery time. A DRP network has a ring topology with multiple switch nodes, each of which may be a switch or a switching end node. Each node requires an integrated switch with at least two ports (ring ports) connected to the ring, and which is able to detect and recover from failures in accordance with the DRP protocol. Each node has equal management role in a DRP ring network. It means that each node observes and controls the ring topology by multicasting a ring test frame RingCheck and an inter-switch link test frame LinkCheck cyclically, and reacts on network faults. The LinkCheck test frame provides the mechanism to detect the failure of a switch node.

16.7 Summary

The following table summarizes the reliability properties of the different protocols presented in the IEC62439 standard. The information presented in the following table is taken from the Table 2 page 1024 of IEC 62439.

Table 30 - Reliability properties overview of the protocols defined by IEC62439.

Protocol	Frame Loss	Network topology	Recovery time for the considered failure
MRP	Yes	Ring	500 ms, 200 ms, 30 ms or 10 ms worst case for 50 switches depending on the parameter set
PRP	No	Doubly meshed, independent	0s
HSR	No	Ring, meshed	0s
CRP	Yes	Doubly meshed, cross connected	1 s worst case for 512 end nodes
BRP	Yes	Doubly meshed, connected	4,8 ms worst case for 500 end nodes
DRP	Yes	Ring, double ring	100 ms worst case for 50 switches

17. Utility Oriented Protocols

17.1 Proprietary protocols

In the early development of microprocessor relays, the communications port was included principally for the purpose of connecting a computer in order to program and set the relay. The electrical interfaces were serial communications ports as used on personal computers (RS-232). Each manufacturer developed its own interface program or command set to be used with terminal emulator programs. It was also recognized that event analysis and fault locating would be aided by reviewing data stored in the microprocessor relays. Each manufacturer typically developed its own proprietary protocol for efficiently transmitting data to and from the relay in a binary format. The proprietary protocols allowed for faster data transmission and low processor overhead, both of which were important for the low baud rates and limited processing power available at the time. Subsequently, it was recognized that direct communications between protective relays could be used to create advanced protection schemes by performing logic on data and measurements taken simultaneously from multiple sources.

This need also required speed and efficiency of communications and the requirements were first met with manufacturer-specific proprietary means. For example, the communications of line current data between the line differential relays at the terminals of a transmission line may be communicated between the two relays over a direct fiber optic link. The precise format of the data transmission between the two devices is likely to be unknown except to the manufacturer of the relays and isn't of particular concern to the user. But this approach typically requires a dedicated communications link and requires that the relays are of the same make and model. The desire for interoperability between devices from multiple suppliers such as various relay manufacturers, SCADA system manufactures, and communications equipment manufacturers and the advantages of interoperability witnessed in the computer industry has led to standardization efforts.

17.2 Modbus Protocol

17.2.1 Introduction

In 1979, Modicon published the Modbus communication interface for a multi-drop network based on a master/client architecture. Modbus is managed by the Modbus-IDA User Organization. It is an open Master/Slave application protocol that can be used on several different physical Layers. Modbus is an application-layer messaging protocol, positioned at level 7 of the OSI model. It provides client/server communication between devices connected on different types of buses or networks.

The physical layer of the interface was free to choose but it was originally used on wired serial communication lines. It was an open standard that covered communication between the nodes of the network by means of messages. The form of the message was described in the standard. Later extensions to the standard were made to suit wireless communication and TCP/IP networks.

[11] Modbus was mostly used with programmable logic controllers (PLCs). It has become a de facto standard communications protocol in industry, and is now the most commonly available means of connecting industrial electronic devices. The main reasons for the extensive use of Modbus over other communications protocols are:

- it is openly published and royalty-free
- it can be implemented in days, not months
- it moves raw bits or words without placing many restrictions on vendors

Modbus allows for communication between many devices connected to the same network, for example a system that measures temperature and humidity and communicates the results to a computer. Modbus is often used to connect a supervisory computer with a remote terminal unit (RTU) or a Programmable Logic Controller (PLC) in supervisory control and data acquisition (SCADA) systems. Versions of the Modbus protocol exist for serial port and Ethernet.

For serial connections, two variants exist, with different representations of numerical data and slightly different protocol details. Modbus RTU is a compact, binary representation of the data. Modbus ASCII is human readable, and more verbose. Both of these variants use serial communication. The RTU format follows the commands/data with a cyclic redundancy check checksum, while the ASCII format uses a longitudinal redundancy check checksum. Nodes configured for the RTU variant will not communicate with nodes set for ASCII, and the reverse.

For connections over TCP/IP (e.g. Ethernet), the more recent variant Modbus/TCP exists. It is easier to implement than Modbus/ASCII or Modbus/RTU because it does not require a checksum calculation.

Data model and function calls are identical for all three communication protocols; only the encapsulation is different.

An extended version, Modbus Plus (Modbus+ or MB+), also exists, but remains proprietary to Modicon. It requires a dedicated co-processor to handle fast High-Level Data Link Control

(HDLC)-like token rotation. It uses twisted pair at 1 Mbit/s and includes transformer isolation at each node, which makes it transition/edge triggered instead of voltage/level triggered. Special interfaces are required to connect Modbus Plus to a computer, typically a card made for the ISA, PCI or PCMCIA bus.

Each device intended to communicate using Modbus is given a unique address. Any device can send out a Modbus command, although usually only one master device does so. A Modbus command contains the Modbus address of the device it is intended for. Only the intended device will act on the command, even though other devices might receive it. All Modbus commands contain checking information, ensuring that a command arrives undamaged. The basic Modbus commands can instruct an RTU to change a value in one of its registers, as well as commanding the device to send back one or more values contained in its registers.

There are many modems that support Modbus. Some of them were specifically designed for this protocol. Different implementations use wires, wireless communication and even SMS or GPRS. Typical problems the designers have to overcome include high latency and timing problems.

17.2.2 Message structure

Four basic elements are present in each message, in the same sequence as indicated in Table 31.

Table 31 Modbus Message Structure

Field	Description
Device address	Address of the receiver
Function code	Defines message type
Data	Information
Error check	Check value to test for communication errors

A “conversation” is started by a master sending a message addressed to one or more slaves. The slave defined by the message address will respond while all others ignore the message.

Serial modbus connections use either ASCII or RTU transmission modes in their coding of messages. RTU transmission mode uses binary coding which reduces the size of the message and/or leaves more room for data. All nodes in a network must use the same transmission mode.

Messages are framed to allow receivers to recognize the start and finish of a message. ASCII coding uses the colon: to indicate the start and CR/LF to indicate the finish. RTU uses time gaps of silence on the communication line for this purpose. A message must be preceded by a time a gap of at least 3.5 characters. ASCII coding allows time gaps (up to a second) between bytes of a message whereas RTU requires messages to be sent as a continuous stream with no more than a 1.5 character gap between bytes. If a receiver detects a gap in excess of 1.5 characters it assumes a new message is coming and clears the receive buffer.

(Comment – how do we know which byte is for which part of the message? Are there a fixed number of bytes for each?)

17.2.3 Addressing

The first information in a message is the address of the receiver (the device to which the message is being sent). In a Modbus device the holding registers, inputs and outputs are each assigned a number between 1 and 10000. Unfortunately Modbus message addresses use 0 to 9999 so that if you want to read the value in output register (called a coil!) 18 you have to specify the value 17 in the Modbus query message. This is a common source of error and has to be watched when designing an application. Table 32 shows the address ranges for coils, inputs and holding registers and the way the address in the Modbus message is calculated from the address of the item in the Modbus device.

Table 32 Modbus Address Ranges

Device address	Modbus address	Description
1…….10000	address -1	coils (outputs)
10001….20000	address - 10001	Inputs
40001….50000	Address - 40001	holding registers

(The maximum value used in the device address is device dependent)

17.2.4 Function codes

Table 33 Modbus Typical Function Codes

Code	**Description**
01	Read coil status
02	Read input status
03	Read holding registers
04	Read input registers
05	Force single coil
06	Preset single register
07	Read exception status
15	Force multiple coils
16	Preset multiple registers
17	Report slave ID

This is the second parameter in the Modbus message. It defines the message type and the action required by the slave. It contains one byte of information. Valid function codes are in the range 1….255 and unfortunately not all Modbus devices recognize the same set of function codes. Table 33 shows typical Modbus function codes.

17.2.5 Limitations

Modbus was designed in the late 1970's to communicate to programmable logic controllers (PLCs). The following limitations have been identified:

- The number of data types is limited to those understood by PLCs at the time.
- Large binary objects are not supported.
- No standard way exists for a node to find the description of a data object, for example, to determine if a register value represents a temperature between 30 and 175 degrees.
- Since Modbus is a master/slave protocol, there is no way for a field device to "report by exception" - the master node must routinely poll each field device, and look for changes in the data.
- This consumes bandwidth and network time in applications where bandwidth may be expensive, such as over a low-bit-rate radio link.
- Modbus is restricted to addressing 254 devices on one data link, which limits the number of field devices that may be connected to a master station.
- Modbus transmissions must be contiguous which limits the types of remote communications devices to those that can buffer data to avoid gaps in the transmission.
- Only one Master can retrieve information from the Slaves, one slave at a time.

17.2.6 Modbus messaging on TCP/IP

Modbus can be used on communication media such as an Ethernet TCP/IP network where it shares the medium with other information.

The general modbus frame described above is replaced by a slightly different message structure. The device address is replaced by an Modbus Application Protocol (MBAP) Header and the error check takes place in Ethernet rather than the modbus message. The MBAP header carries length information to allow the recipient to recognize message boundaries even if the message has been split into multiple packets for transmission.

Modbus-TCP means that the Modbus protocol is used on top of Ethernet-TCP/IP. Modbus-TCP is an open Industrial Ethernet network which has been specified by the Modbus-IDA User Organization in co-operation with the Internet Engineering Task Force (IETF) as an RFC Internet standard. Modbus devices are certified by the Modbus-IDA User Organization for interoperability and conformance to the Modbus specification.

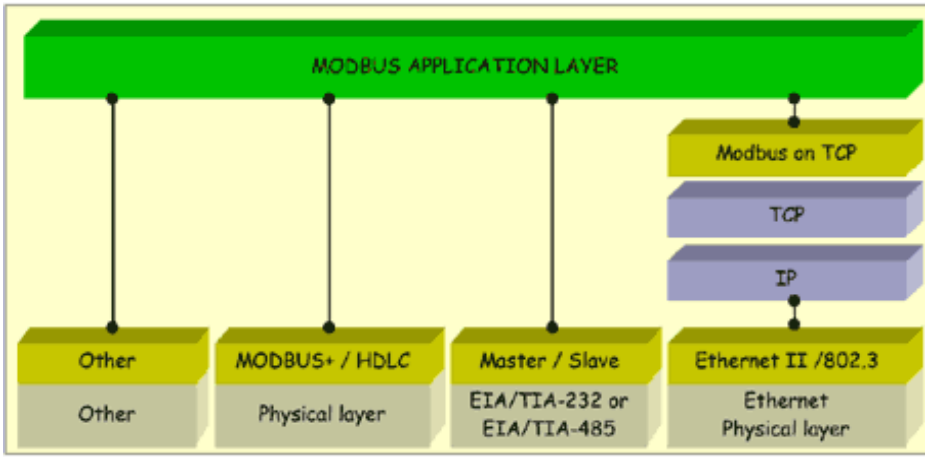


Figure 67 – OSI Model for Modbus TCP

Modbus-TCP isn't really anything new, it was solely necessary to approve Ethernet-TCP/IP as an additional data transmission technology for the Modbus Protocol. The well-proven Modbus services and the object model which has been available since the original Modbus protocol version are unchanged, and have simply been adapted to TCP/IP as the data transmission protocol. This extends the Modbus family with an additional product range, which now consists of the classical Modbus-RTU (asynchronous data transmission via RS-232 or RS-485), Modbus-Plus (high speed communication via a Token Passing Network) and Modbus-TCP (Ethernet-TCP/IP-based client/server communication). All of these versions share the same application protocol, which specifies a universal object module for user data and communication services.

Modbus is a request/reply protocol and offers services specified by function codes. Modbus function codes are elements of Modbus request/reply Protocol Data Units (PDUs). Modbus provides a set of functions to read and write data in the field devices. Modbus supports bit or word data transfers.

The performance of a Modbus-TCP network is highly dependent on the type and design of the Ethernet network which is used and on the performance of the processors in the communication interfaces of the respective devices.

Modbus-TCP is a pragmatic approach to using Ethernet as a data transmission medium for automation applications. The additional costs of the network infrastructure (star topology with intelligent switches) can be justified by the advantages of Ethernet such as the large number of stations in a network and by substantial benefits due to additional IT functions embedded (Internet, email and file transfer) which can use the same medium.

Table 34 Modbus TCP Facts

Network Type:	**Ethernet-TCP/IP based simple Client/Server network**
Topology	Very flexible with star, tree or line structures. All topologies that can be implemented with standard Ethernet technology including switched networks are applicable.
Installation	Standard 10, 100 or 1000 Mbit/s Ethernet technology based on copper cables, fiber optics or wireless standards can be used.
Speed	10, 100, 1000 Mbit/s/s
Max. Stations	nearly unlimited
Data	Up to 1.500 Bytes per Telegram frame Total: nearly unlimited
Network Features	Simple Client/Server network based on standard Ethernet technology and TCP/UDP/IP protocols in Layer 3-4.
User Organization	Modbus-IDA User Group

17.3 Distributed Network Protocol (DNP) 3

[12] Distributed Network Protocol (DNP) 3 is a set of communications protocols used between components in process automation systems. Its main use is in utilities such as electric and water companies. Usage in other industries is not common, although technically possible. Specifically, it was developed to facilitate communications between various types of data acquisition and control equipment.

DNP3 plays a crucial role in SCADA systems, where it is used by SCADA master stations at control centers, Remote Terminal Units (RTUs), and Intelligent Electronic Devices (IEDs). It is used only for communications between a master station and RTUs or IEDs.

17.3.1 History

While IEC 60870-5 was still under development and had not been standardized, there was a need to create a standard that would allow interoperability between various vendors' SCADA components for the electrical power grid. Thus, in 1993, GE-Harris Canada (formerly known as Westronic, Inc.) used the partially completed IEC 60870-5 protocol specifications as the basis for an open and immediately implementable protocol that specifically catered to North American requirements. The protocol is designed to allow reliable communications in the adverse environments that electric utility automation systems are subjected to, being specifically designed to overcome distortion induced by EMI, aging components (their expected lifetimes may stretch into decades), and poor transmission mediums.

Although the protocol was designed to be reliable, it was not designed to be secure from attacks by hackers and other malevolent forces that could potentially wish to disrupt control systems to disable critical infrastructure. Thus, much work is currently being done to provide security for the systems that use the DNP3 protocol.

The DNP3.0 protocol is also referenced in IEEE Std. 1379-2000 published in 1998, which recommends a set of best practices for implementing modern SCADA systems for communications between substation computers, RTUs (Remote Terminal Unit), IEDs and master stations; over serial or LAN-based systems.

In standard networking terms, it is a layer 2 protocol. It provides multiplexing, data fragmentation, error checking, link control, prioritization, and layer 2 addressing services for user data.

DNP3 was developed to achieve interoperability among systems in the electric utility, oil & gas, water/waste water and security industries. Many modern applications can now carry DNP3 messages over TCP/IP.

It makes particularly heavy use of Cyclic Redundancy Checks (CRCs) embedded in its data packets, in an attempt to deal with the very noisy environments in which it is typically used.

17.4 IEC 60870-5

[13] IEC 60870-5 provides a communication profile for sending basic telecontrol messages between two systems, which uses permanent directly connected data circuits between the systems. The IEC Technical Committee 57 (Working Group 03) has developed a protocol standard for Telecontrol, Teleprotection, and associated telecommunications for electric power systems. The result of this work is IEC 60870-5.

Five documents specify the base IEC 60870-5:

- IEC 60870-5-1 Transmission Frame Formats
- IEC 60870-5-2 Data Link Transmission Services
- IEC 60870-5-3 General Structure of Application Data
- IEC 60870-5-4 Definition and Coding of Information Elements
- IEC 60870-5-5 Basic Application Functions
- The IEC Technical Committee 57 has also generated companion standards:
- IEC 60870-5-101 Transmission Protocols, companion standards especially for basic telecontrol tasks
- IEC 60870-5-102 Companion standard for the transmission of integrated totals in electric power systems
- IEC 60870-5-103 Transmission protocols, Companion standard for the informative interface of protection equipment
- IEC 60870-5-104 Transmission Protocols, Network access for IEC 60870-5-101 using standard transport profiles

17.4.1 IEC 60870-5-101

IEC 60870-5-101 (IEC101) is an international standard prepared by TC57 for power system monitoring, control & associated communications for telecontrol, teleprotection, and associated telecommunications for electric power systems. This is completely compatible with IEC 60870-5-1 to IEC 60870-5-5 standards and it uses standard asynchronous serial telecontrol channel interface between data terminal equipment (DTE) and data circuit-terminating equipment (DCE). The standard is suitable for multiple configurations like point-to-point, star, multidropped, etc.

17.4.1.1 Frame Format

Character format of IEC 101 uses 1 start bit, 1 stop bit, 1 parity bit & 8 data bits. FT1.2 (defined in IEC 60870-5-1) is used for frame format of IEC 101 which is suitable for asynchronous communication with hamming distance of 4. This uses 3 types of frame formats - Frame with variable length, Frame with fixed length and single character. Single character is used for acknowledgments, fixed length frames are used for commands and variable lengths are used for sending data. The details of variable length frame are given below in Table 35.

17.4.1.2 Features

- Supports unbalanced (only master initiated message) and balanced (can be master/slave initiated) modes of data transfer.
- Link address and ASDU (Application-layer Service Data Units) addresses are provided for classifying the end station and its different segments.
- Data is classified into different information objects and each information object is provided with a specific address.
- Facility to classifying data into high priority (class-1) and low priority (class-2) and transferring data using separate mechanisms.
- Possibility of classifying the data into different groups (1-16) to get the data according to the group by issuing specific group interrogation commands from the master and obtaining data under all the groups by issuing a general interrogation.
- Cyclic and Spontaneous data updating schemes are provided.
- Facility for time synchronization.
- Schemes for transfer of files.

Table 35 IEC 101 Frame Format & Variable Length

Data unit	Name	Function
Start Frame	Start Character	Indicates start of Frame
	Length Field (*2)	Total length of Frame
	Start Character (repeat)	Repeat provided for reliability
	Control Field	Indicates control functions like message direction
	Link Address (0,1 or 2)	Normally used as the device / station address
Data Unit Identifier	Type Identifier	Defines the data type which contains specific format of information objects
	Variable Structure Qualifier	Indicates whether type contains multiple information objects or not
	COT (1 or 2)	Indicates causes of data transmissions like spontaneous or cyclic
	ASDU Address (1 or 2)	Denotes separate segments and its address inside a device
Information Object	Information Object Address (1 or 2 or 3)	Provides address of the information object element
	Information Elements (n)	Contains details of the information element depending on the type
Information Object-2	-----	
-----	-----	
Information Object-m		
Stop Frame	Checksum	Used for Error checks
	Stop Char	Indicates end of a frame

17.4.2 IEC 60870-5-103

IEC 60870-5-103 [IEC103] is a standard prepared by International Electrotechnical Commission Technical committee 57 for power system control and associated communications. It defines a companion standard that enables interoperability between protection equipment and devices of a control system in a substation. The device complying with this standard can send the information using two methods for data transfer - either using the explicitly specified application service data units (ASDU) or using generic services for transmission of all the possible information. The standard supports some specific protection functions and provides the vendor a facility to incorporate its own protective functions on private data ranges.

17.4.2.1 Frame Format

IEC 103 uses FT1.2 (defined in IEC 60870-5-1) for frame format, which provides options of frames with variable length, frames with fixed length and single character frames. Single character frames are used for acknowledgments, fixed length frames are used for commands and variable length frames are used for sending data. This is similar to IEC 101, however, the frame format of IEC 103 differs from IEC 101 in information object address, which is split into function type (ftype) and information number (inumber) in IEC 103. Also IEC 103 can have only a single information object in a frame whereas IEC 101 can have multiple information objects. Many of the field sizes are also restricted in IEC 103. The details of variable length frame are given below in Table 36.

Table 36 IEC 103 Frame Format & Variable Length

Data unit	Name	Function
Start Frame	Start Character	Indicates start of Frame
	Length Field (*2)	Total length of Frame
	Start Character (repeat)	Repeat provided for reliability
	Control Field	Indicates control functions like message direction
	Link Address (0,1 or 2)	Normally used as the device / station address
Data Unit Identifier	Type Identifier	Defines the data type which contains specific format of information objects
	Variable Structure Qualifier	Indicates whether type contains multiple information objects or not
	COT (1 or 2)	Indicates causes of data transmissions like spontaneous or cyclic
	ASDU Address (1 or 2)	Denotes separate segments and its address inside a device
Information Object	Function Type	Provides function type of the protection equipment used
	Information Number	Defines the information number within a given function type
	Information Elements (n)	Contains details of the information element depending on the type
Stop Frame	Checksum	Used for Error checks
	Stop Char	Indicates end of a frame

17.4.2.2 Supported Types

- Type 1 – Time-tagged message
- Type 2 – Time-tagged message with relative time
- Type 3 – Measurands I
- Type 4 – Time-tagged measurands with relative time
- Type 5 – Identification
- Type 6 – Time synchronization
- Type 7 – Start of General interrogation
- Type 8 – General interrogation termination
- Type 9 – Measurands II
- Type 10 – Generic data
- Type 11 – Generic identification
- Type 23-31 – Used for transferring disturbance files

17.4.3 IEC 60870-5-104

With the rapid advancement of technology and up-gradation of control center, there is a growing desire to use the 60870 Standard to communicate between Telecontrol stations via Internet services. A new Companion Standard called IEC 60870-5-104 has been in use for this purpose. IEC 60870-5-104 is briefly explained below.

IEC 60870-5-104 (IEC 104) protocol is an extension of IEC 101 protocol with the changes in transport, network, link and physical layer services to suit the complete network access. The standard uses an open TCP/IP interface to network to have connectivity to the LAN (Local Area Network), and routers with a different facility (ISDN, X.25, Frame relay etc) can be used to connect to the WAN (Wide Area Network). Application layer of IEC 104 is preserved the same as that of IEC 101 with some of the data types and facilities not used. There are two separate link layers defined in the standard, which are suitable for data transfer over Ethernet and serial line (PPP - Point-to-Point Protocol).

17.4.3.1 Additional Synchronization Mechanisms

The 104 protocol, as well as the 101 protocol, has a control field used as protection mechanism against lost messages (ASDU's), flow control and watchdog function. The 3 different formats I, S, U have different functions as described below:

- I Format – It is used to perform numbered information transfer. It contains a send-sequence number and a receive-sequence number. The transmitter station increases the send-sequence number when it sends any data and the receiver increases the receive-sequence number when it receives any data. The sending station has to hold the send APDUs (Application Protocol Data Units) in the buffer until it receives back the send sequence numbers as the receive sequence number from destination station.
- S Format – It is used to perform numbered supervisory functions. In any cases where the data transfer is only in a single direction, S-format APDUs must be sent in the other

direction before timeout (t2), buffer overflow or before it has crossed maximum number of allowed I format APDUs without acknowledgement (w).

- U Format – It is used to perform unnumbered control functions. This is used for activation and confirmation mechanisms of start data transfer (STARTDT), and stop data transfer (STOPDT) and TESTFR (test APDU).

17.5 IEC 61850 Standard

17.5.1 Introduction

The success of a Substation Automation System (SAS) relies on the use of an effective communication system to link the various protection, control, and monitoring elements within a substation. The major challenge faced by substation automation design engineers is to provide interoperability among the protection, control, and monitoring devices from the various manufacturers. Up until recently, all the manufacturers are/were using their own proprietary communication protocols. Huge investment is needed to develop costly and complicated protocol converters. To address these SAS issues, IEC (International Electro-technical Commission) working group TC57 has published IEC 61850 named as "Communication Networks and Systems in Substations" in 2003. IEC started work on developing a common standard for substation communication in 1994. At the same time IEEE started a similar work on developing a common communication protocol called UCA. In 1997 both IEEE and IEC agreed to work together and develop a common standard for substation communication, IEC 61850. This standardization process involved leading product/system manufacturers and also major utilities. The primary objective of the group was to develop a communication protocol for substation communication, which will ensure the following:

Interoperability: The ability for the IEDs from one or several manufacturers to exchange information and use the information for their own functions.

Free configuration: The standard shall support different philosophies and allow free allocation of functions.

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.

17.5.2 Description of IEC 61850 standard

The standard that defines the new IEC 61850 protocol is divided into 10 parts as described below:

Part 1: This part provides an introduction and overview to the IEC 61850 standard.

Part 2: Contains the glossary of the terminology and definitions used in the context of substation automation system in the different parts of the standard.

Part 3: Gives the general requirements of the communication network with emphasis on quality requirements. It also specifies the environmental operating conditions to which the communication network devices should conform, to ensure reliable operation.

Part 4: Pertains to the system and project management with respect to engineering process and its supporting tools, life cycle of IEDs and overall system, and quality assurance.

Part 5: This part defines the performance requirement of different functions being implemented using communication. All known functions are included. This part is the basis on which the architecture of the communication network and the applications that can be implemented for a given network are to be decided.

Part 6: Specifies a file format for describing communication related IED configurations and IED parameters, communication system configurations, switchyard (function) structures, and the relations between them. The main purpose of this format is to exchange IED capability descriptions and SA system descriptions, between IED engineering tools and the system engineering tool(s) of different manufacturers in a compatible way. The defined language is called Substation Configuration description Language (SCL). The configuration language is based on the Extensible Markup Language (XML) version 1.0.

Part 7-1: The purpose of this part of the IEC 61850 standard is to provide *"from a conceptual point of view"* assistance to understand the basic modeling concepts and description methods.

Part 7-2: Applies to the Abstract Communication Service Interface (ACSI) communication in substations and feeder applications. The ACSI provides:

- Abstract interface describing communications between a client and a remote server.
- Abstract interface for fast and reliable system-wide event distribution between an application in one device and many remote applications in different devices and for transmission of sampled measured values.

Part 7-3: Specifies common attribute types and common data classes related to substation applications. This standard is applicable to the description of device models and functions of substations and feeder equipment.

Part 7-4: This part specifies the information model of devices and functions related to substation applications. In particular, it specifies the compatible logical node names and data names for communication between IEDs. This includes the relationship between Logical Nodes and Data. The names defined in this document are used to build the hierarchical object references applied for communicating with IEDs in substations and on distribution feeders. The naming conventions of IEC 61850-7-2 are applied in this part.

Part 8-1: This part specifies a method of exchanging time-critical and non-time-critical data through local-area networks by mapping ACSI to Multimedia Messaging Service (MMS) and ISO/IEC 8802-3 frames.

Part 9-1: This part of IEC 61850 specifies the mappings for the communication between bay and process level, and it specifies a mapping on a serial unidirectional multi-drop point to point link in accordance with IEC 60044-8.

Part 9-2: Defines the Specific Communication Service Mapping (SCSM) for the transmission of sampled values according to the abstract specification in IEC 61850-7-2. The mapping is that of the abstract model on a mixed stack using direct access to an ISO/IEC 8802-3 link for the transmission of the samples in combination with IEC 61850-8-1.

Part 10: Specifies the procedure for conformance testing of products implemented with this communication protocol.

17.5.3 Approach of IEC61850

To meet the basic requirements of the standardization process, that is interoperability and to be future proof, the IEC61850 standard is built over a standard OSI 7 layer model. The data services and applications related to the power system substation are built above the 7th layer (application) of the OSI model. This ensures that the substation communication can evolve with the evolution of communication technology using its strength. Figure 68 below shows this approach to the standardization process.

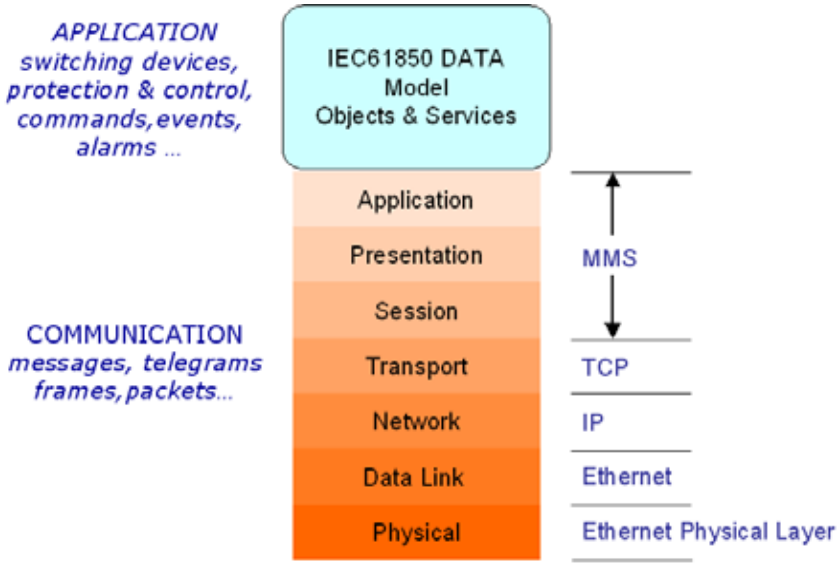


Figure 68 – IEC61850 approach to standardization

17.5.4 Organization of logical device

The data models are divided into logical groups called devices, nodes, classes and data. Each functional element is defined as a logical node. A physical device (IED) can house multiple logical nodes in it. Each logical node is a collection of standard data classes. The possible values that can be assigned to the data classes are called as data. Figure 69 pictorially represents the physical device, logical nodes, data classes and data.

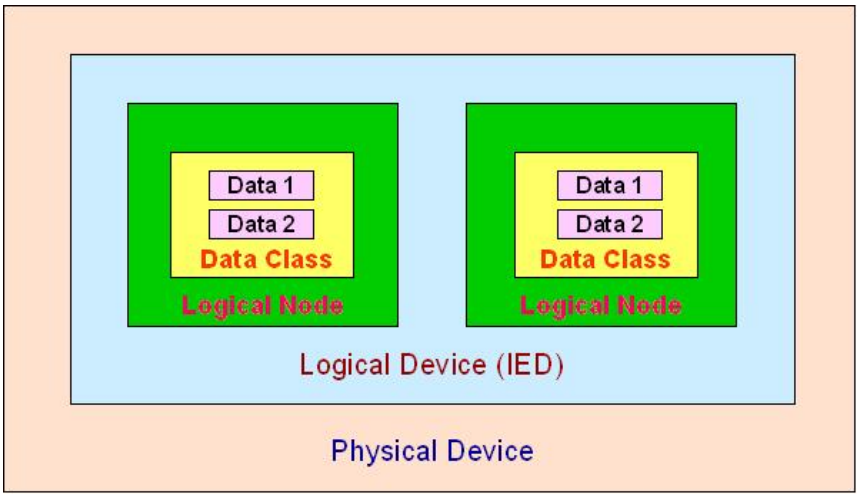


Figure 69 – Organization of Logical device, logical nodes, data classes and data

Every control or automation function (in fact any function) can be broken down to a collection of different logical nodes. These logical nodes can be housed in a single IED or distributed among multiple IEDs. All the different logical nodes of a specific application are interconnected using logical connections. These logical connections can be over a single or multiple physical connections.

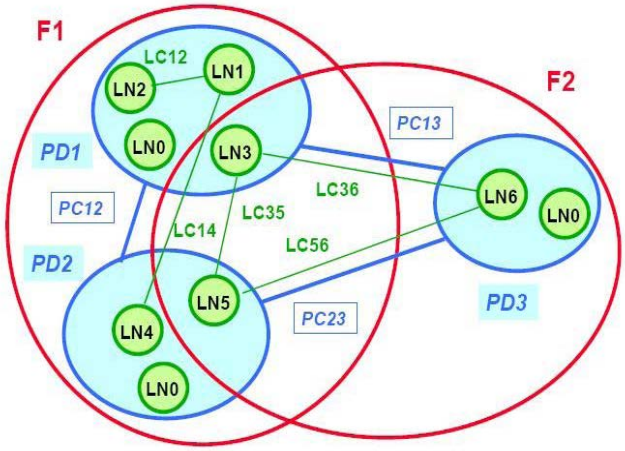


Figure 70 – Building functions from multiple logical nodes

Figure 70 illustrates how functions are realized using logical nodes and logical connections. In this example two functions, F1 and F2 are shown. Function F1 is split into 5 logical nodes (LN1 to LN5). Function F2 is split into three logical nodes LN3, LN5 and LN6. These logical nodes are housed in three different physical devices (IEDs), PD1, PD2 and PD3. The logical node LN0 is the node carrying the identification of the physical device. The logical connections between the logical nodes are marked as LC and the physical connections between the physical devices are PC.

17.5.5 OSI-7 stack for message communication

The modeling of IED shall be based on the communication stack specified in IEC 61850. According to IEC 61850-5 and IEC 61850-8, messages are classified into 7 categories based on the performance requirements.

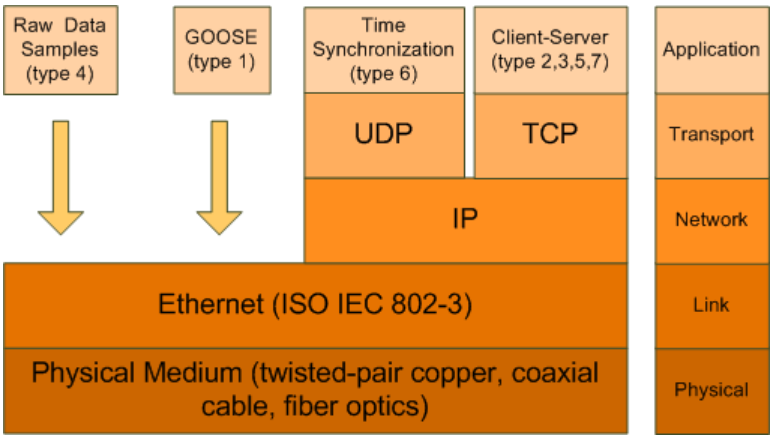


Figure 71 – Message communication OSI-7 stack

The seven types of messages are mapped into different communication stacks. As shown in Figure 71, the raw data samples (type 4) and GOOSE messages (type1, 1A) are time critical and are, therefore, directly mapped to low–level Ethernet link layer. This gives the advantage of improved performance for real time messages by shortening the Ethernet frame (no upper layer protocol overhead) and reducing the processing time. The medium speed message (type 2), the command message with access control (type 7), the low speed message (type 3) and the file transfer functions (type 5) are mapped to MMS protocol suits which has a TCP/IP stack above the Ethernet layer. The time synchronization messages (type 6) are broadcasted to all IEDs in substation using UDP/IP.

Table 37 summarizes these messages and transfer time requirements based on IEC 61850 standard.

Table 37 Message Types & Performance requirement in SAS

Sr. No.	Message Type	Application (In PICOM)	Transfer Time Limit (ms)
1	Type 1 1a – Trip 1b – Others Message	Trigger	10-100
		Complex block or release	10-100
		Fast broadcast Message	1
		Process State Changed	1-10
		Trip	1
2	Type 2 Medium Speed Message	Process value in r.m.s	50-1000
		Request for syn. check interlocking	10-100
		Process State	1-100
		Calculated State	1-100
		External Condition	1-100
3	Type 3 Low Speed Message	Measured value	100-1000
		Meter value	100-1000
		Non – electrical Process value	1000-5000
		Fault value	1000-5000
4	Type 4 Raw Data Message	Process value (Sample voltage & Current)	0.1-10
5	Type 5 File Transfer	Report e.g. Energy list	1000-5000
		Mixed fault info.	1000-5000
		Mixed fault data	5000
		Event/Alarm List	100-1000
		ID data, Setting	1000-5000
		Diagnostic data	5000
6	Type 6 Time Synchronization Message	Synchronise of pulse	0.1-10
7	Type 7 Command Message with Access Control Message	Command (From local to remote HMI)	1-1000

17.5.6 Substation Configuration Language (SCL)

It is important to configure the entire substation IEDs according to the specific substation configuration. In order to simplify this process, IEC 61850 part-6 has proposed an eXtensible Markup Language (XML) based substation configuration language (SCL). This facilitates the description of the relations between substation automation system and substation (switchyard). SCL specifies a file format for describing communication related IED configurations, IED parameters, communication system configurations, switchyard (function) structures, and the relations between them. The various SCL files include system specification description (SSD), IED capability description (ICD), substation configuration description (SCD), and configured IED description (CID) files.

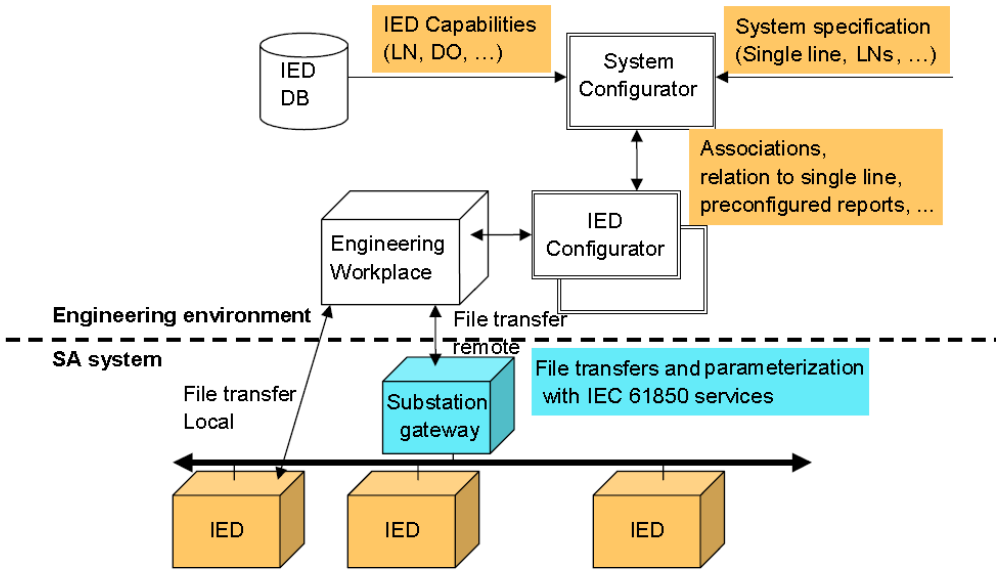


Figure 72 – Reference model for information flow in the configuration process

Figure 72 explains the usage of SCL data exchange in the engineering process. The text boxes above the dashed line (for engineering environment) indicate where SCL files are used. The IED configurator is a manufacturer-specific tool that shall be able to import or export the files defined by part-6 of IEC 61850. It provides IED-specific settings and generates IED specific configuration files, or it loads the IED configuration into the IED. The System Configurator is an IED independent system level tool that shall be able to import or export configuration files defined by part-6 of IEC 61850. It shall be able to import configuration files from several IEDs, as needed for system level engineering, and used by the configuration engineer to add system information shared by different IEDs. Then the system configurator shall generate a substation related configuration file as defined by part-6 of IEC 61850, which may be fed back to the IED configurator for system related IED configuration.

SCL can be used to restructure the entire power system design process to eliminate manual configuration, eliminate manual data entry errors, and reduce misunderstanding between system capabilities and requirements.

18. Serial to Ethernet Conversion

18.1 Introduction

Protocols such as Modbus and DNP were developed at the time when serial communications was the predominant media for SCADA. The popularity of Ethernet forced the development of Ethernet versions of the same protocols often referred to as Modbus or DNP over Ethernet. For the most part, the TCP version is simply packets encapsulated in standard TCP/IP packets. This enables Modbus or DNP TCP devices to immediately and easily connect and communicate over existing Ethernet and fiber networks.

In the case of Modbus TCP, it also allows many more addresses than RS-485, the use of multiple Masters, and speeds in the gigabit range.

While Modbus RTU has a limitation of 247 nodes per network, Modbus TCP networks can have as many slaves as the physical layer can handle. Often this number is somewhere around 1024.

Ethernet's rapid adoption within the process control and automation industry has allowed Modbus TCP to become the most widely used, fastest growing and supported industrial protocol over Ethernet.

Although PLC vendors of all sizes have adopted their own proprietary protocols over Ethernet, almost all of them support Modbus TCP. For those PLC vendors who don't currently support Modbus TCP, there are many companies like Prosoft Technologies and SST that offer chassis-style slide in Modbus TCP communication cards and stand alone gateways.

18.2 Serial to Ethernet Technologies

18.2.1 Overview

Serial servers utilize the Serial-to-Ethernet technology that allows connecting serial devices that do not have Ethernet capabilities to the local area network (LAN). The main benefits of being able to connect to the substation LAN are:

- High-speed peer-to-peer communications between IEDs
- Reduced inter-IED wiring
- Coexisting multiple protocols (e.g. DNP, Modbus, IEC61850) on the same physical network
- Enables "Data over IP" for easy access to substation data
- Serial communications normally would not provide protection for losing links.
- Using Serial over Ethernet protocols allows for ring architecture implementation utilizing protection protocols like eRSTP for more reliability should a link failure occur.
- Over all result is a protected network architecture that provides reliability and high availability with all components integrated on the same Ethernet backbone network at lower cost.
- Serial servers allow integrating serial devices that are not Ethernet capable together with Ethernet capable devices on the same network.
- A connection to the enterprise network can be made and users can have access from anywhere to monitor, control and manage different components according to needs.

The requirement to move from legacy manufacturing systems to improved systems where data can be analyzed at a central location is becoming more viable as costs and manpower decrease.

Ethernet infrastructure is usually in existence, or can be easily implemented. Buildings tend to have existing Ethernet networks. PLC and RTU manufacturers are starting to develop Ethernet add-ons to network their products, at a premium cost for this functionality.

The most cost-effective solution is to use serial device servers to convert serial data to Ethernet data. The cost of laying serial cables over long distances can prove to be expensive. Even legacy

software applications can be fooled into thinking it is using a serial port on the remote control PC by using a Virtual COM Port Redirection.

With Virtual COM Port Redirection, a transparent serial tunnel is created over Ethernet. This all happens without changing much of the existing setup. The ability to create Virtual COM Ports eliminates the need to upgrade PLCs or RTUs with network add-on modules.

18.2.2 What is Ethernet Encapsulation?

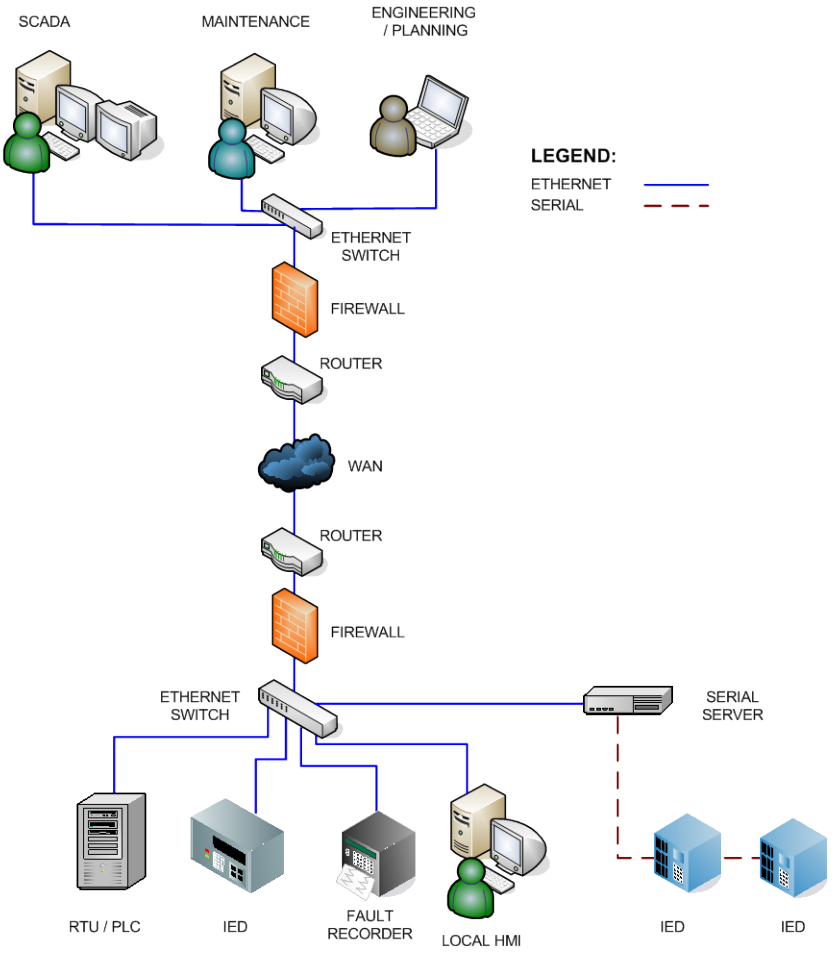


Figure 73 – Serial Server in a SCADA Application

Ethernet Encapsulation provides a virtual serial port on the workstation or SCADA Server. Use existing serial drivers in the OPC server to communicate to networked PLCs as if they were connected directly to the workstation or SCADA Server.

With the Serial Server, serial devices can now be connected to an Ethernet network, with it collecting data to a SCADA Server without running extra Virtual COM Port Redirector applications. Figure 73 shows one possible concept of an application of a Serial Server for SCADA involving both Ethernet ready IEDs as well as legacy IEDs with serial communications.

There are “many ways to skin a cat” which is true when it comes to migrating from Serial to Ethernet. There are three ways to achieve Serial to Ethernet Conversion:

- RaW Socket TCP / IP
- Protocol Conversion via Serial Servers
- The Gateway approach

18.3 RaW Socket TCP/IP

The basic idea behind Raw Socket is extending a serial network behind serial communications limitations by encapsulating serial data in IP datagrams that can travel over a standard IP network that spans across cities, countries, and sometimes continents.

Socket mode of operation provides a way of directly accessing device servers across a TCP/IP network without first having to install a driver. Sockets are standard APIs (Application Programming Interfaces) used to access network devices over a TCP/IP network. Two socket API standards are in common use. The original standard, known simply as 'Sockets', was developed for the Unix/Linux environment. The Windows alternative is 'Win Sock'. Although there are fundamental differences between these two standards, most of the API function calls from either system have the same structure and consequently, socket based network control programs are portable across almost all system platforms.

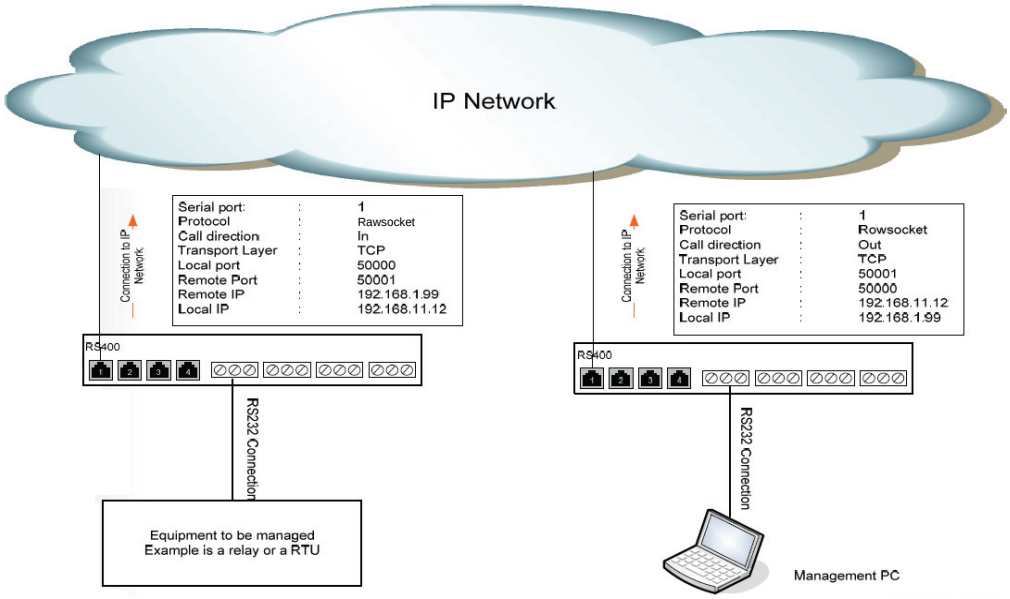


Figure 74 – RaW Socket Operation

Two appropriately configured device servers can work in unison to form a serial tunnel. The serial tunnel operates by encapsulating serial data in a TCP/IP packet, which is then transported across

an Ethernet network. This operation mode allows transparent connection of all serial devices and is also a good way to network DOS based PCs or PDAs. Because the connection is truly transparent, proprietary Siemens or Allen-Bradley, etc, PLC protocols can be transmitted.

Figure 75 shows the OSI Model applied to RaW Socket serial to Ethernet mode of operation.

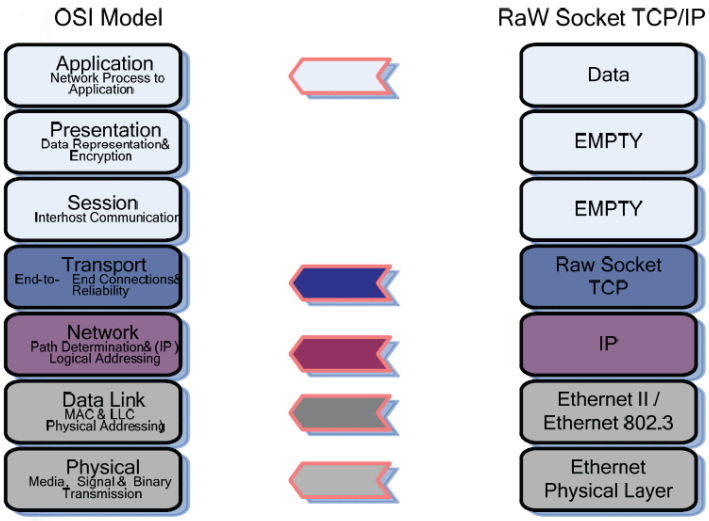


Figure 75 – OSI Model of RaW Socket TCP/IP

Raw Socket encapsulation will allow encapsulating serial traffic into IP packets. During the encapsulation process a decision will need to be made about when to packetize serial information.

The following options are available on state of the art serial server devices for Raw Socket encapsulation:

Packetize on receiving a Specific character: The server will examine each received character and will packetize and forward upon receiving the specific character. The character is usually a <CR> or an <LF> character but may be any 8 bit (0 to 255) character.

Packetize on timeout: The server will wait for a configurable time after receiving a character before packetizing and forwarding. If another character arrives during the waiting interval, the timer is restated. This method allows characters transmitted as a part of an entire message to be forwarded to the network in a single packet, when the timer expires after receiving the very last character of the message.

Packetize on full packet: The server will always packetize and forward on a full packet, i.e. when the number of characters fills its communications buffer (1K bytes).

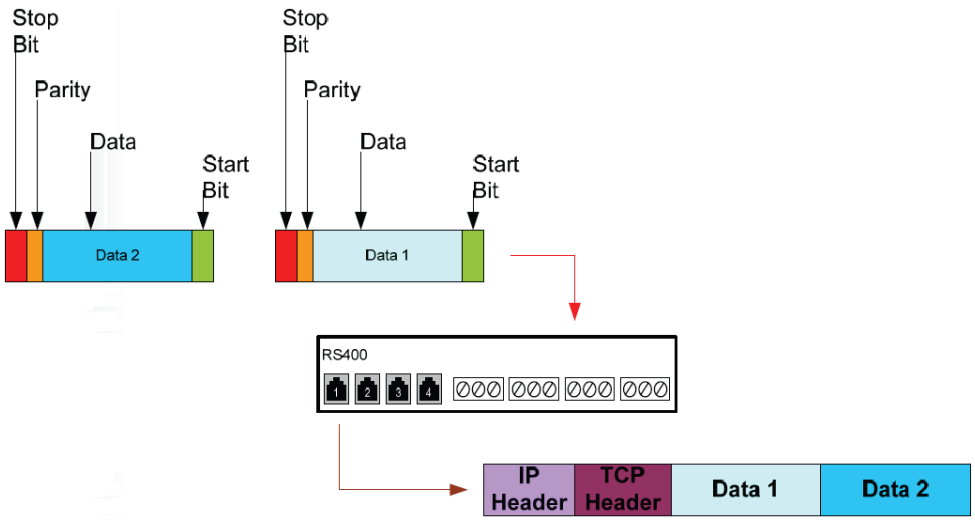


Figure 76 – RaW Socket Packatization

18.4 Serial Server – Serial to TCP Protocol Converter

As an example to illustrate how Serial Servers help bridge serial protocols to TCP/IP level, we will use MODBUS Protocol. Similarly, other protocols such as DNP 3.0 can also be handled by Serial Servers allowing MODBUS RTU serial devices to be seamlessly connected to Ethernet networks.

Figure 77 shows how serial devices can communicate over the same bus and at the same time utilize a gateway to convert Modbus-Serial to Modbus-TCP to communicate with other MODBUS-TCP/IP native devices and other Modbus-Serial devices behind another gateway.

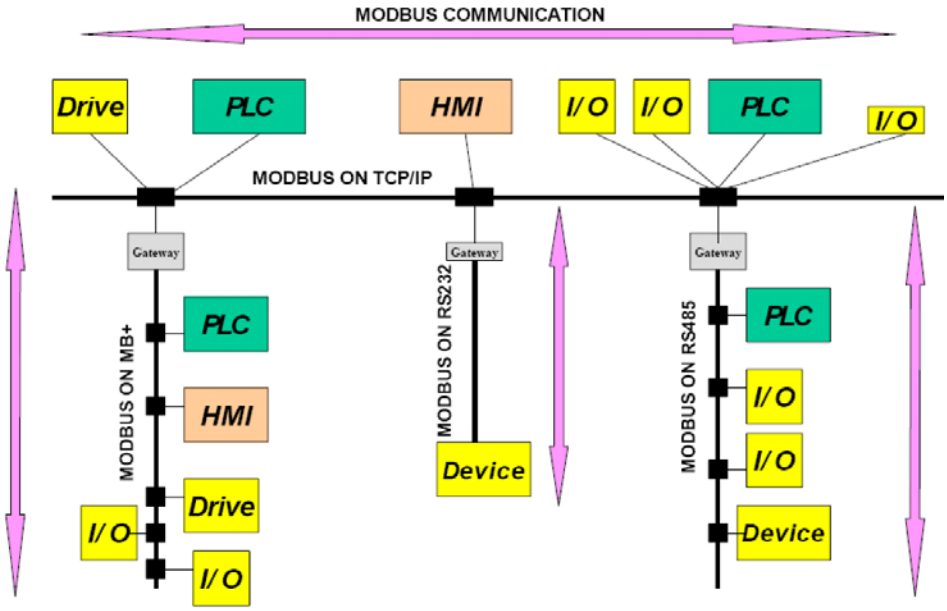


Figure 77 – Modbus Operation

Serial servers will serve as gateways to convert Modbus-Serial to TCPModbus facilitating the communication between serial devices over IP networks.

Some RTUs and PLCs have native Ethernet ports and directly support TCPModbus without the need for serial servers.

On MODBUS Serial Line, the Address field only contains the slave address.

As shown in Figure 78, the Modbus frame over serial can be described as follows:

- The valid slave nodes addresses are in the range of 0 – 246 decimal. The individual slave devices are assigned addresses in the range of 1 – 247. A master addresses a slave by placing the slave address in the address field of the message.
- When the slave returns its response, it places its own address in the response address field to let the master know which slave is responding.
- Modbus master node has no address assigned.
- The function code indicates to the server what kind of action to perform.
- The function code can be followed by a data field that contains request and response parameters.
- Error checking field is the result of a "Redundancy Checking" calculation that is performed on the message contents.

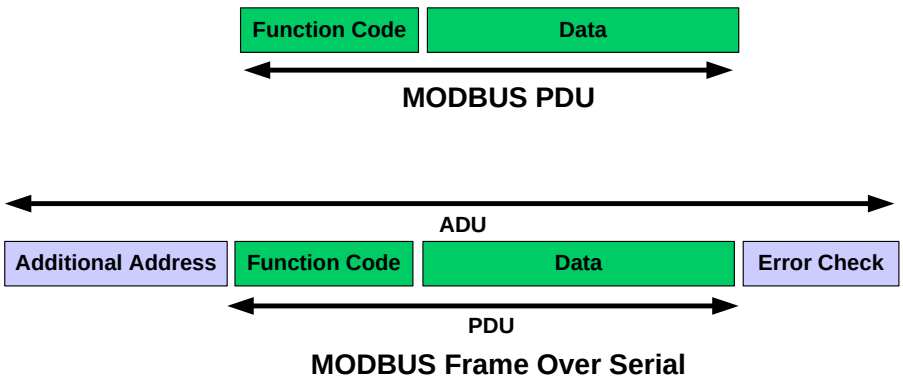


Figure 78 – Modbus Serial - Link Layer

Things to note with regards to the Modbus Protocol are:

- The Modbus Serial Line protocol is a Master-Slaves protocol.
- Only one master (at the same time) is connected to the bus.
- Up to 247 slave nodes can be connected to the same serial bus.
- Modbus communication is always initiated by the master.
- Slave nodes will never transmit data without receiving a request from the master node.
- Slave nodes will never communicate with each other.
- The master node initiates only one Modbus transaction at a time.

The difference between Modbus serial and Modbus TCP/IP OSI Model can be noticed in Figure 79.

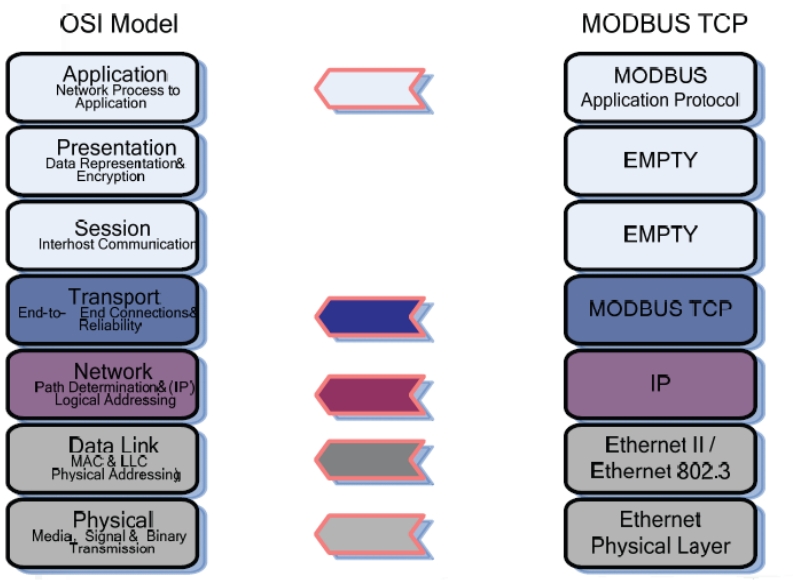


Figure 79 – OSI Model of Modbus TCP/IP

The MODBUS protocol defines a simple Protocol Data Unit (PDU) independent of the underlying communication layers. The mapping of MODBUS protocol on specific buses or networks can introduce some additional fields on the Application Data Unit (ADU).

A dedicated header is used with TCP/IP to identify the MODBUS Application Data Unit. It is called the MBAP header (MODBUS Application Protocol header).

The ‘MODBUS slaves address’ field usually used on MODBUS Serial Lines is replaced by a single byte ‘Unit Identifier’ within the MBAP Header. The ‘Unit Identifier’ is used to communicate via devices such as bridges, routers and gateways that use a single IP address to support multiple independent MODBUS end units.

All MODBUS requests and responses are designed in such a way that the recipient can verify that a message is finished. For function codes where the MODBUS PDU has a fixed length, the function code alone is sufficient. For function codes carrying a variable amount of data in the request or response, the data field includes a byte count.

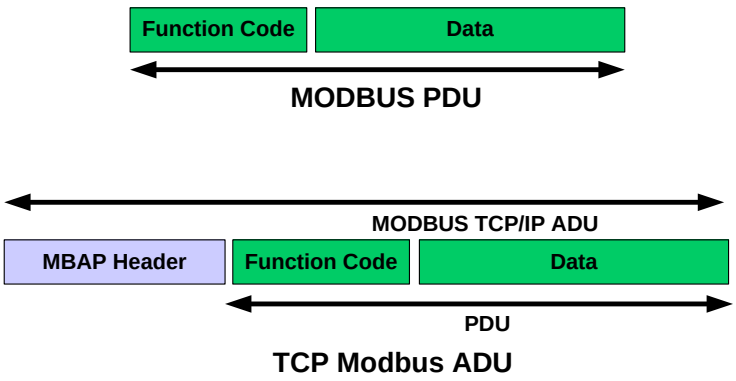


Figure 80 – TCP Modbus Application Data Unit (ADU)

When MODBUS is carried over TCP, additional length information is carried in the MBAP header to allow the recipient to recognize message boundaries even if the message has been split into multiple packets for transmission. The existence of explicit and implicit length rules and use of a CRC-32 error check code (on Ethernet) result in an infinitesimal chance of undetected corruption to a request or response message.

Modbus Client/Server Operation is done in accordance to the following sequence:

- The Modbus Client application accepts Modbus polls from a master and determines the IP address of the corresponding RTU utilizing the device address table.
- The client then encapsulates the message in TCP using TCPModbus protocol, and forwards the frame to a Server Gateway or a native TCPModbus RTU.
- The Modbus Server application accepts TCP encapsulated TCPModbus messages from Client Gateways and native masters.
- After removing the TCP headers the messages are issued to the respective RTU according to the local device address table.
- Responses are TCP encapsulated and returned to the originator.
- Returning responses are stripped of their TCP headers and issued to the master.

A graphic representation of what was described above can be found in Figure 81.

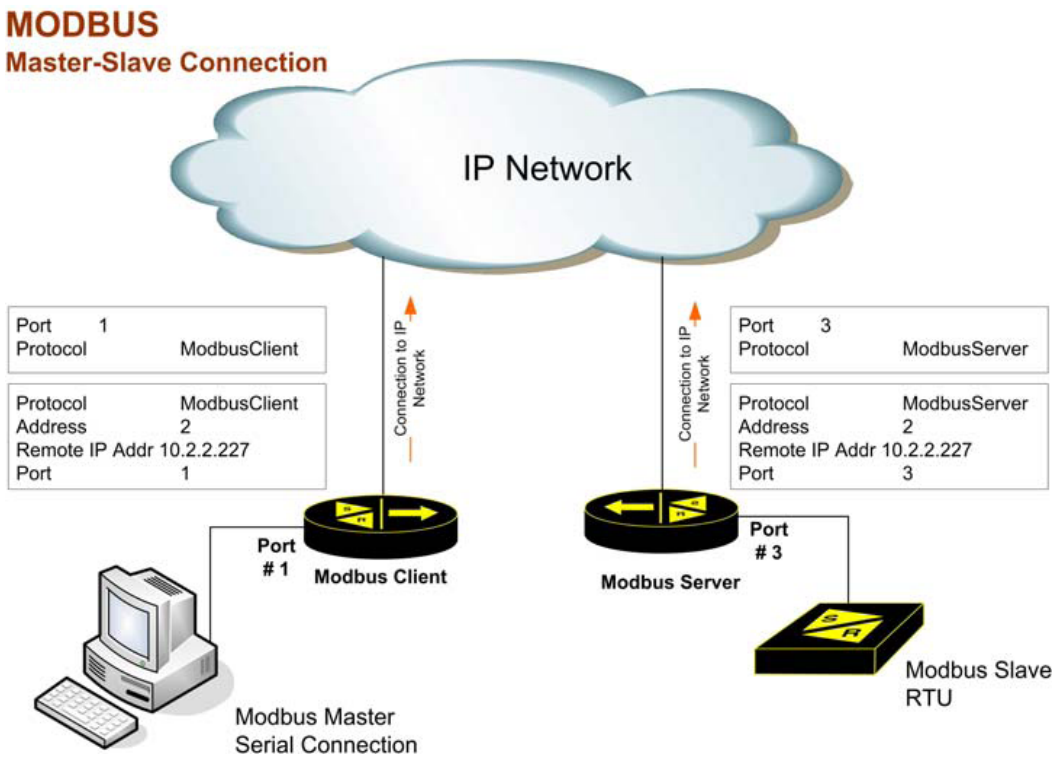


Figure 81 – MODBUS Master-Slave Connection

18.5 Gateway Approach

Another approach to facilitate the migration of serial devices to Ethernet LANs is the use of Gateways, which are more complex than Serial Servers, and also popular in Automation Projects involving legacy devices.

Substation automation projects pose a number of challenges:

- Protocol conversion
- Communication between devices and system components
- Support for legacy devices and control centers
- Equipment monitoring and control (I/O)

A typical automation system consists of a SCADA system, located in a control center, which connects to devices such as RTUs, and local computers located in the substation site. The SCADA regularly polls the devices in order to retrieve device readings, statuses, and sequence of event reports. The operator also uses the SCADA system to perform control functions on selected devices.

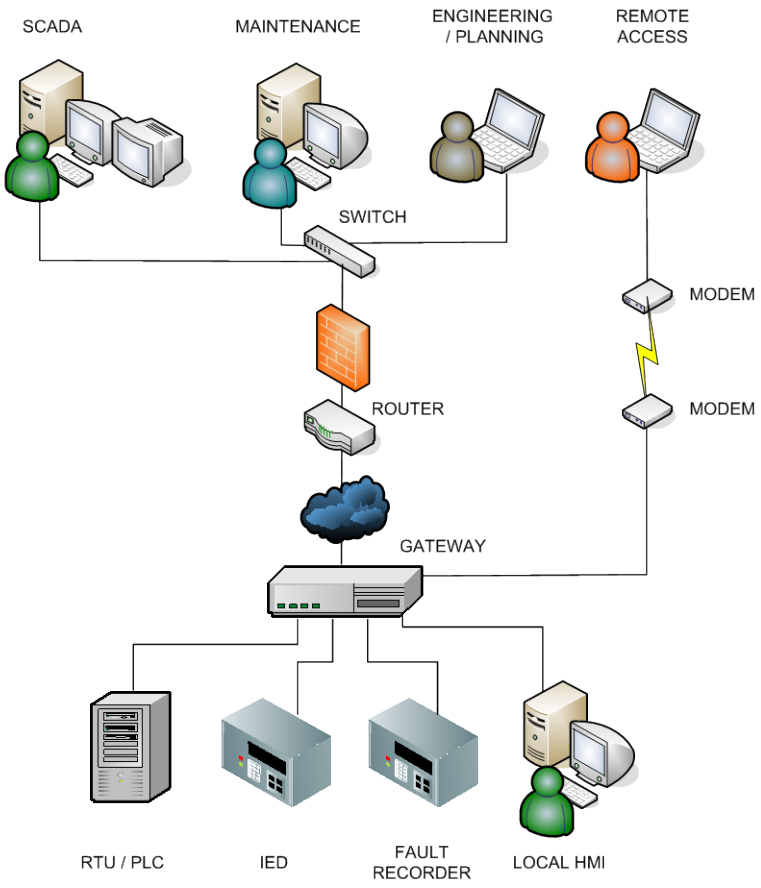


Figure 82 – Gateway in a SCADA Application

Gateways streamline automation by providing a more complete and efficient solution. Gateways have the capability of processing data locally, making it easy to add new devices without affecting control centers.

Some of the most important features of Gateways are:

- Integration of legacy and new SCADAs, PLCs, RTUs, IEDs
- Reduce overall network bandwidth
- Local and remote clients have access to all substation data using various applications
- Data concentration - collect data from all connected devices, regardless of protocol, and make it available to control centers using LAN, WAN or serial connections
- Protocol Conversion – standard or proprietary device protocols to control center protocols
- Local or remote HMIs
- Serial Server – Provide communications path to connected IEDs for maintenance, monitoring and control. Connecting through the Gateway can also provide an encrypted communication channel and ensures that only authorized personnel can modify device settings.

Some Gateways have the ability to act as both a slave and a master. The SCADA system interrogates Gateway as if it were a substation device. The Gateway is thus a slave to the SCADA.

However, since it is connected to the substation devices, it must also be able to perform the functions of a master, such as polling for data and sending control requests.

Gateway internal architecture is based on a series of software components:

- Slave protocol components to implement all the functions necessary to process requests received from a SCADA or control center.
- Master protocol components to implement the functions necessary to poll devices and send control requests. This component is responsible for device polling for data collection which is stored in the Gateway internal data base, where it becomes available to the SCADA.
- Communication components including RS-232, RS-485 or TC/IP interfaces used by the protocol components to communicate with control centers and devices.

The Gateway database provides time and date stamping and stores:

- Power System values
- Device tags used for control functions
- Sequence of Event files.
- Oscillography files

Since it is connected between the substation devices and the control centers, the Gateway is available for implementation of advanced processing functions that would be impossible to perform with less sophisticated devices. The Gateway can also be capable of providing automation functionality such as programmable logic which eliminates the need for an external PLC to implement automation scripts, such as those used for reclosers and load balancing.

19. IEEE 1588 Precision Time Protocol (PTP)

19.1 Brief history of Precision Time Protocol

Precision Time Protocol (PTP) has come about as a natural progression to Network Time Protocol (NTP). Over time, it became apparent that a more precise timing protocol that was usable across multiple transport technologies was necessary. There is a hierarchy for the Timing protocols, starting from the least accurate to the most. Table 38 shows the relationship between these protocols.

Precision Time Protocol was first voted a standard in 2002, with changes needed over the next several years culminating in the v2 standard in 2008.

Table 38 Timing Protocol Hierarchy

Specification	RFC/IEEE	Accuracy
SNTP (1992)	RFC 2030	50-150msec
NTP (1985)	RFC 1305	500usec-50msec
PTP (2002)	IEEE 1588	1nsec-100usec
PTP v2 (2008)	IEEE 1588 v2	

19.2 What is Precision Time Protocol?

Timing relationships between devices are integral to industrial systems. These temporal (time based) requirements are met in one of three ways:

- Message based- the periodic activation of a function based upon the receipt of a message.
- Cyclic based- cyclic-systems timing is periodic and is usually defined by the characteristics of an out of band cyclic network or bus. The accuracy is dependent upon the accuracy of the cycle. Sercos is the most used cyclic system in industrial networks. IRIG-B is another example of a cyclic based timing used in Utilities based systems.
- Timing based- In time-based systems the execution of events and functions is based on a common sense of time. Time based systems operate in band- that is in the data stream. If each device knows precisely when 3 o'clock is and knows what position or action is to be taken at 3 o'clock, it only takes one controller to make the whole system function in an accurately coordinated manner. It also allows devices in the time based network to work on different time schedules using the same master clock for reference. PTP is a time based system.

PTP is the latest iteration of standards based timing protocols, such as Simple Network Time Protocol (SNTP) and NTP. It addresses a need that has been identified for a highly tuned and interactive timing protocol that is able to dynamically measure and compensate for timing differences between nodes in a control environment, whether it is motion control, breaker actuation, distributed printing or any other application that would require highly accurate time. In electric utility applications, PTP will be used for digital fault recording, IEC 61850 process bus and synchrophasor applications.

PTP is a protocol that is transport protocol agnostic, meaning that the operation of PTP is not impeded by the transport protocol it runs on. So it can run on RS-232, T-1 frame relay, Ethernet, etc. The implementation for use in Utility environments is mainly Ethernet based. IEC 61850 is currently undergoing changes that will bring in and standardize the use of IEEE1588, but it is still a work in progress. The IEEE PSRC working group PC37.238 (as of May 2011) is close to finalizing an "IEEE 1588 Power Profile" that will standardize how PTP is used in electric utility applications. The Power Profile will also specify default parameters and accuracy requirements that will allow Engineers to design communication networks that will also deliver highly accurate time synchronization.

The use of PTP can vary depending on the application. Table 39 shows the overall synchronization requirements for various applications.

Table 39 Timing Requirements for Applications

Applications	Synchronization Accuracy
Low speed sensors	Milliseconds to Seconds
Common electromechanical devices such as breakers, relays, solenoids, etc.	Low Milliseconds
General automation- Process and materials handling	Milliseconds
Motion Control- coordinated printing, robotics, high speed labeling	Low microseconds
High speed electrical devices- synchrophasor synchronization, IEC 61850 Control Bus	Microseconds
Electronic ranging	Sub Microsecond, Nanosecond

PTP can be software based or hardware based for implementation. Of the two, hardware based is the most accurate as the time stamping is done very close to the physical layer, whereas software based is done much higher up the OSI protocol stack. To achieve the 1us accuracy as specified in the PC37.238 Power Profile hardware based time-stamping will be required.

Figure 83 shows the operation of IEEE1588 inside a device.

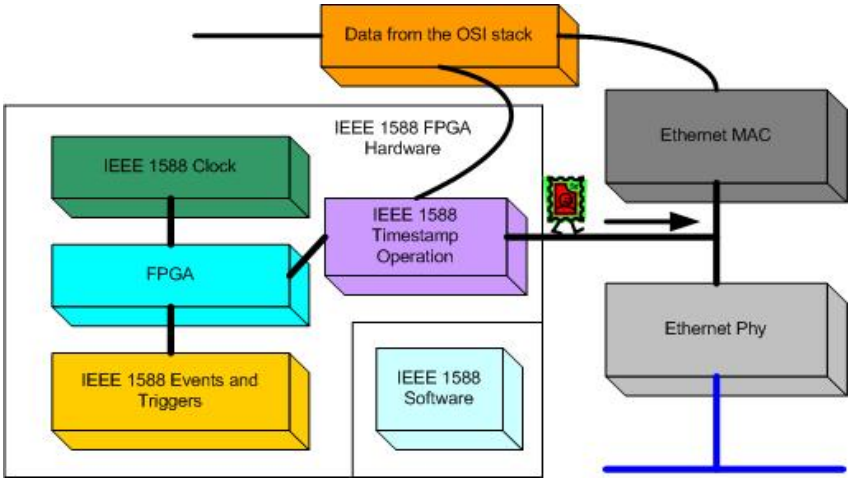


Figure 83 – IEEE 1588 Hardware Device Diagram

Of course, the preferred operation for IEEE1588 is hardware based, but software based operation can be useful for devices that do not need extreme time accuracy but still need to maintain semi accurate timing for events management like PCs and servers.

19.3 How PTP works…

First and foremost, PTP is an interactive protocol between devices. To prevent confusion, we will be concentrating on IEEE 1588 v2, which uses an operation called transparent clock. In PTP environments, there are several needed parts to make it all work.

- Ordinary or Slave clock- a PTP clock with only one port, normally used in end devices or IEDs
- Master clock- In IEEE 1588, each PTP domain must have a clock from which all timing is derived for the domain. Each master clock can have a backup in case of failure.
- Grand Master clock- this is a highly tuned source clock for the IEEE 1588 network where all the time is derived. Grand master clocks generate the central timing for the master clocks of each domain. In electric utility applications, the Grand Master clock will often be synchronized by a GPS source to ensure high accuracy. If there is only one identified domain, the master clock is also the grand master.
- PTP domain- in PTP, you can group devices into logical associations that have the same master clock serving them. You can have multiple domains resident on the same physical network infrastructure.
- Transparent clock- A new addition to the IEEE 1588 v2 standard, a transparent clock is built into a network switch, allowing the switch to forward time synchronization packets from the master to slave without adding time inaccuracy. The switch measures switch residence time and propagation delay and compensates for it in the sync packet in one-step mode or in the follow-up message in two step mode.

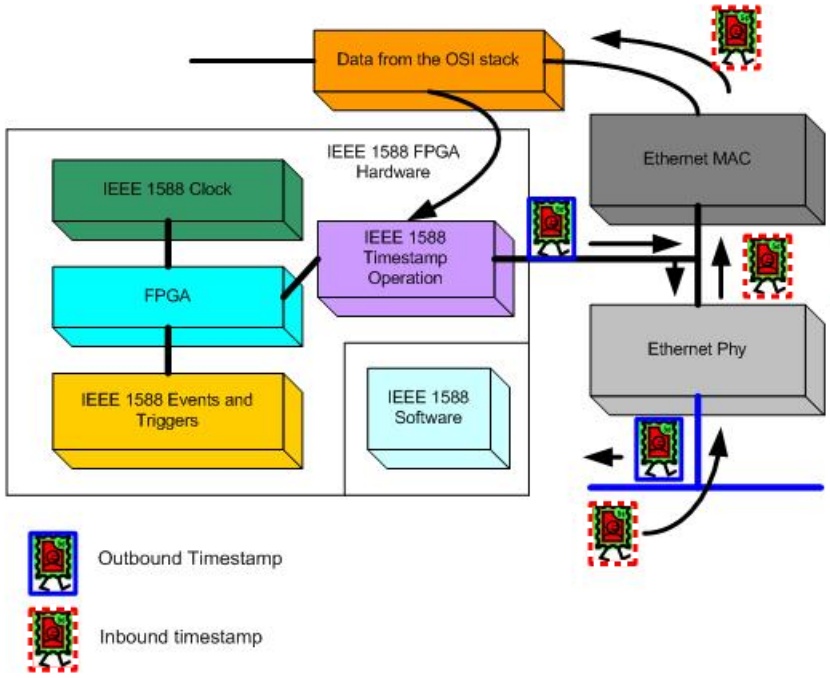


Figure 84 – Inter-device timestamp movement for PTP

Figure 84 shows the operation of the time stamping and sync messages that are passed across the network at the device level. Figure 85 shows an example of a PTP network including the transparent clock (TC) operation in Ethernet switches supporting IEEE 1588.

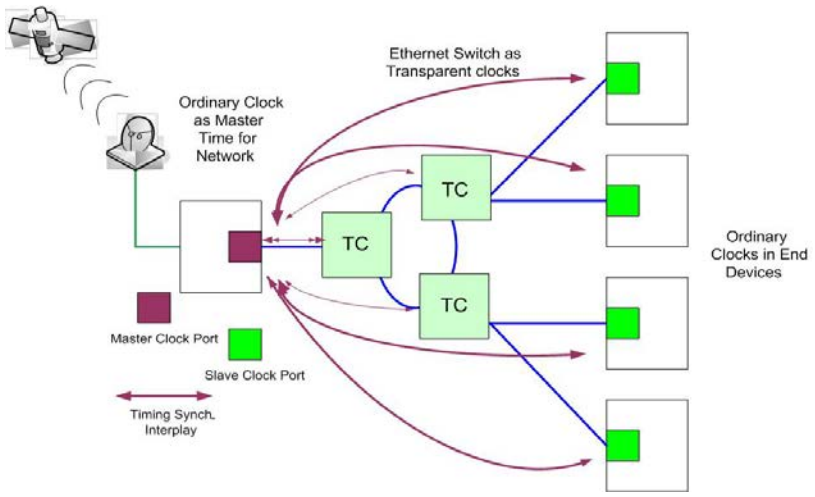


Figure 85 – IEEE 1588 v2 Overall PTP Network Example with Transparent Clocks

Transparent clocks came about because it was noticed that in the first version of IEEE 1588, that the clock used, called a boundary clock, made each switch in the Ethernet network be the master clock for everything attached to it, including the next switches in the network. End users typically cascade Ethernet switches, causing a huge swing in the timing accuracy to the point that some applications such as coordinated motion control were almost unusable. A transparent clock used in version 2 eliminates this issue by allowing the time synch messages to pass through the switch and keeping the same timing source active across the whole network rather than multiple distributed clocks as in the old method. Figure 86 shows the boundary clock example.

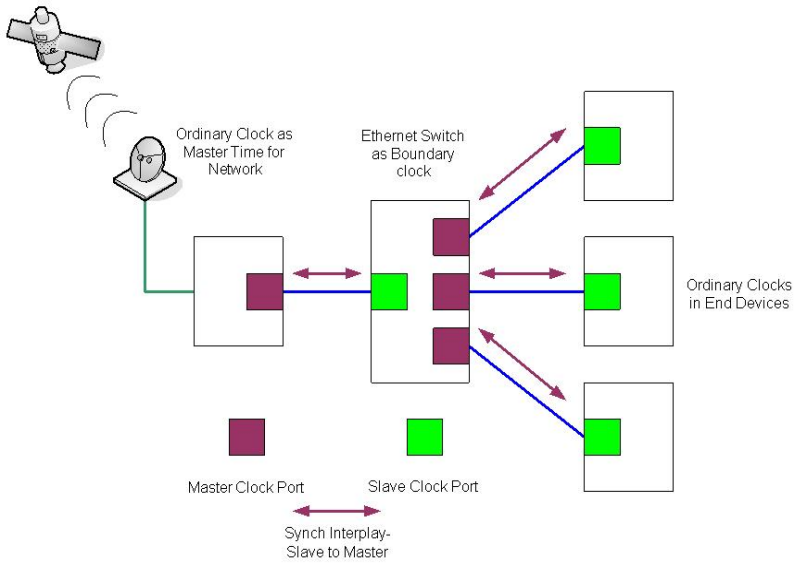


Figure 86 – IEEE 1588 v1 Boundary clock example

PTP synchronization is a multi-step process that is an interaction between the master switch and the slave switch. Figure 87 shows the basic time synch operation between the master clock and end device.

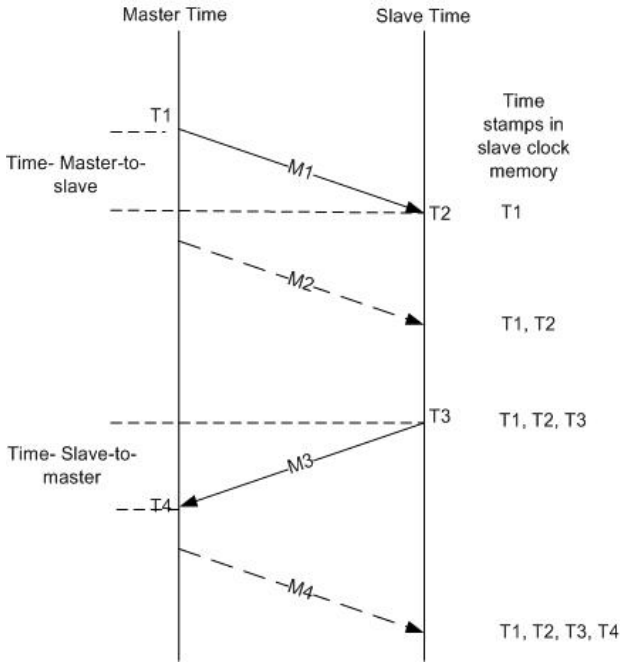


Figure 87 – Basic PTP Synch Message Operation

The message exchange pattern is:

- The master clock sends a message M1, referred to as Sync Message, to the slave clock and notes the time, t1, at which it was sent.
- The slave clock receives the message M1 and notes the time of reception, t2.
- The master clock conveys to the slave the timestamp t1 by:
    - Embedding the timestamp t1 in message M1. This requires some sort of hardware processing for highest accuracy, or
    - Embedding the timestamp t1 in a second message M2, referred to as Follow_Up. This can be done in software since the timing is not critical.
- The slave clock sends a message M3, referred to as Delay_Req, to the master clock and notes the time, t3, at which it was sent.
- The master clock receives the message M3 and notes the time of reception, t4.
- The master clock conveys to the slave clock the timestamp t4 by embedding it in a message M4, referred to as Delay_Resp

The slave clock then takes all four timestamps it has received and computes the offset and mean propagation times between the master and slave clocks. When computing the offset and mean propagation times between the master clock and slave clock with an Ethernet network in the middle, the intervening switches that support PTP must also add Peer Delay measurements so that the proper offset between the master and slave take into consideration the delay of the data going across the Ethernet switches. Figure 88 shows the basics of this operation.

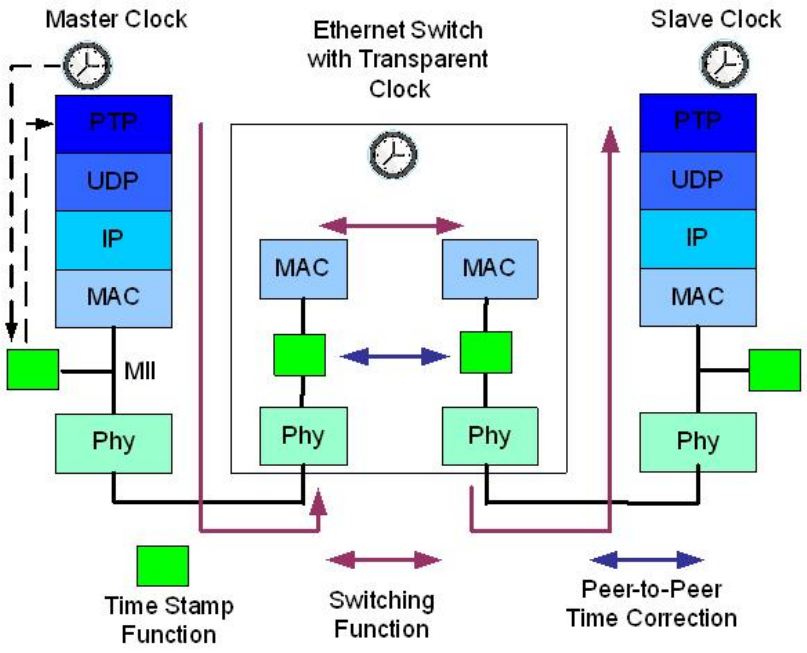


Figure 88 – PTP Message Interaction with Ethernet Switch

19.4 PTP Applications

PT has seen much growth in use over the last several years as hardware has been developed that can handle the needs of the PTP applications. These applications are primarily within the Industrial, Utility, Military and Telecommunications communities.

19.4.1 Utility- IEC 61850 Process Bus

With the advent of merging units within 61850 that are able to monitor multiple aspects of the transmission system (voltage transformers, current transformers, I/O operation) and send this information to a central site as well as utilize peer-to-peer communication within the station with other merging units monitoring other lines, it is necessary to have extremely accurate timing between the merging units. PTP can provide this timing embedded within the Ethernet network that is connected to the merging units.

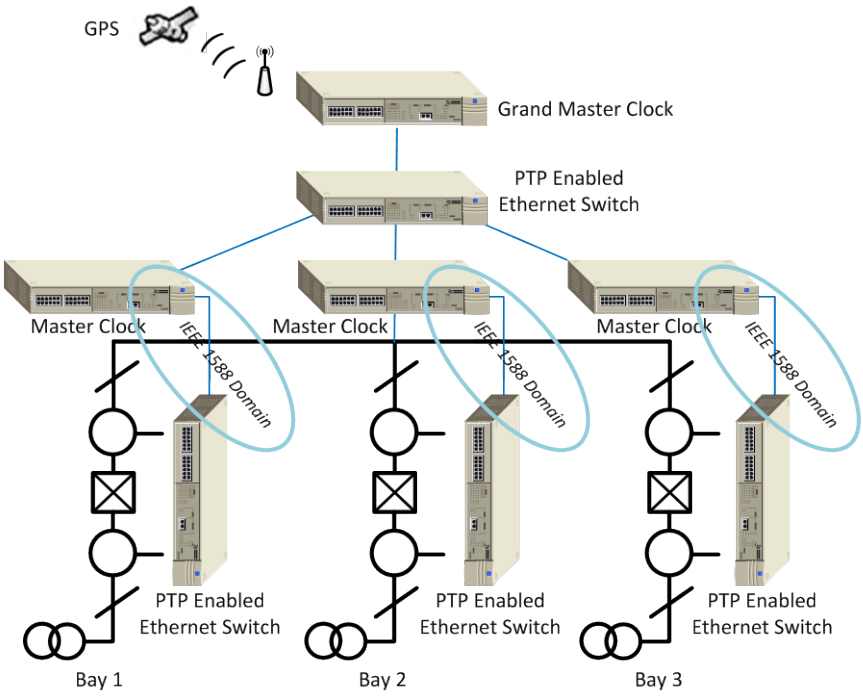


Figure 89 – PTP Applied for Process Bus Time Synchronization

19.4.2 Utility- Distributed generation of IRIG-B cyclic timing

As a way to provide Utility end customers the ability to slowly back out devices that rely on IRIG-B for timing, it is possible to generate the IRIG-B cyclic time from an IRIG module on a PTP hardware enabled Ethernet switch. This lets the customer remove most of the necessary coax cable that is run through a transmission substation and only leave the coax to connect to the Ethernet switch IRIG-B module. This is a money saver for several reasons:

- It allows the customer to do a phased replacement of IRIG-B timed devices to IEEE1588 timed devices.
- It removes extra coax cable which is expensive to support and replace. Using Ethernet cable to distribute the data and PTP timing in a converged network is a much cheaper option to install and maintain.

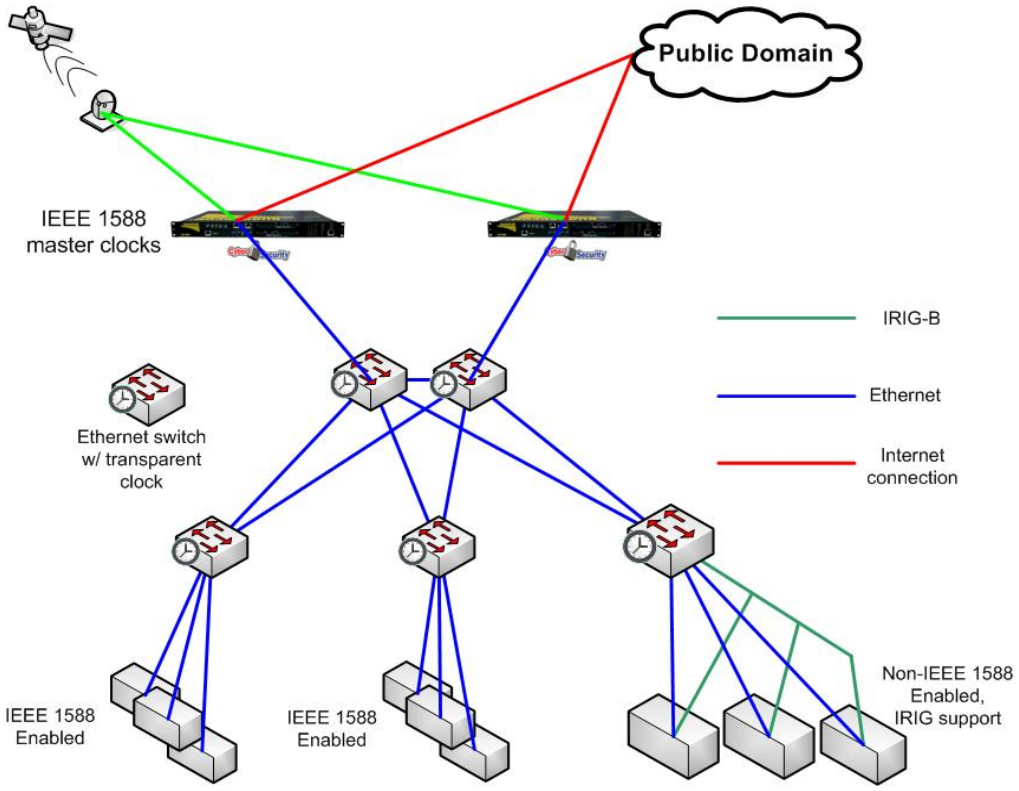


Figure 90 – Time Synchronization Methods

20. Power Line Carrier

20.1 Media

Power Line Carrier Communication (PLCC) involves transmission of communication signals over power transmission lines, either overhead or underground. For relaying purposes, the frequency of the carrier communication signal is typically in the range of 20 kHz to 500 kHz. Since this range falls well between audio and radio frequencies, the interference is minimal. Carrier signal can be transmitted over one, two or three phase conductors. Overhead transmission lines have good high-frequency transmission characteristics. They allow only 0.02 to 0.2 db/km loss in signal, depending on the line voltage and frequency. Thus, this technique provides a robust, reliable low-loss transmission path that is in full control of utility. In some applications the Ground Cable has been used as the communications media.

Signal attenuation is not affected appreciably by rain, but serious increase in loss may occur when the phase conductors are thickly coated with frost or ice. Attenuations of up to three times the fair weather value have been experienced. Receiving equipment commonly incorporates automatic gain control (AGC) to compensate for variations in attenuation of signals. The signal attenuation also increases during faults, the value depending on the type of fault. Most utilities select a nominal value, usually between 20 and 30 dB, as an application guide to account for attenuation during faults [1]. A protection signal boost facility can be employed to account for this increase in

attenuation, to maintain an acceptable signal-to-noise ratio at the receiving end, so that the performance of the service is not impaired.

20.2 System Overview

In the picture below the main PLCC components are depicted, where the line trap, also know as wave traps, (shown as TRAP), the Coupling Capacitor (CC) and Line Tuner (LTU) are located outdoor in the substation yard; the PLCC radio equipment with Teleprotection, packet switching, voice channels, data channels, telemetry channels, etc. shown in the figure as DPLC, CH-1 and CH-2 is the indoor equipment, usually collocated with the protection and control equipment in the control room. The outdoor and indoor equipment is connected via a coaxial cable installed through the substation trenches.

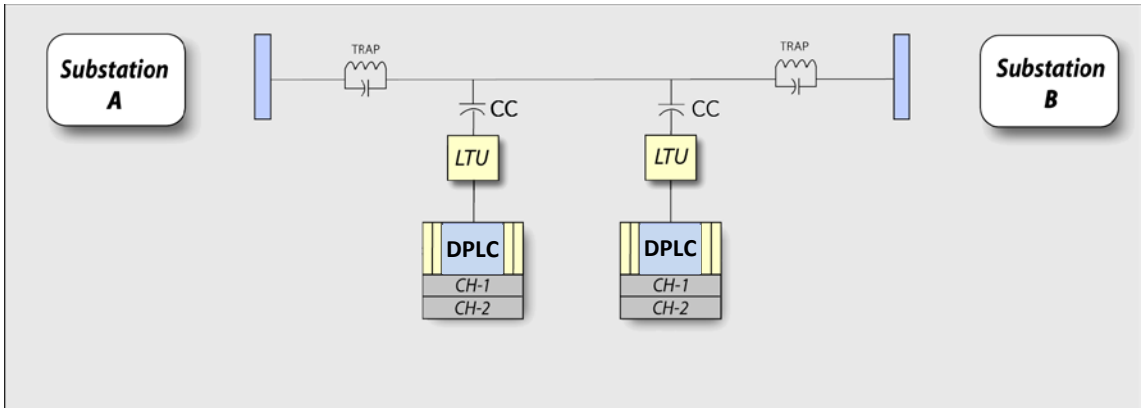


Figure 91 – PLC System Diagram

20.3 Coupling

The coupling to the high voltage power line is performed using three components, the line trap, the coupling capacitor and the line tuner. The line trap is an air core coil which blocks the PLCC frequencies going to the transformer. The coupling capacitor and the line tuner works in conjunction as a RF filter, either low pass, high pass or bandpass. The filter is tuned to the best impedance matching between the power line and the PLCC radio equipment.

20.3.1 Coupling Schemes

[27] As with most systems, there is more than one way to couple the carrier to the power line. The deciding factor may be economy, performance or a compromise of the two. That is, the best performance may be too expensive to justify for the line being protected so the next best one may be the preference. Most protective relay channels use single-phase-to-ground coupling, requiring only one set of coupling equipment (line tuner, coupling capacitor and line trap). Multi-phase coupling may be used to improve dependability, but requires multiple sets of coupling equipment. The coupling schemes with least losses (ranked in order of least losses) are shown below:

- Mode 1 Coupling (Out on two outer phases, in on the center phase)

- Center phase to outer phase (push-pull)
- Center phase to ground
- Outer phase to outer phase with ground return (push-push)
- Outer phase to ground (only on short lines)

On important, long EHV lines, mode 1 coupling has been justified, even though it requires line traps, coupling capacitors and line tuners in all three phases.

What follows is a brief description of the more typical forms of coupling.

Single Line to Ground

The best single-phase-to-ground scheme uses the center phase for coupling. The center phase provides the most mode 1 coupling. Using one of the outside phases will introduce more mode 2 and mode 3 coupling than desired. Figure 92 shows an example of phase-to-ground coupling.

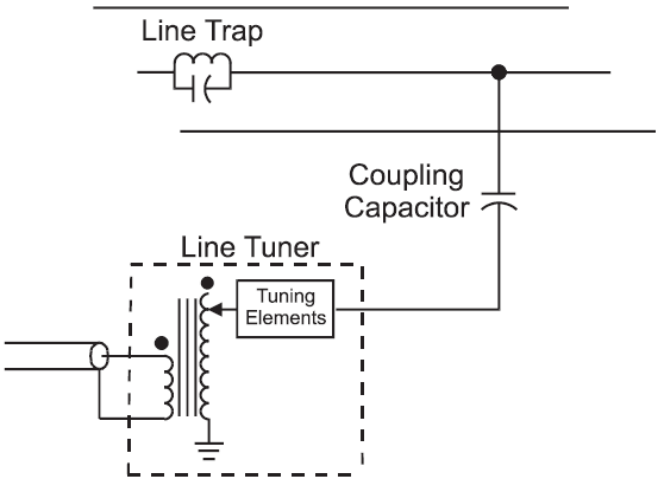


Figure 92 - Single Phase-to-Ground (Center Phase) Coupling

Phase to Phase

Some applications will require greater dependability. When the protected line is of significant importance and the type of protection requires receipt of the signal during an internal fault, multiphase coupling improves dependability of the signal being transmitted through the fault.

Since the most frequent type of power system fault is a phase to ground, you can improve your chances of receiving the signal through the fault if more than one phase is used.

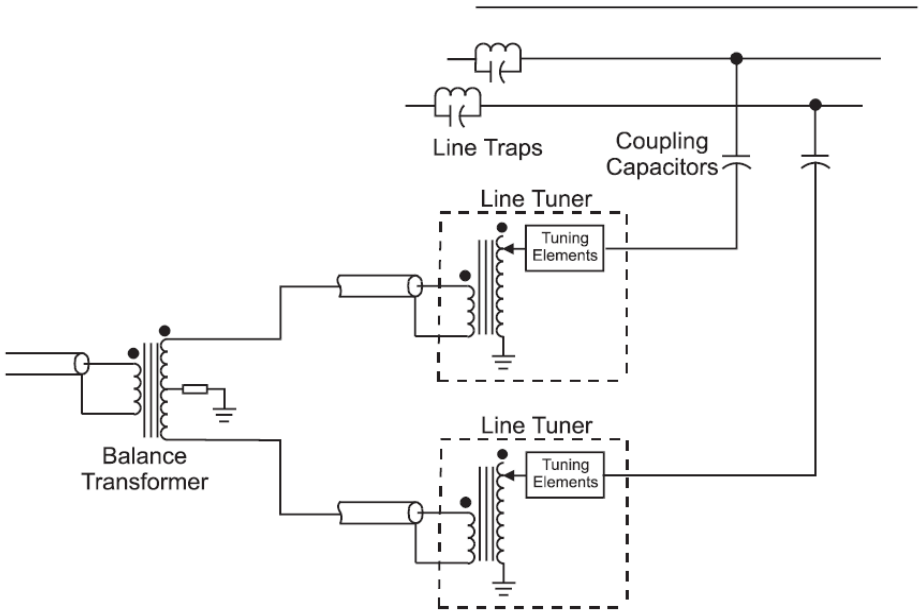


Figure 93 - Phase-to-Phase Coupling

Mode 1

In EHV applications where the protected line is long and of major importance, mode 1 coupling is used to get the maximum received signal.

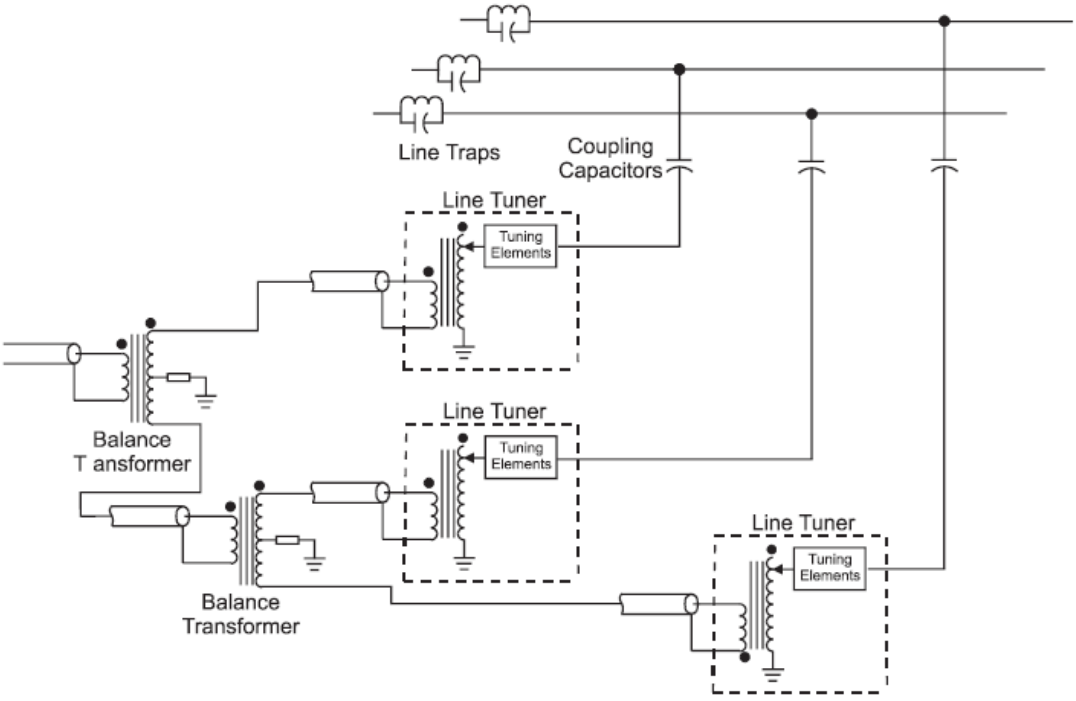


Figure 94 - Mode 1 Coupling

As shown in Figure 94, this requires the use of three sets of coupling equipment as well as additional balancing transformers.

20.3.2 Line Trap

The Line Trap, also known as Wave Trap, is an air core type of coil inserted in series with the high voltage power line to prevent carrier-frequency loss of a signal in the range of 20 to 500 kHz. A special type has been made for the ground wire which varies between 0.1µH and 2.0 mH. Its application size will depend on the nominal current and voltage of the particular system.

Figure 95 – Line Trap

The line trap consists of three main components: main Coil, Tuning Device and Protective Device.

20.3.2.1 Main Coil

The main coil carries power frequency currents as well as short-circuit currents of the power system. The main coils should be made with a very strong structure as well as materials that should not be susceptible to aging in outdoors extreme weather conditions to provide high mechanical strength, corrosion-resistance and low loss.

20.3.2.2 Mounting Options

The mounting options are three:

- Horizontal
- Vertical
- Suspension

20.3.3 Tuning Device

The tuning device generally consists of a capacitor, inductor and resistor, combined with the main coil to form a resonant circuit to block carrier signals. High voltage capacitors should be used to provide proper insulation. This tuning pack makes the line trap either wideband, narrowband or single frequency and high pass.

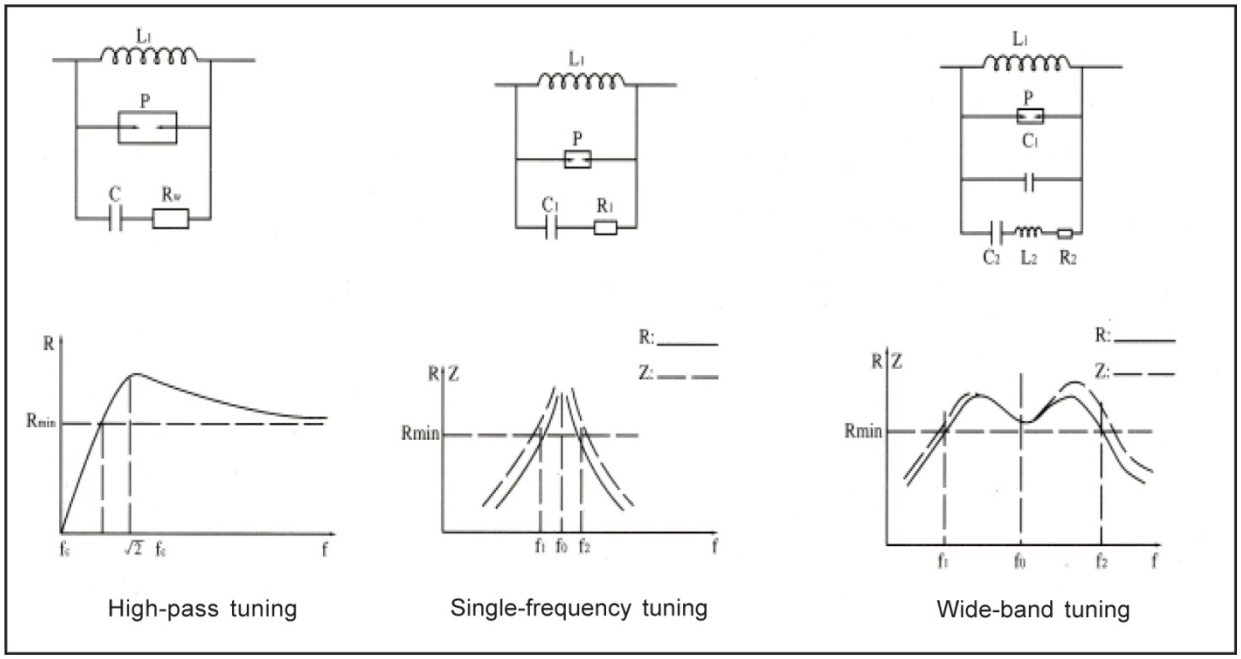


Figure 96 – Tuning Device Circuit Diagrams

20.3.4 Protective Device

The protective device is used to protect the main coil and the tuning device. It should limit lightning and switching over-voltages applied across line traps to a certain extent.

20.3.5 Coupling Capacitor

The coupling capacitor is made of capacitors in series covered by high voltage insulation. Additionally, in the base, there are other devices like the drain coil, which serve as the carrier connection accessory or inductive potential transformers to supply the high voltage measurement. Typical values range from 1,500 to 25,000 pF. The application value will depend of the type of coupling required for a specific system. The line trap usually mounts over the coupling capacitor. The carrier accessories are the voltage limiter, grounding switch and drain coil. All these devices are found in a box at the base of the coupling capacitor.

One side of the capacitor goes to the power line and the other side goes to the drain coil. The drain coil other side is connected to ground. In the connection between the capacitor and the drain coil is where the PLCC signals are injected. The drain coil value is such that the low frequencies go to ground and the high frequencies see a large impedance.

The installation of the coupling capacitor is over a pedestal.

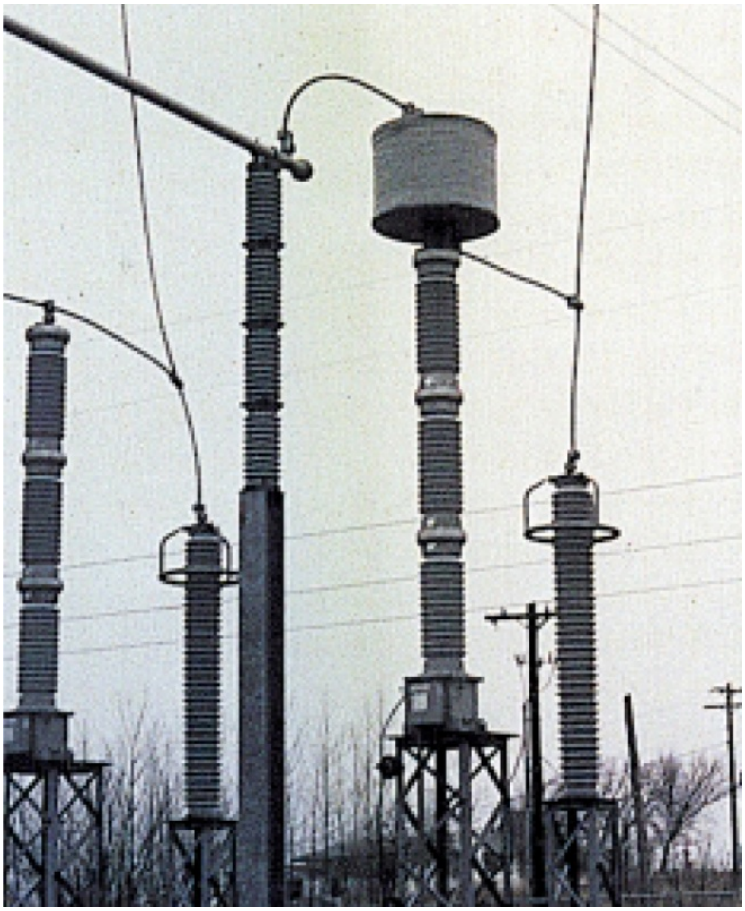


Figure 97 – Coupling Capacitor and Line Trap Assembly

20.3.6 Line Tuner

The line tuner matches the impedance of the power line carrier terminal to that of the high voltage power line in order to reduce the insertion loss for the transmission of PLC signals over the power line. In addition the line tuner provides voltage isolation and protects against transient overvoltages. The peak envelope power (PEP) rating should be over 400 watts.

Figure 98 – Typical Line Tuning Assembly

There are different types of line tuners, including high pass, low pass and band pass (narrow or wide). The line tuner has many capacitors and inductors, the arrangement will depend on the type of line tuner.

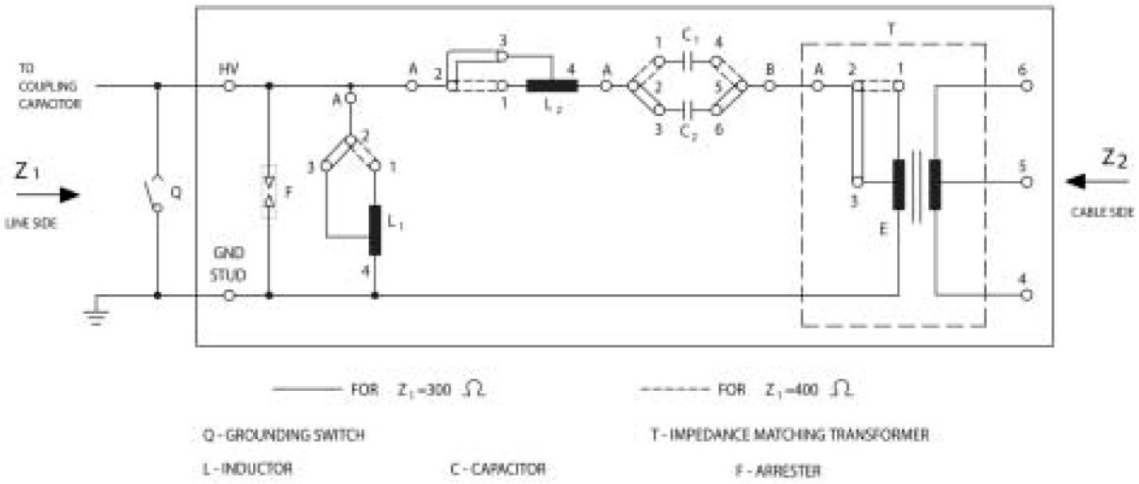


Figure 99 – Line Tuner Circuit Diagram

20.4 PLCC Equipment

There are different types of PLCC, depending on the application:

- FSK

- Tone ON/OFF
- Multifunction Analog
- Multifunction Digital

20.4.1 FSK PLCC

This equipment is a Frequency-Shift Keyed power line carrier system type of modulation. Typical applications include Direct Transfer Trip (DTT- single or dual channel), Permissive Transfer Trip (PTT), Directional Comparison Unblocking (DCU) and dual phase comparison. The equipment can be used as transceiver (Tx/Rx), transmit only (Tx), receive only (Rx), dual transmitter (Tx/Tx), or dual receiver (Rx/Rx).

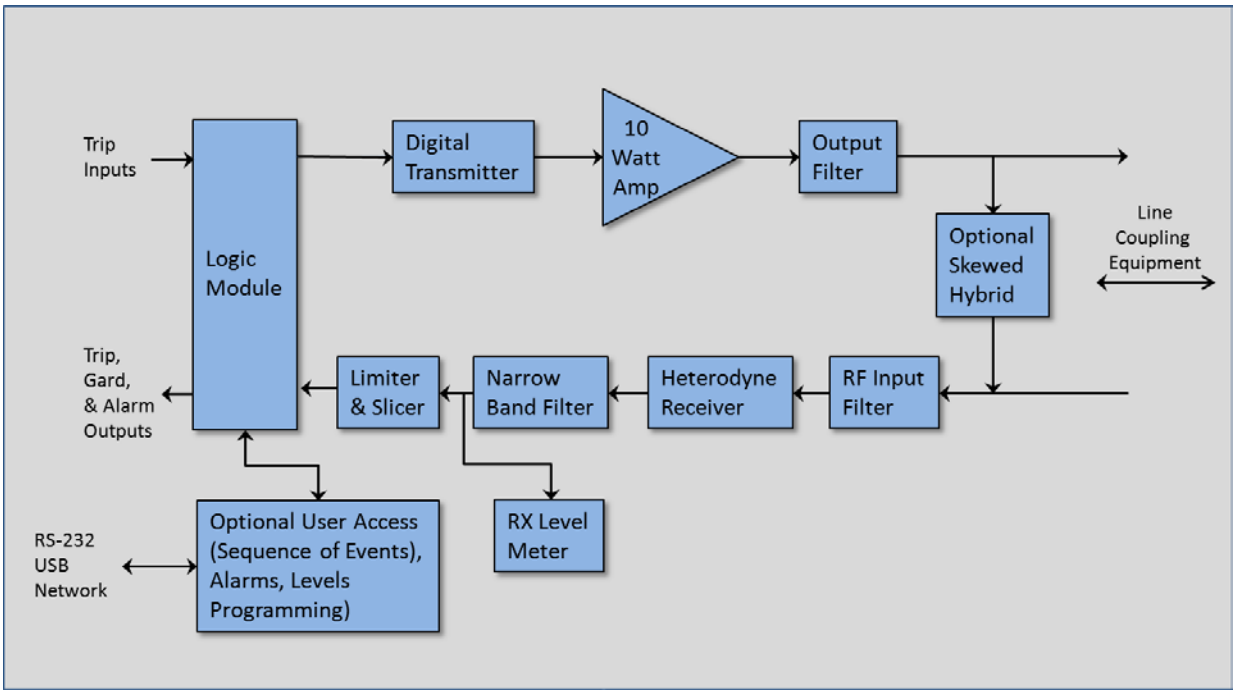


Figure 100 – FSK PLCC Block Diagram

20.4.2 ON/ OFF PLCC

The ON/OFF PLCC is an amplitude-modulated power line carrier transmitter/receiver. It is used for directional comparison blocking applications in high speed protective relaying communications. Sometimes there is a service voice channel available.

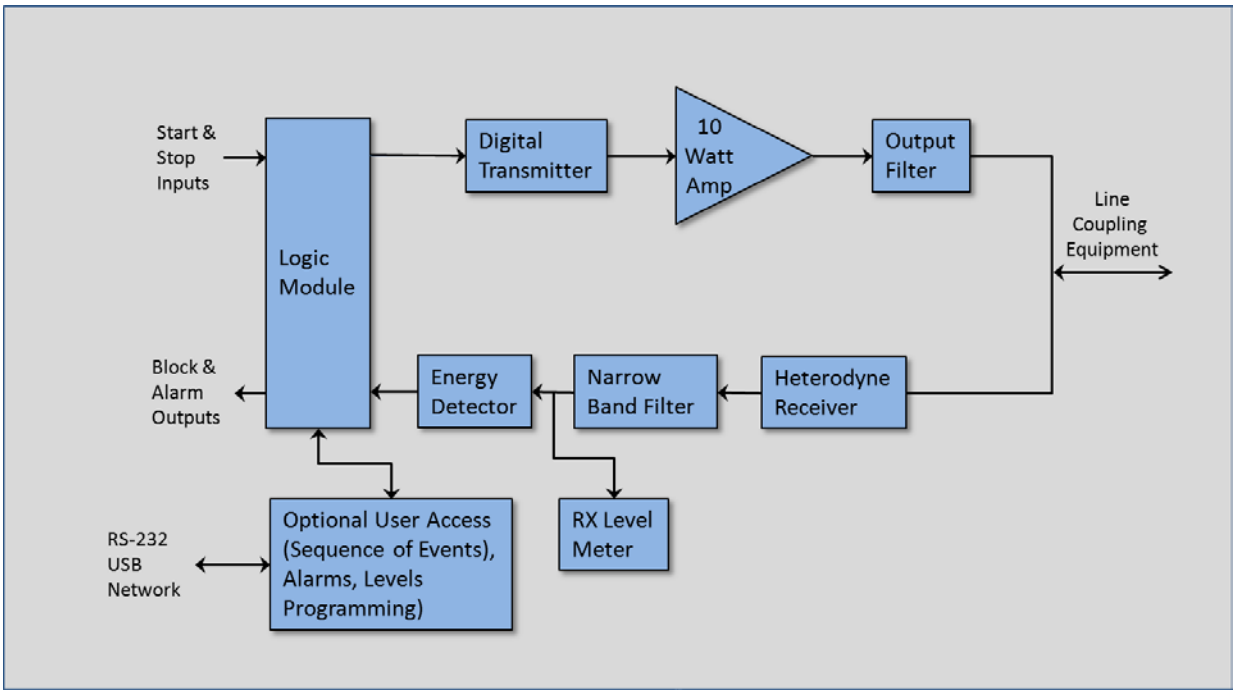


Figure 101 – ON/ OFF PLCC Block Diagram

20.4.3 Multifunction

The Multifunction PLCC is a piece of equipment that accepts various inputs, such as: voice, low speed data, telemetering and teleprotection. All these inputs are multiplexed and sent/received by a modulated carrier, which is typically is SSB, QAM or OFDM. SSB (Single Side Band) is an analog type of modulation and the other two, QAM (Quadrature Amplitude Modulation) and OFDM (Orthogonal Frequency Division Multiplexing), a digital type of modulation.

20.4.4 Analog PLCC

The analog multifunction PLCC has been in use for a long time, providing many functions, all multiplexed and modulated by an SSB type of modulation.

Digital Signal Processing technology (DSP) is sometimes used for filtering purposes to replace LC (inductance and capacitive) filters. In conjunction with intensive math algorithms, the same DSP technology can replace the modulation and demodulation stages.

Transmission channels are from 20 to 500 kHz in steps of 4 kHz. Voice, data, telemetry and teleprotection channels are multiplexed to be transmitted. Adjacent channel selectivity needs to be of high quality. Cross talk, idle channel noise and spurious outputs are required to be minimized.

20.4.4.1 System Architecture

Figure 102 below depicts a system architecture containing the following modules found in a PLCC:

- Teleprotection
- Transceiver
- Voice Interfaces
- Data Interfaces
- Line Interface
- Power Amplifier
- Hybrid
- Tx and Rx Filters

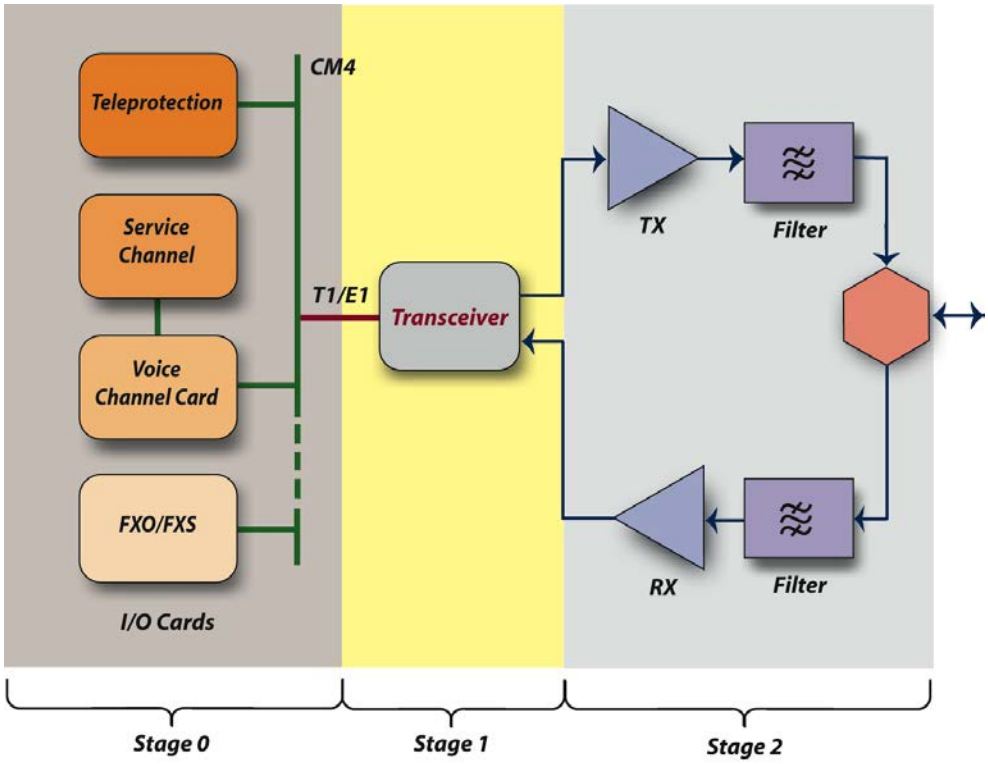


Figure 102 – Analog PLCC System Architect Block Diagram

20.4.4.2 Detailed Functionality

Transceiver

The Power Line Carrier Transmitter and Receiver typically include the Modulator and Demodulator, Digital Filtering, Numerical Control Oscillator (NCO) and RS-232 interface for configuration. This module has many functions as follows:

- Provide SSB modulation and demodulation
- Translate and convert the analog source to a digital frame, this frame is properly filtered and then translated into the frequency range from 20 to 500 kHz, once at line frequency is converted from a digital processed frame to an analog signal.

- Perform line frequency programming, setting of the speech plus filters, configuration, diagnostics, impedance matching and level adjustment for Transmission and Reception.
- Perform Automatic Gain Control (AGC) to compensate for variations in signal level caused by line attenuation changes.

Channel Multiplexer

The channel multiplexer integrates voice and data traffic across a single channel.

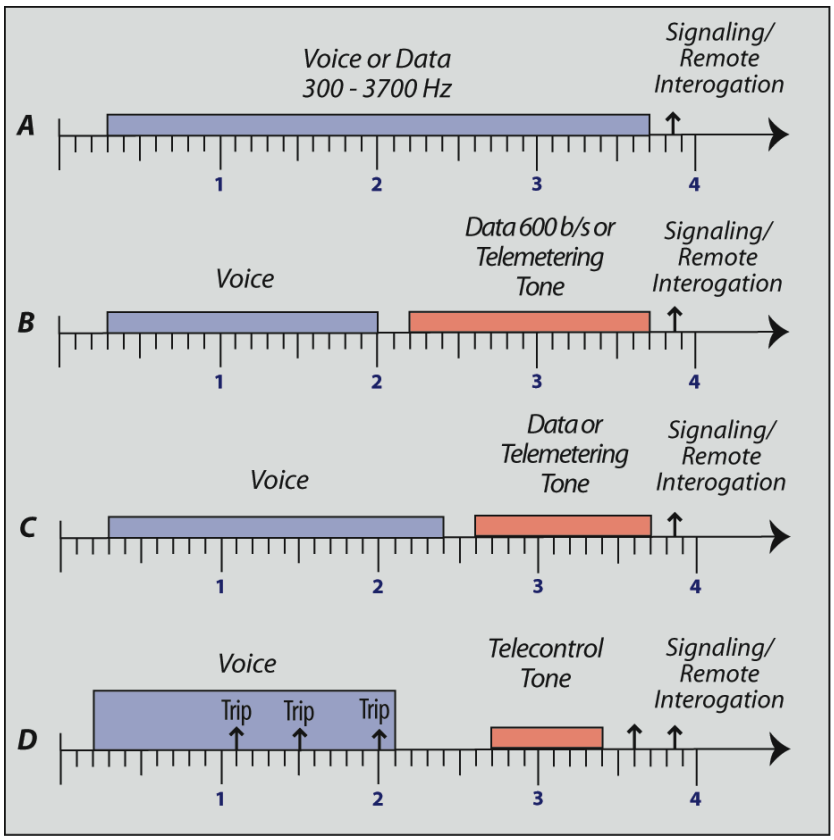


Figure 103 – Data / Voice Multiplexing

20.4.4.3 Human Machine Interface

A software interface (GUI) program allows the user to configure the internal parameters like the carrier frequency to the NCO (Numerical Control Oscillator), adjust output power level, as well as to measure the SNR, alarms, etc. See Figure 104 for typical setup screen.

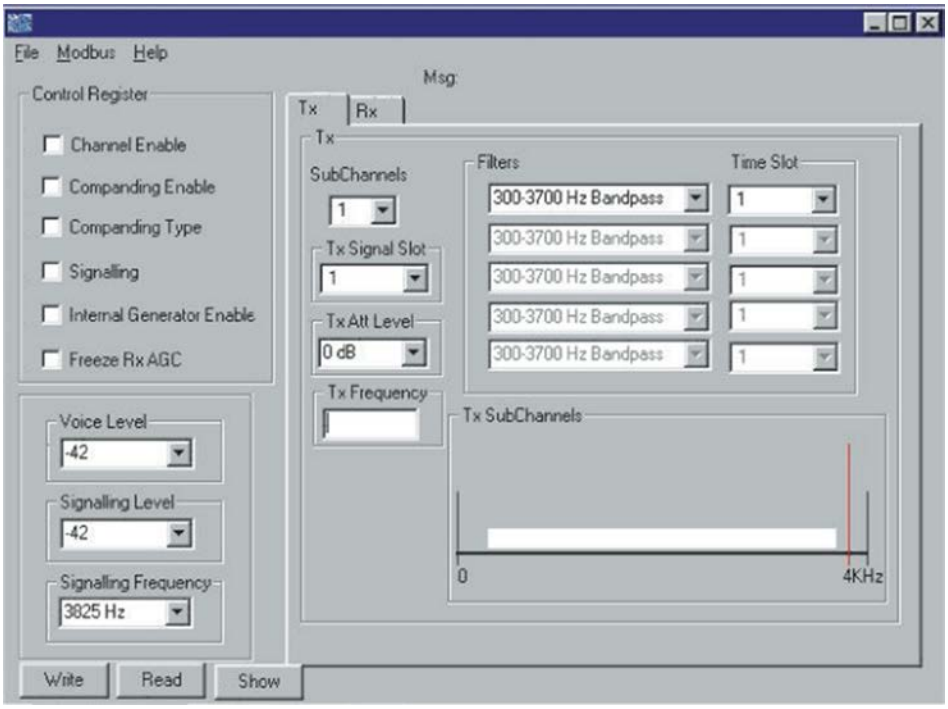


Figure 104 – Typical Analog PLCC Human Machine Interface

20.4.5 Digital PLCC

The digital multifunction PLCC is much newer in the market providing multiple functions multiplexed in a data stream and modulated by QAM or OFDM type of modulation.

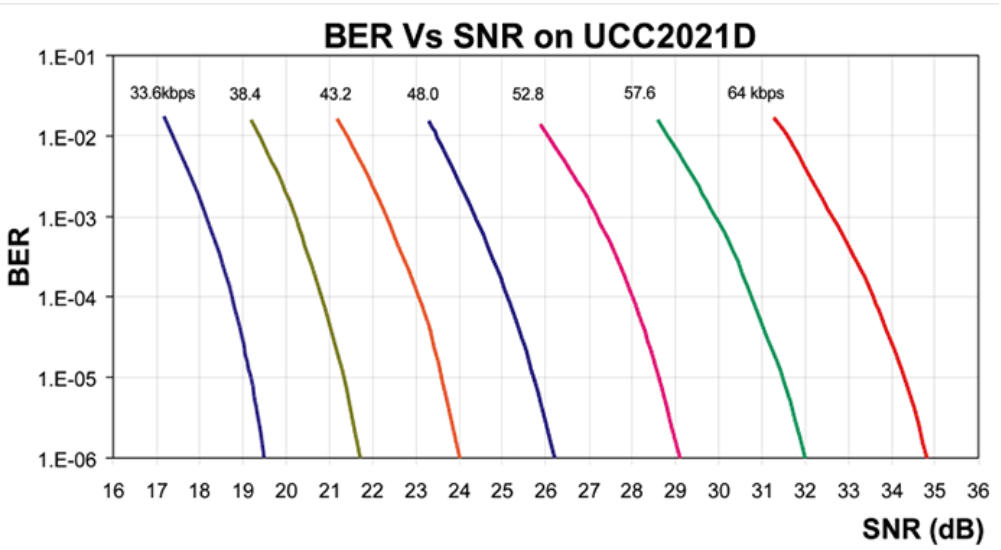


Figure 105 – Digital PLC Bit Error Rate vs. Signal-to-Noise Ratio Diagrams

Digital Signal Processing technology (DSP) is the basis for this type of equipment. DSPs are a specific type of microprocessor that can perform digital filtration, voice processing, data

processing and digital modulation at a very high speed. Teleprotection is done in parallel in the analog domain due delay constraints. A data packetizer multiplexing technique is also used allowing digitized voice switching.

A transmission channel occupying a total bandwidth of 8 kHz will permit up to 64KBps digital data stream, making it suitable to replace analog systems using their existing frequency assignments. The DPLC may also operate in a bandwidth of 4 kHz at a reduced rate. The DPLC is programmable via the GUI or user interface, either locally or remotely.

For robustness, various algorithms for error detection and correction are used in order to achieve better performance in the presence of channel noise.

20.4.5.1 System Architecture

Figure 106 below depicts a system architecture containing the following modules found in a DPLC:

- Teleprotection
- Transceiver
- Data Packetizer
- Voice Interfaces
- Data Interfaces
- IP interface
- Line Interface
- Power Amplifier
- Hybrid
- Tx and Rx Filter

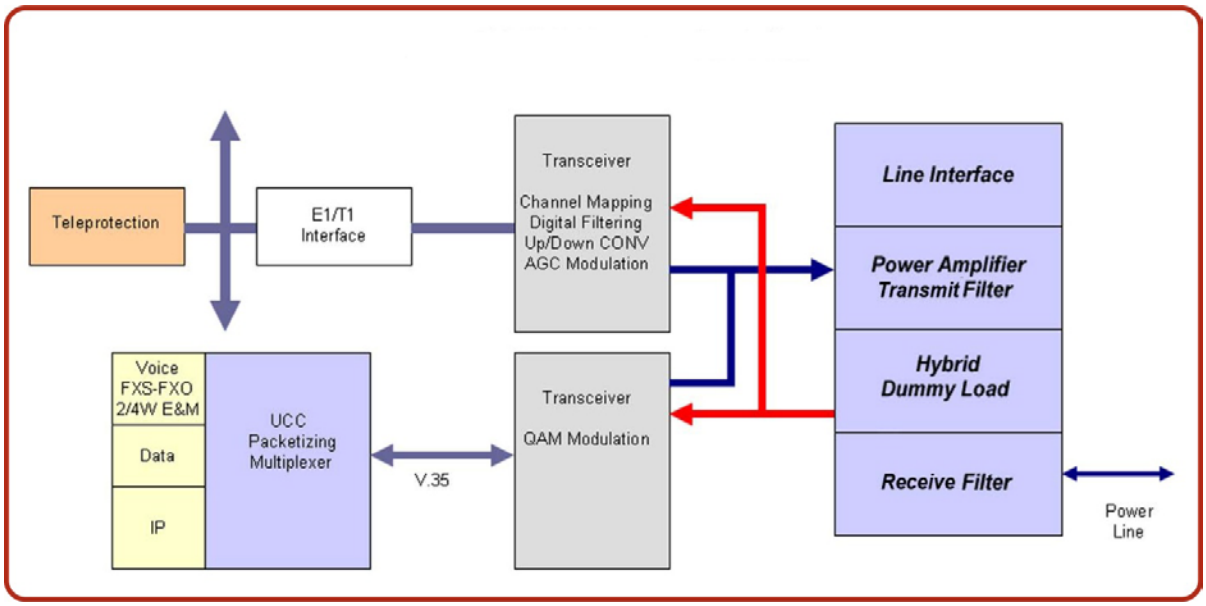


Figure 106 – Digital PLC System Architect

20.4.5.2 Detailed Functionality

Transceiver

The Power Line Carrier Transmitter and Receiver typically include the Modulator and Demodulator, Digital Filtering, Numerical Control Oscillator (NCO) and RS-232 interface for configuration. This module has many functions as follows:

- Provide Quadrature Amplitude Modulation (QAM) modulation
- Translate and convert the digital baseband source from the digital frame into the frequency range from 20 to 500 kHz
- Translate and convert the Line Frequencies into digital baseband or the digital frame
- Perform line frequency programming, setting of the speech plus filters, configuration, RS-232 Network Management System (NMS) Interface, diagnostics, impedance matching and level adjustment for Transmission and Reception.
- Perform Automatic Gain Control (AGC) to compensate for variations in signal level caused by line attenuation changes.

Packetizing Multiplexer

The packetizing multiplexer integrate voice and data traffic across a single, converged network utilizing a multi-service access gateway that uses data packets switched for distributed substation utility applications.

Analog and digital telephony channels as well as multiple data interfaces and serial data ports maybe included, some optimized specifically for distributed enterprise networks that have needs for multiple WAN connectivity requirements and differing needs for functionality, density, performance and connectivity.

Human Machine Interface

A software interface (GUI) program allows the user to configure the internal parameters like the carrier frequency to the NCO (Numerical Control Oscillator), adjust output power level, as well as to measure the SNR, alarms, etc. See Figure 107 for typical setup screen.

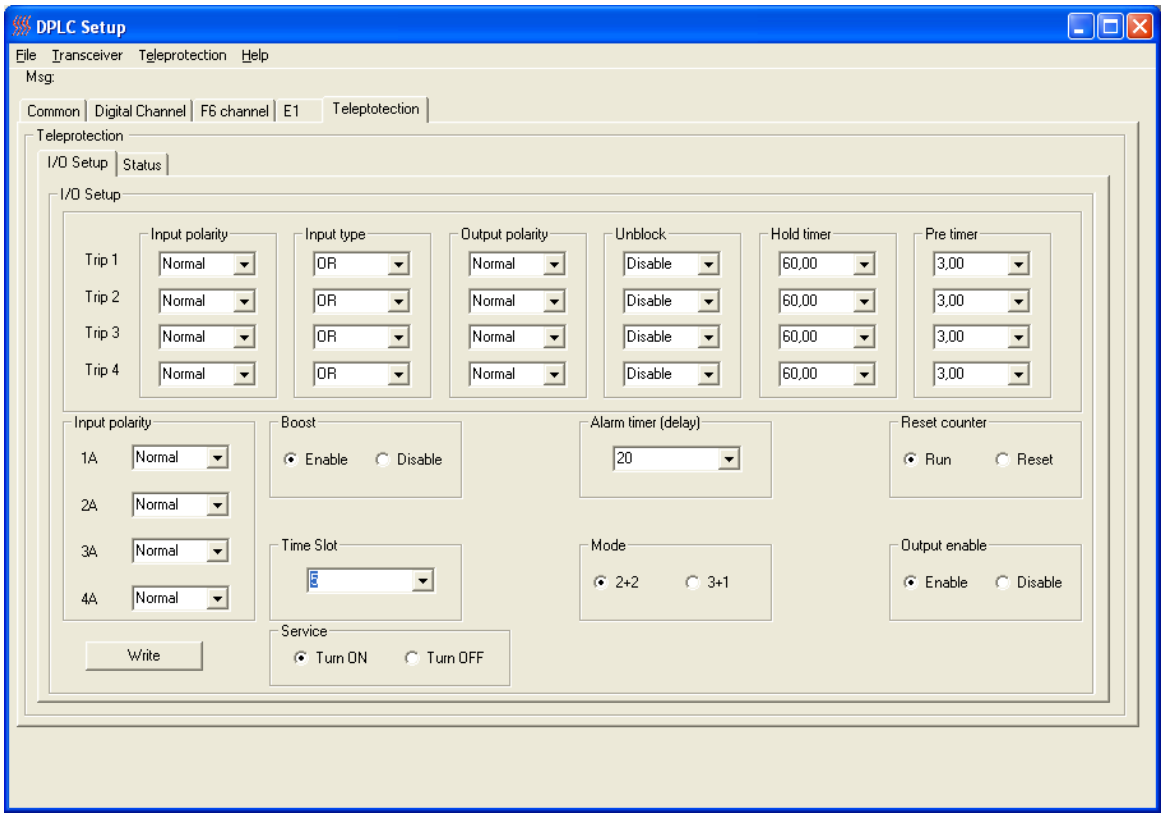


Figure 107 – Typical Digital PLC Human Machine Interface

Telephony Features

The voice delivery is performed by packetizing and compressing the telephony traffic, there are many voice compression algorithms like ACELP-CN (8K/6K with fallback), G.711 (PCM 64K), G.723.1 (Low 5.3K/High 6.3K), G.726, (ADPCM 16K/24K/32K/40K), G.729 and G.729a (8K)

The analog telephony channels: FXS, FXO and four wire E&M should be digitized by an A/D converter prior to compression and transmission.

Network Management

The DPLC creates a WAN (Wide Area Network) in a narrow band system and is able to use many of the features of a wideband network like the NMS or Network Management System. This NMS allows the remote control and configuration of all the devices in the network by a console connection over either Ethernet or traditional serial (RS-232 / RS-485).

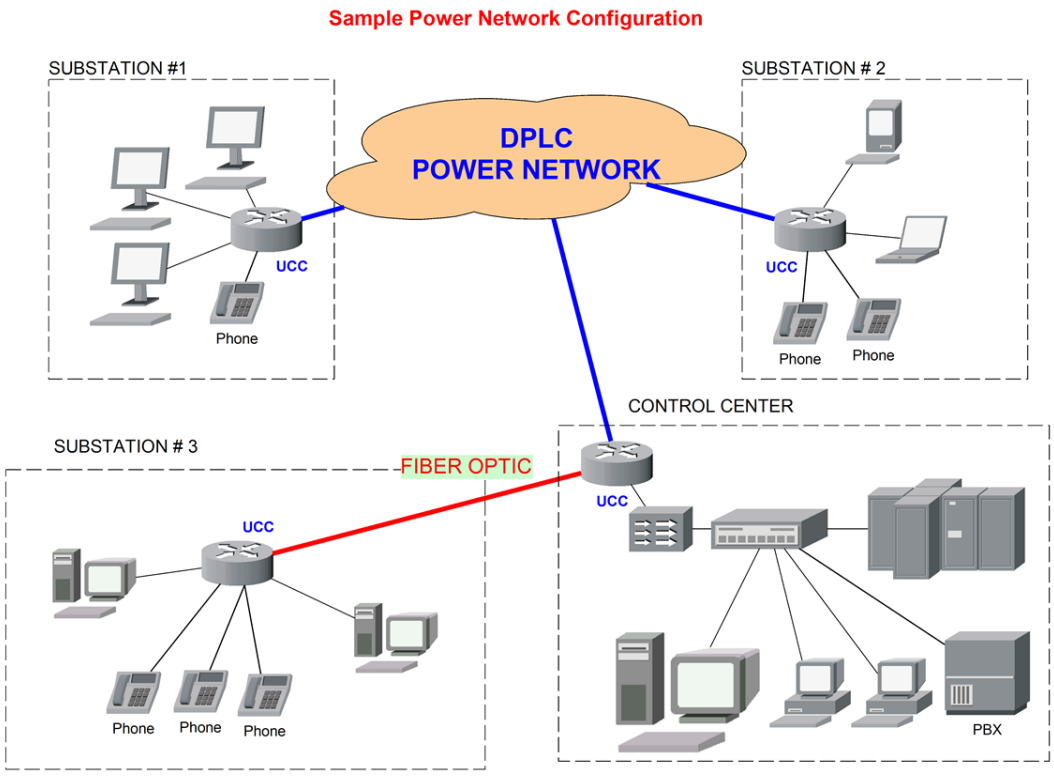


Figure 108 – PLCC Power Network Configuration

Frequency Plan

Performance Calculations

The performance of any PLCC system is determined by the Signal to Noise Ratio (SNR), the calculation of the SNR is different from a single function to a multifunction PLCC. In the case of Single Side Band (SSB) multifunction, the magnitude of the output signal will depend of the combined instantaneous signals, even not all the signals are not on continuously, a share of the total modulation must be reserved for them.

Procedure to calculate SNR

The SNR of a channel is the difference between the received signal level and the noise level, since the received level depends of the transmission side, there are three main considerations:

- Effective Transmitted Power
- Path attenuation
- Line Noise

Path Attenuation

The path attenuation is the sum of the carrier- frequency losses between the transmitter and the receiver, these losses include:

- *Line attenuation*
  The line attenuation is a function of several variables such as:
    - Frequency
    - Type of line construction
    - Line Voltage
    - Conductor size
    - Presence of ground wires
    - Methods of coupling
    - Weather conditions
    - Transpositions.
- *Coupling and shunt losses*
  The coupling loss is due to the resistive component of the line tuner and coupling capacitor, and is function of frequency, design, line impedance, bandwidth and size of coupling capacitor, for estimating purposes a value of 3dB per terminal is commonly used.
  The shunt loss consist of the losses contributed by all leakage paths to ground, it is a function of line trap impedance and varies from 1 to 3 dB per terminal, the higher value occurring at the lower values of trap impedance such as 400 ohms. To simplify calculations the coupling and shunt losses combined can be estimated in 6dB per terminal.
- *By Pass losses*
  All by-passes at the location of taplines of discontinuities in the power line must be fully trapped , by-pass losses are a combination of coupling, tuning and trap losses, estimate the combined losses at 6-12 dB per by-pass
- *Tap line losses*
  All tap lines must be fully tapped to avoid line reflections and non-linear attenuation characteristics, under this circumstances losses in tap lines can be ignored in calculating path attenuation.

Line Noise

Noise values for fair and adverse weather are provided by the curves in Figure 109

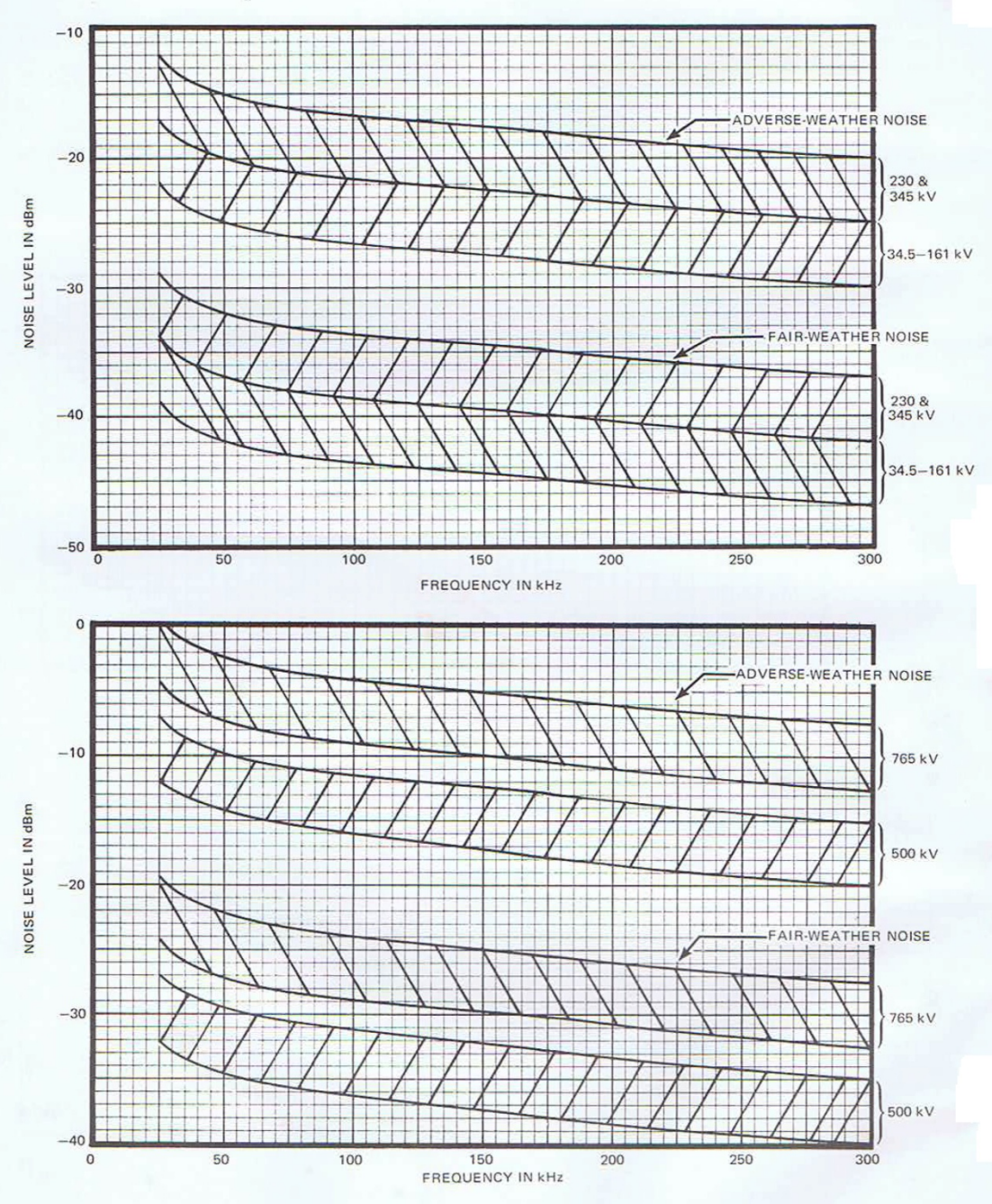


Figure 109 – Line Noise Diagrams

21. Networks Communication Topologies

There are many different types of configurations that comprise a communications network. A network is defined as an interconnected group of nodes. A network is typically comprised of nodes and line segments that link the nodes together. The different communication configurations are typically referred to as network topologies. This section addresses some of the various

network topologies in use today from the most simplistic point-to-point to the more complex ring networks.

21.1 Point-to-Point

A point-to-point system is the simplest configuration for a digital communications system. Channel(s) are available between only two pieces of equipment or nodes. Point-to-point systems are common in networks where the channel switching is provided by separate switching equipment than the communications transmission equipment or where there is a lot of traffic or information is required between two points.

21.2 Star

A star configuration is comprised of multiple point-to-point systems all with one common point. At the common point, or hub, the channels from one spoke of the star can be rerouted to another spoke of the star via digital cross connect equipment. To reduce the vulnerability of the spokes of this star configuration, redundant systems are commonly used.

21.3 Linear Drop and Insert

A drop and insert system allows multiple sites to communicate with each other along a fiber optic or other digital communications media route. In a drop and insert system, a DS0 channel can be configured between any two points or nodes. Information communicated between two non-adjacent nodes is passed directly through intervening nodes. Once a channel has been dropped, the bandwidth can be reused for other channels within the system. A single intermediate drop and insert node replaces two "back-to-back" nodes in a system configured as point-to-point systems. Drop and insert is illustrated in Figure 110, communications between Point "A" and "B" and points "B" and "C" are using the same channel. The communications between points "A" and "C" pass directly through the node at point "B".

This linear system design does not provide channel backup against fiber or equipment failures as ring topology designs do.

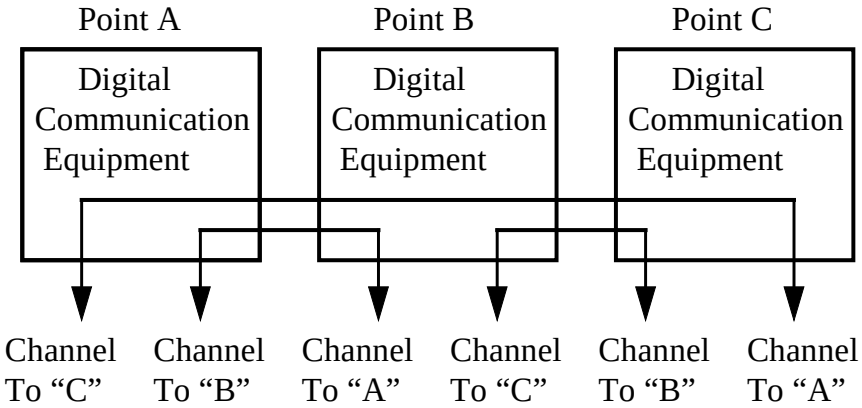


Figure 110 – Drop and Insert System

21.4 Ring

Ring is a network topology in which each node connects to exactly two other nodes, forming a circular pathway for traffic in a closed loop configuration. It is used to reference a group of nodes that are connected via Line Ports such that if a packet were passed through all nodes it would eventually return to the source. The main advantage of a ring topology is to eliminate single points of failure in a network thus providing added reliability in the event of a fiber cut or node failure. The multiplexers have the intelligence to send traffic affected by the failure via the alternate path around the ring. Maximum ring protection requires the diverse routing of fibers from any one node to its two different adjacent nodes. The only disadvantage of a ring topology is the added cost of equipment and fibers to implement. Ring topologies are typically the recommended network for any mission critical traffic.

22. Role of Telecommunications in Protection Schemes

22.1 Introduction

The use and need of communications in the electrical substation is growing and will continue to do so. Whether it is digital or analog communications, the protective relay engineer should be aware of the type of communications they may encounter and their use in relaying schemes, as discussed in this section. Also discussed are the various types of communications that are used in the setting and control of Intelligent Electronic Devices (IED) and their ability to share post-disturbance analysis either locally or remotely. IED's may use several types of communications for the different tasks the unit needs to perform its protective relaying function.

22.2 Communication assisted schemes (Phase and Directional Comparison)

In general, there should not be any problems applying traditional distance pilot schemes over a digital communications network. They are all less demanding than a Direct Transfer Trip (DTT) application with regards to security as a local conditional trip is made; the local relay has to make a decision about the system condition before it acts on a received communication signal (or, in the case of Directional Comparison Blocking (DCB), the lack-of-received signal).

Dependability, or rather any lack of dependability, will affect the pilot schemes in different ways. In case the communication signal is lost, the permissive schemes will suffer lack-of-operation while the blocking and unblocking schemes may overtrip for simultaneous external faults.

Typical SONET channel delays fall well within the range for conventional communication media. Minor asymmetric delays should not be of any concern to a conventional distance pilot scheme. The relays at the line ends are not synchronized with respect to each other and as long as channel delay falls within acceptable limits for the relay's pilot logic design, the scheme should work as intended. However, it is important to avoid any "intermediate" devices in the communication link that may add unspecified amount of delay. The use of a substation multiplexer with teleprotection interfaces is often practical.

Most distance relay pilot logic has been designed to suit conventional communication channel media and great care has been taken to coordinate the relay elements with the behavior of power line carrier or audiotone channels. There might be a need to review that this logic is not defeated by a channel that has different characteristics with respect to channel delay and channel reset times. Especially unblock, transient block or other channel related logic might be of concern.

On the other hand, a digital communication channel's advantages compared to conventional media might warrant a change of preferred pilot scheme. The traditional schemes were all designed to overcome shortcomings of the communications channel. For instance, with SONET ring topology providing channel redundancy and immunity to interference from line faults, perhaps a directional comparison unblocking (DCUB) is better suited than a directional comparison blocking scheme (DCB). DCB was designed for use with power line carrier, and the risk of losing a communication signal at the time of a fault was overcome by requiring transmission on a non-faulted line only. A digital communications channel should not be affected by any power system fault and the benefit of the DCB scheme to handle such a condition is no longer as important. DCUB provides the advantages of a permissive scheme by not requiring any blocking timer coordination while at the same time offering a trip window for the 60 ms SONET switch time, should a fault occur simultaneously with SONET channel switching.

22.3 Current Differential Schemes

22.3.1 Pilot Wire Relays

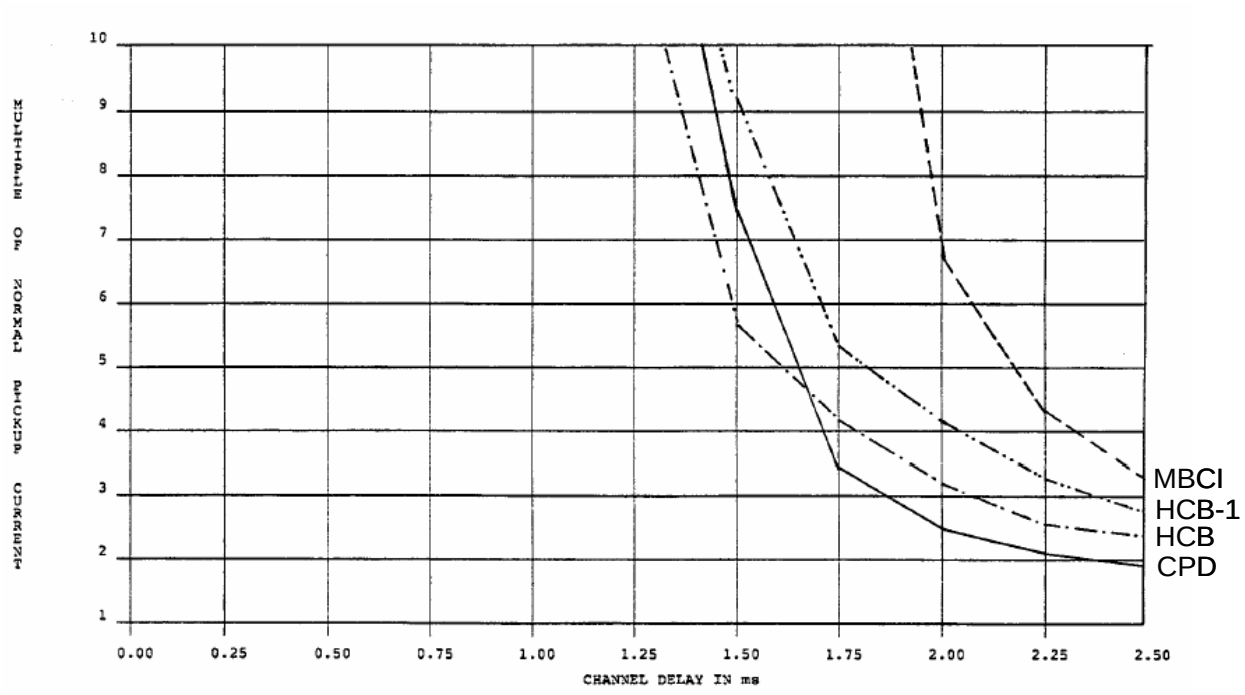


Figure 111 – Pilot wire relay operating current as a function of channel delay at external faults

Pilot wire relays were designed to use a metallic pilot wire as communication link. As the pilot wires are expensive to maintain and the lifetime of the pilot wire is shorter than the for the relay, it is tempting to substitute it with any of the digital pilot wire relay interfaces available on the market

and use a digital channel. However, as the relay was not designed to take any channel delay into account, this is the most demanding application for digital communication networks. Not only is asymmetrical delay unacceptable, but end-to-end delay must be very short; less than 1 ms is desirable and more than 2 ms is prohibitive. The effect of channel delay on some typical electromechanical relays is shown in Figure 111. The curves show the measured operating current in multiples of pickup for increasing channel delays. Above 1.25 ms channel delay, all of the types shown risk misoperation.

Typically, a SONET backbone cannot fulfill this stringent delay requirement unless care is taken to limit the number of nodes between the two line ends. A communications network with multiplexers designed for teleprotection is preferred for this application. These multiplexers are optimized with regards to through-delay and can provide very short switch-over times. Any asymmetric channel delay is eliminated by the use of a Bi-directional Line Switched Ring (BLSR) topology rather than Unidirectional Path Switched Ring (UPSR) topology.

AC Pilot Wire relaying is used for short line or cable protection. Relays at line or zone ends continuously communicate line current information. Relay tripping occurs when differences between local and remote current information exceeds the relay setting. Relay settings allow for a certain deviation due to system unbalances, communication noise, and current transformer inaccuracies.

AC Pilot Wire relaying was popularly used when dedicated twisted pair copper was available for relay end to end continuous communications. This service is no longer available from telephone companies. Consequently, protection systems had to be modified or replaced. Fiber optic current differential replacement is a popular choice.

AC pilot wire relays do not have facilities for compensating channel delay so it is important to establish that the characteristics of the interface and the channel delay are suitable. Depending upon the relaying accuracy required and the application (2 or 3 terminal), the total relay to relay delay must be less than 1.25 ms. It is also important that the Analog to Digital (A/D) has sufficient dynamic range for the application.

One method of connecting an AC Pilot Wire Relay to a digital channel bank is shown in Figure 112. Arrangement A is an AC Pilot Wire (PW) relay connected to a PW adapter that does the required A/D conversions and provides the power to drive the sensing element of the relay. Connection to the digital system is through a 56/64 kbps digital interface (DIF) module in the channel bank. The other end of the line uses Digital to Analog (D/A) and a PW adapter as well.

Figure 112 Arrangement B is another connection method to a Pilot Wire Interface Module (PWIM) that is part of the channel bank. The PWIM performs the functions of both the PW adapter and DIF in arrangement A. PWIMs are generally available only in channel banks especially designed for substation use, not in general-purpose telephone channel banks.

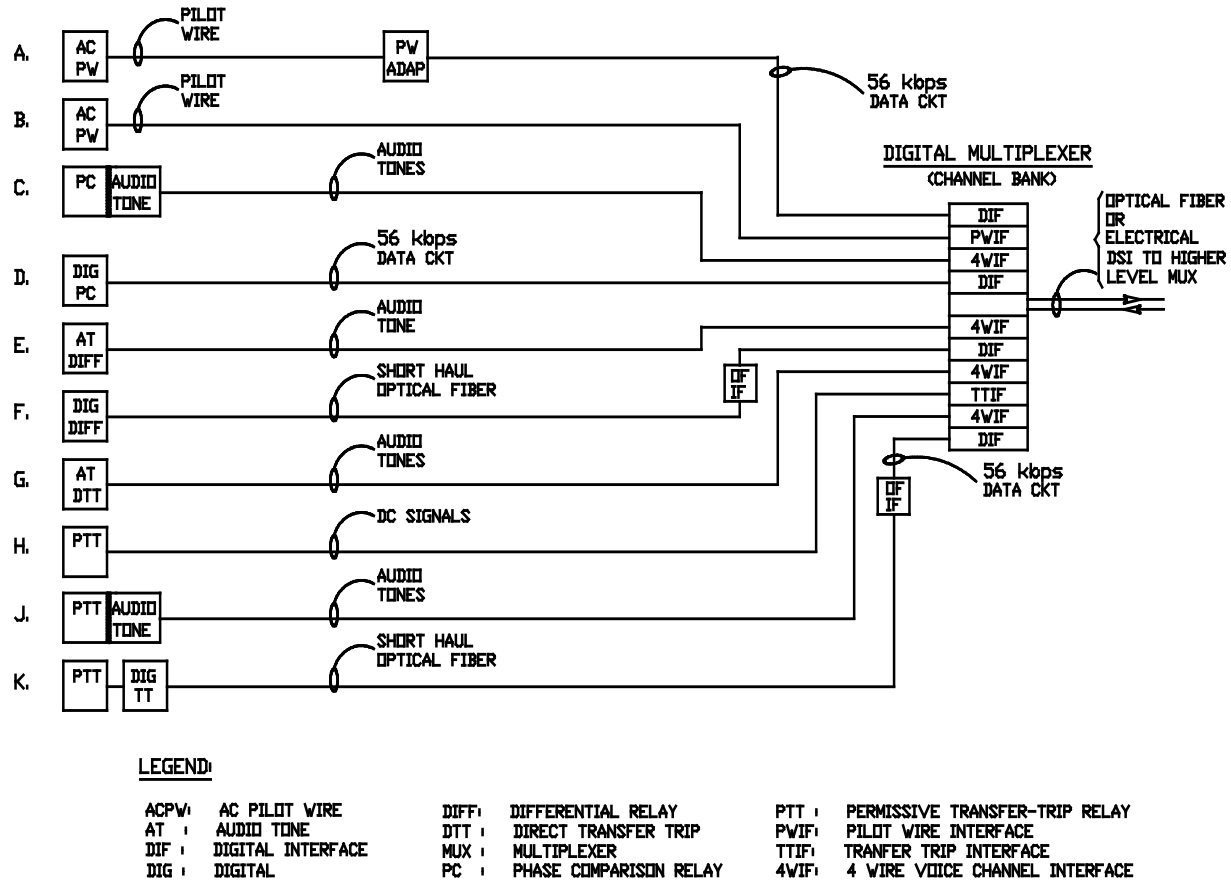


Figure 112 – Interconnecting Relays with Digital Channels

22.3.2 Digital Current Differential Relays

Newer current differential relay designs provide a variety of communication interface options. In addition to the direct fiber interface (as used for dedicated fiber point-to-point applications) interfaces for multiplexed communication systems are available. For multiplexer systems, RS-449 electrical interface or a C37.94 fiber interface is used. G.703, X.21 and V.35 interfaces might also be used for multiplex interfacing. Most relays today operate at 64 kbps over multiplexed systems even though higher data rates might be used over a direct fiber link.

The data format used to communicate current information from the relay in one line end to the relay in the remote end(s) is unique for each relay design, and sometimes unique for the actual relay firmware version. The C37.94 standard ensures that a relay can communicate though a multiplexer on optical level, but the actual data used by the relay is not standardized. Consequently, the relays need to be identical in all line ends.

The communication is synchronous, and referenced to the multiplexer clock (or to an internally generated clock source in the case of dedicated fiber). The synchronous communication provides continuous channel monitoring. Validation of received data has to be performed by the relay as the multiplexer is protocol transparent and pass exactly what is received through the system. The

multiplexer will detect transmission errors but as the SONET[1] requirements allow for a 10 ms detection time, the relay must detect invalid data during this period. In addition, it is of essence that the relay aligns received current data with local data. Any sudden change of channel delay time must be detected as the current comparison would otherwise be out-of-phase and could cause misoperation.

Current information is exchanged in a variety of ways; Fourier coefficients, phasors, current charge, or status of instantaneous current samples. Depending on what measuring method and algorithm is used, various names are given to the protection: current differential, charge comparison, phase comparison or current comparison. They all operate on the same principle though; the difference in currents as measured in all line ends of the protected line section.

Current values can be sent on a per phase basis (phase segregated) or by a combined quantity (sequence measurement). Different methods require different amount of data to be sent. Also, the frequency of sending a data frame differs between designs, from one frame per 0.2 ms to one frame per half-cycle (8 ms) and the entire 64 kbps band does not necessarily has to be used for data; "idle" time can be inserted between data frames.

Most digital current differential relay designs have the ability of measuring and compensating for channel delay. Channel delay estimation is made by ping-pong measurement. The exact method and measurement frequency vary but the principle is similar. One end sends out a special message that is echoed back from the remote end. The loop time less the "turn-around" time divided by two is then the one-way delay. Using the references in Figure 113, channel delay is calculated as:

Channel delay = $[t3 – t0 – (t2 – t1)]/2$
With asymmetric delay, i.e. $t3' – t2 \neq t1 – t0$, the calculated one way delay becomes:
Asymmetric channel delay = $[t3' - t0 – (t2 – t1)]/2$ and the error consequently is
Error = $(t3' – t3)/2$

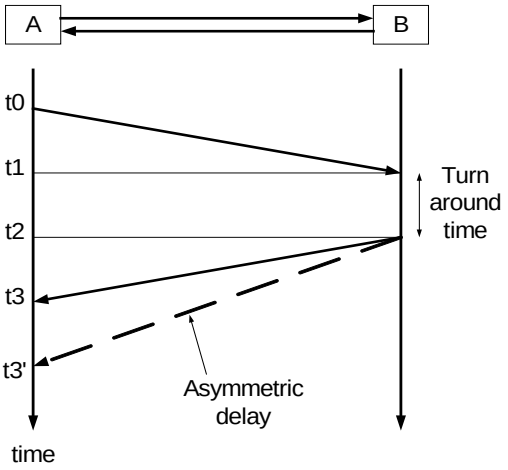


Figure 113 – Ping-pong time delay measurement

[1] For information on SONET Systems refer to Section 4 Digital Communications

Some current differential relays offer GPS clock synchronizing to eliminate the ping-pong error at asymmetrical channel delays. In these relays, a time-tag is part of the data frame so that the receiving relay can recognize that the actual one-way delay differs from the measured ping-pong delay, and compensate for it.

Channel delay measurement is used by the relays to align received current data from the remote end with memorized local current so that current is compared at the same instant in time. This is illustrated in Figure 114.

The calculated one way delay is used by the relay to align the received current information with local, stored current measurement that was made one channel time delay period previously. As long as measured channel delay equals actual channel delay, there is no error (except small inherent errors due to the finite sampling frequency, timer resolution, accuracy, etc.).

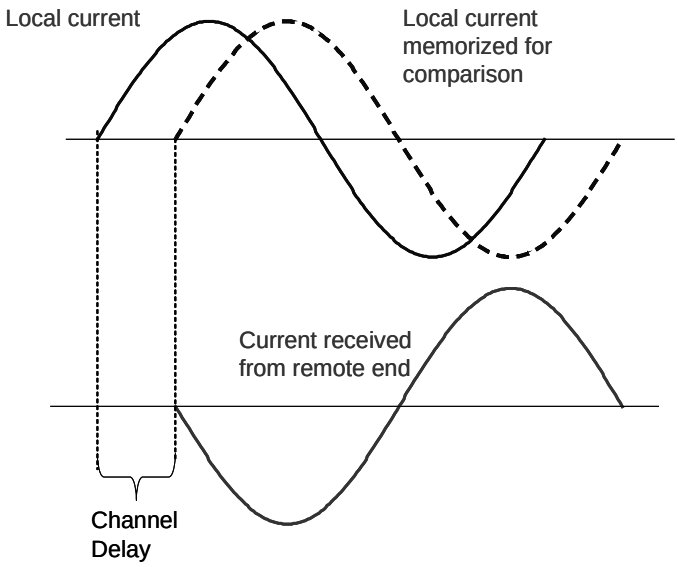


Figure 114 – Channel delay compensation

When the actual delay deviates from measured delay, the error introduced to the relay will look like a differential current. As the currents in the two line ends are not compared at the same instant in time, a false difference will be produced. Different relay designs deal with this condition in different ways. In general, measuring principles based on the phase relationship between the currents in the line ends are more tolerant to channel delay errors than measuring principles based on amplitude comparison.

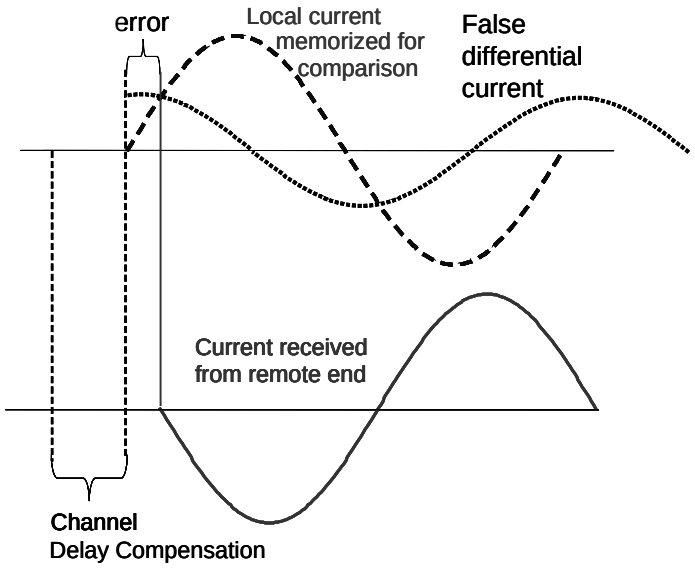


Figure 115 – False differential current due to channel delay error

While GPS synchronizing bears the promise of an efficient method to handle asymmetrical delay, it may not be required for all current differential relays used in multiplexed communication networks. The possibility of asymmetric delay may be eliminated by proper network design so that both transmit and receive path are switched at the same time, as described in Appendix A. In addition, some current differential relay measuring principles can handle up to 4 ms delay error without affecting performance. Note that 4 ms one-way error equals 8 ms difference between transmit and receive path as the error is divided by 2 in the ping-pong measurement. Few, if any, existing SONET networks would manifest such a large difference.

22.3.3 Phase Comparison and Current Differential

Phase comparison and current differential relaying systems send current phase information and current phase and magnitude information respectively making these schemes highly dependent upon the communications channels for proper definite zone operation.

Early forms of phase comparison systems utilized single frequency half duplex ON-OFF power line carrier (PLC) for communicating information between relays. The ON carrier state was used to block tripping and the OFF carrier state was used to allow tripping. Each relay used the same one half cycle of power line current information to determine a trip or block condition. Later forms of phase comparison systems utilized two or three state frequency shift modulated (FSK) channel equipment on power line carrier or audio tone equipment.

One of the critical specifications of the channel in a phase comparison and current differential application is the absolute delay of the channel. Since the phase of the power frequency current is being compared to the phase of the current at the other end of the line, any time delay added to the remote signal is a phase error in the comparison process. For example, a channel delay of 1 ms creates a phase error of 21.6 degrees and that will have a significant impact on relay reliability. In a current differential system, a 1 ms delay creates a false differential current equal to about 37.5%

of the through current. For this reason, channel delay compensation is usually added to each relay before phase information is compared.

Analog phase comparison and current differential relays generally have only manually adjustable time delay compensation. Accordingly, variable time delay media, such as those from path switching, are not recommended if the changes would exceed the tolerance of the relay.

Microprocessor-based phase comparison or current differential relays can have automatic time delay compensation, based on continuous delay measurement. This makes them much more tolerant of path switching than earlier types. However, automatic compensation schemes that assume equal channel delays in each direction may be fooled by some digital network arrangements, e.g. SONET rings in which all traffic flows around the ring in one direction.

Phase comparison or current differential relays using audio tones can communicate over digital systems using 4-wire voice frequency interfaces modules (4WIF), as shown in Figure 112 Arrangements C and E respectively. This method does not change the system operation in any way and the same relay system equipment can be used without replacement of any parts. Utilizing a digital communications system in this manner does not benefit the security and dependability except to the extent that the digital channel may be using a better medium, i.e., fiber optics. The relay system reliability may increase because of the increased reliability of the fiber optics.

Microprocessor-based phase comparison and current differential relays can utilize a 56 or 64 kbps direct digital interface (DIF) with the digital communications equipment, as shown in Figure 112 Arrangements D and F respectively. Arrangement F shows an optical fiber and optical fiber interface (OFIF) option that may be useful for lengthy relay to communications equipment runs. This option will reduce interference and ground potential rise problems. The digital channel also has additional capacity over the analog channel that may be used to communicate additional information, such as relay channel performance data.

22.3.4 Directional Comparison

Directional comparison schemes were developed to provide fast tripping for faults anywhere on the transmission line. These schemes combine the directional and distance characteristics of an impedance relay with various pilot communication channels. Impedance relays typically determine direction by comparing the phase angles of various operating voltages and currents either measured or computed by the relay. Typical directional or polarization quantities include the faulted phase voltages and currents, quadrature voltage and fault current, and positive, negative, and zero sequence voltages and currents. Most relays today will use pre-fault voltage to ensure the integrity of the fault direction.

Pilot or communications channels for directional comparison can operate over a wide range of choices such as audio tone, power line carrier (PLC), microwave, and optical fiber. Channel type will either be on/off or frequency shift keying (FSK) carrier depending on the type of scheme implemented. Channel delay is not as critical as for current comparison schemes.

General coordination rules must be observed when the different channel types are integrated with the various distance elements in a number of different directional comparison schemes such as the dependable direction comparison blocking (DCB) to the secure directional comparison unblocking (DCUB) schemes.

Digital communications can be added to audio tone directional comparison schemes by adding A/D and D/A converters, as shown in Figure 112 Arrangement J. Digital relaying may offer an improved media advantage at the expense of system reliability due to the extra equipment. This has not been a popular approach since directional comparison has been purposefully designed to have less communications dependence than phase comparison or current differential.

22.4 Transfer Trip Schemes

Transfer Trip Schemes use communications to provide trip information to a remote relay. The remote relay then may trip as in the Direct Transfer trip (DTT) schemes or use the additional information local before tripping as in the permissive schemes, i.e., Permissive Overreaching Transfer Trip (POTT) and Permissive Underreach Transfer Trip (PUTT). These schemes typically use frequency shift audio tones over leased telephone, microwave, and fiber optics.

Figure 112 Arrangement G shows a conventional audio-tone direct transfer trip connected to the digital communication system through a 4-wire voice channel interface module.

Figure 112 Arrangements H, J, and K show permissive transfer trip relaying systems. In Arrangement H the relay signaling contacts and received signal indication are connected to the digital system by a Transfer-trip Interface (TTIF) module. These modules are generally available for channel banks intended for substation use, but not in channel banks for general-purpose application.

Figure 112 Arrangement J connects the relay by means of an audio tone transfer-trip equipment connected to a 4-wire interface module (4WIF) in the channel bank.

In Figure 112 Arrangement K, the relay is connected through digital transfer-trip equipment that has a short-haul optical fiber output. As in Arrangement F, an Optical Fiber Interface (OFIF) is then used near or in the channel bank to convert the fiber to a 56 or 64kbps digital signal.

22.4.1 Permissive Overreaching Transfer Trip (POTT) Scheme

This scheme requires a remote trip signal to permit local relay tripping. This is a secure relay scheme since both line end relays input are required before a trip decision is made. The dependability is impacted by the selection of the communications media. Since communications are required during the fault, a separate communications medium and path are desirable.

The traditional POTT scheme is similar to the DCUB scheme except that a signal is sent only when an internal fault is detected. This was a shortcoming when applied on conventional channels as the lack of a guard signal also meant lack of continuous channel status monitoring. However,

when applied over a digital channel, the channel is inherently monitored by the SONET synchronous communication and is never “idle”.

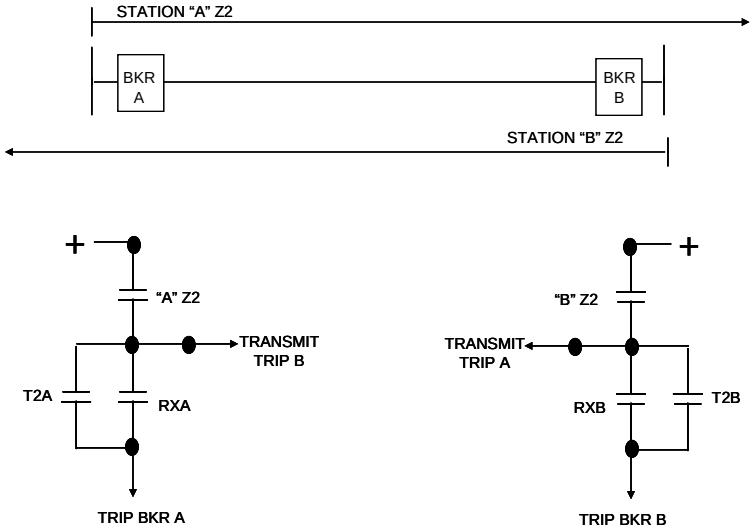


Figure 116 – Permissive Overreach Transfer Trip (POTT)

22.4.2 Permissive Underreaching Transfer Trip (PUTT) Scheme

This scheme is similar to the overreaching scheme, although the relays are set for direction and to underreach the line ends.

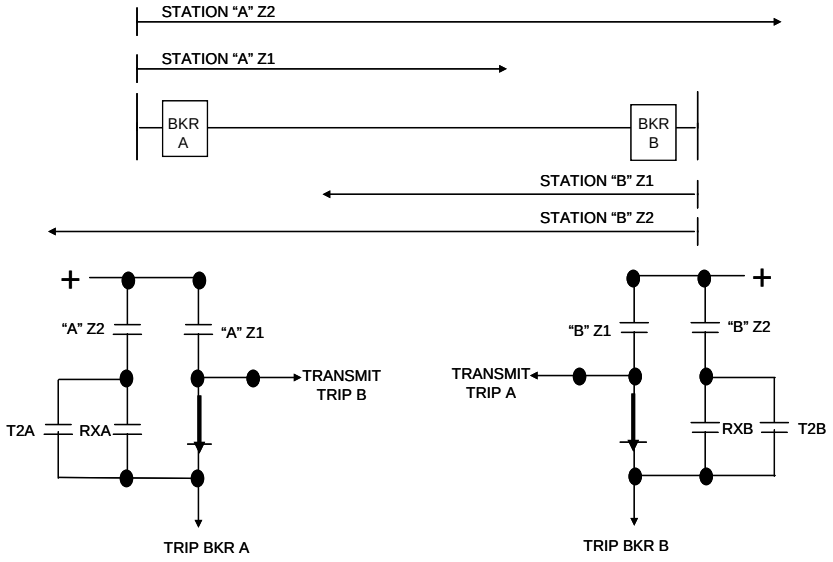


Figure 117 – Permissive Underreach Transfer Trip (PUTT)

The PUTT scheme is similar to POTT but sends a permissive trip signal for faults on the line only. The receiving end is then allowed to trip provided that its forward overreaching zone has also detected the fault. This provides higher security than POTT as no external faults will cause a

permissive signal to be sent. The purpose of the scheme is to speed-up tripping for end zone faults that is outside zone 1 reach from one line end. The scheme was originally made for switched distance relays that only had one zone element, zone 1. On receipt of a permissive signal, the relay was allowed to switch to the longer zone 2 reach and make an immediate trip from this zone that covered the far line end.

The security provided by the PUTT scheme may be advantageous on parallel line applications as transient block logic is not required. It should be confirmed however that the two zone 1 elements cover the center of the line for all possible faults, considering that the reach might have been reduced to mutual coupling effects.

22.4.3 Directional Comparison Blocking (DCB)

DCB is operating on the principle to use a communication channel to block tripping for external faults while no signal transfer is required for internal faults. This scheme is typically applied with ON/OFF Power Line Carrier and has the advantage of not being affected by a possible loss-of-signal for faults internal to the line. Power Line Carrier transmission uses the power line itself and there is a risk of a transmitted signal being shorted or interrupted by a fault on the same conductor or line.

The DCB scheme with non-directional carrier start makes channel time coordination and distance element coordination easy while at the same time, tripping times are minimized for internal faults. The principle is based on the fact that non-directional element's operating time plus ON/OFF channel delay (2 – 4 ms) is shorter than the 21P (forward distance zone) operating time.

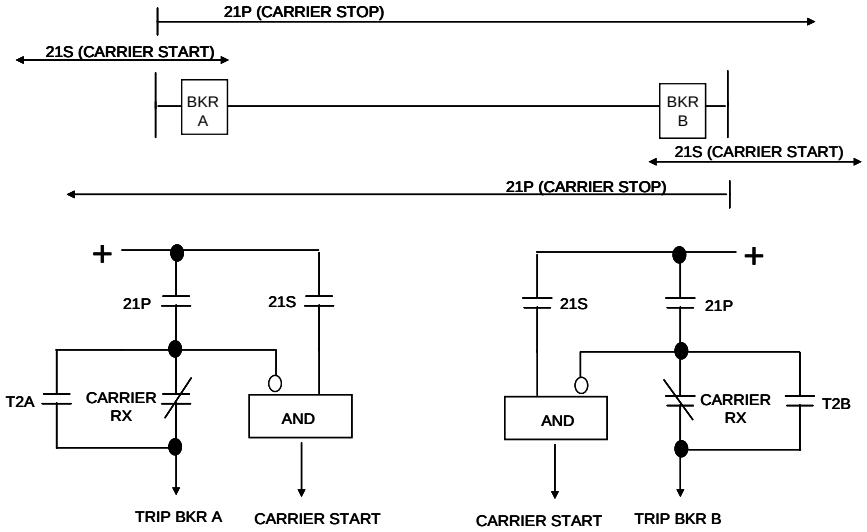


Figure 118 – Directional Comparison Blocking with non-directional carrier start

The distance relay needs only one directional pilot element, in the tripping direction. Another, non-directional, 21S, element is used to start carrier for all faults, sending a blocking signal to the remote end. In case the forward element operates, the carrier is stopped and the remote end is allowed to trip based on its forward operation and resetting of the received carrier blocking signal.

When applying a DCB scheme over a digital channel where longer channel delays than what is typical for an ON/OFF PLC can be expected, a channel coordination timer might be required.

A variation of the basic DCB scheme uses a reverse directional element to start and maintain a carrier block signal. The principle is otherwise similar to the previous scheme, except that a channel coordination timer is required, and a reverse distance zone is required. For a digital channel, the coordination timer should be adjusted to accommodate maximum expected channel delay.

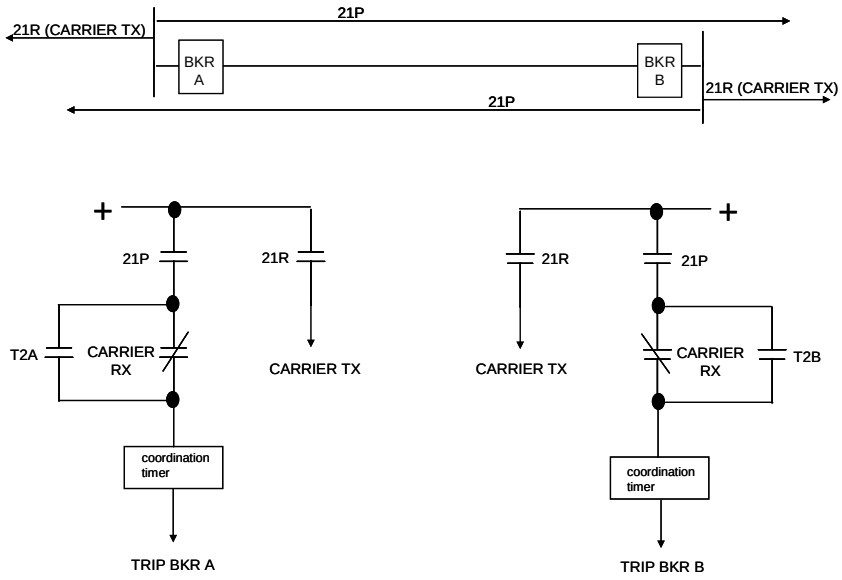


Figure 119 – Directional Comparison Blocking with directional carrier TX

22.4.4 Directional Comparison Unblocking (DCUB)

The DCUB scheme was designed for Frequency Shift Power Line Carrier. The FSK carrier sends a continuous blocking signal. When a forward distance element detects a fault, the transmitted carrier frequency is shifted to a trip signal. The scheme is therefore a permissive principle; forward operation AND received permission are required for a trip. To accommodate for a risk of losing the carrier signal in the fault on the line, an unblock trip window is provided. If the receiver does not detect any signal, neither block frequency (GUARD), nor trip frequency, the relay is allowed to trip from its forward distance element for a period of 150 ms following loss-of-signal.

For a digital channel, the risk of losing the signal should be minimal. However, the DCUB scheme's ability of overriding a 60 ms SONET interruption makes it an attractive candidate for use on digital communication networks. As in other permissive schemes, channel delay is directly added to protection trip times. Excessive channel delays should affect only the operating time of the protection system, but might need to be considered for any built-in channel coordination logic, such as transient block logic for parallel line applications.

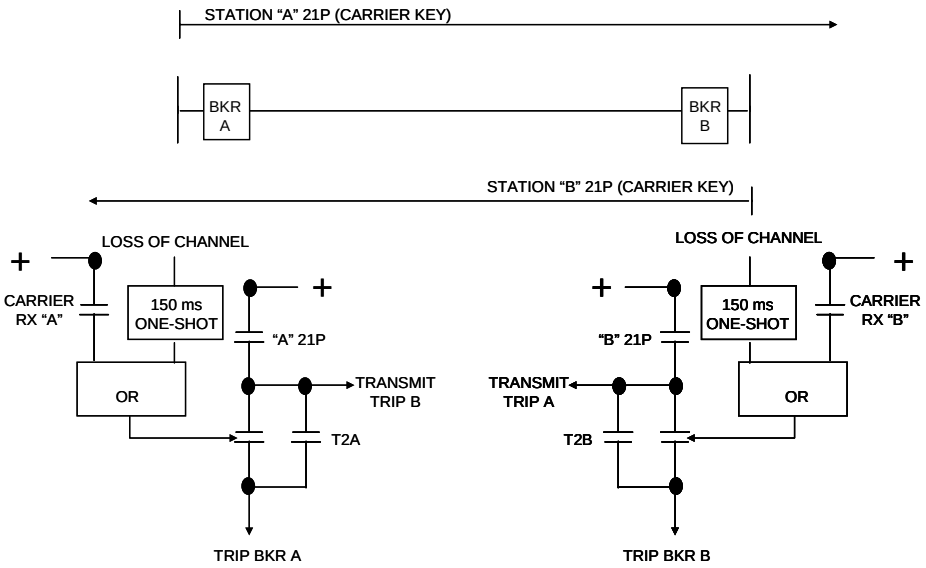


Figure 120 – Directional Comparison Unblocking

22.4.5 Direct Transfer Trip (DTT) Scheme.

This scheme does not need local information for a trip decision, therefore the reliability of the communications circuit is directly related to the systems reliability.

Transfer trip is a relay protection scheme that uses communications between two or more sites separated by distance. The primary purpose of transfer trip is to provide a method for high speed clearing of all terminals associated with a high voltage power line. This is accomplished by using a communication path between the terminals associated with a specific line. There is several type of communication methods by which the transfer trip signal can get from one end of the line to the other. Some of the most commonly used methods for transfer trip are: microwave radio, UHF/VHF radio, fiber optic cable, power line carrier, and pilot wire. These different transfer trip methods are described in other portions of this paper.

When a fault occurs on a power line (e.g. a tree blows into the line) the protective relays at each end of the line will detect the fault. When the fault is located close to one end of the line, the protective relays at that end (local end) will initiate an instantaneous trip to the local power circuit breaker – opening the breaker within 3 to 5 cycles. However, the protective relays at the opposite end of the line (remote end) will have a time delay – because of relay coordination concerns – before initiating the trip signal to its power circuit breaker. If there is no transfer trip associated with the line protection scheme there will be a delayed "clearing" at the remote end of the line of approx 20 to 30 cycles. This delay keeps the fault on the line for an addition 17 or 27 cycles and can result in system stability concerns or damage to high voltage equipment.

When transfer trip is incorporated into a line protection scheme, the trip signal is sent to the remote terminal at the same time the trip signal is sent to the local power circuit breaker. This will result in the remote circuit breaker being tripped open at approximately the same time as the local breaker – the time required for a transfer trip signal to get from the local end of the line to the

remote end and initiate a trip to the remote breaker is generally less than three or four msec. This protection scheme results in the fault being isolated at both ends of the line in three to five cycles, reducing the adverse effects on system stability and stress to high voltage equipment.

Direct Transfer Trip (DTT) is used whenever a trip signal needs to be transported to a remote location. Typical applications are transformer protection and breaker failure protection. DTT is also sometimes used together with Directional Comparison Blocking (DCB) schemes as the DCB will not automatically trip a weak end without sufficient fault current to operate the line relay at this end.

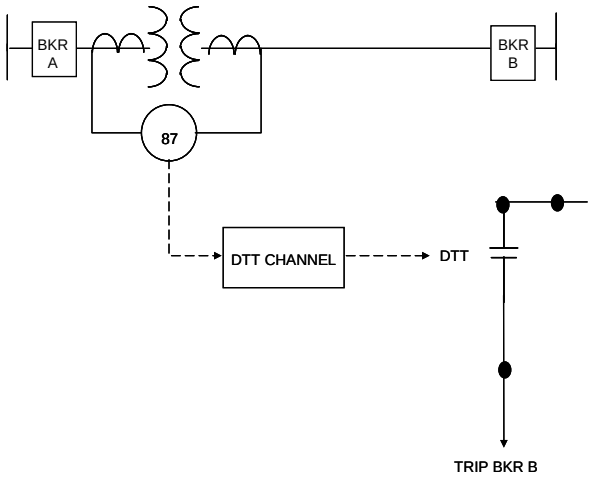


Figure 121 – Direct Transfer Trip scheme

The DTT command is sent in one direction only, possibly to more than one remote location. In a traditional DTT scheme, the receiving end does not make any comparison with local conditions and gives a direct trip command to the breaker. Any false trip command over the communication link that is not detected by data error checking in the receiver will guarantee a false trip of the breaker. Consequently, the security requirements for DTT communications are very high with lesser demands on speed and dependability.

When used over conventional communication channels, security is generally increased by adding time delay. It has not yet been determined if the use of digital communication networks would allow shorter time delay without compromising security. SONET requirements do not specify security but SONET system design provides advanced error check capability. However, it should be remembered that SONET requirements call for <10 ms error detection time and during this time period, erroneous data may be delivered to the receiving device. Therefore, the receiving equipment must be able to make its own error checking to detect and discard the faulty data.

Digital channel delay times should not be an issue for DTT. The digital communications network end-to-end delay is shorter, or as short, as for a conventional communication media. Any asymmetrical delay is of no concern as there is no time coordination required between the two ends of the communication link.

22.4.6 Concluding Engineering Considerations

In summary, the engineering of a successful system requires that the performance of the communications systems meet the requirements of the relaying equipment with particular attention to the following:

22.4.6.1 Delay

Whereas analog systems were typically constant paths, digital systems can have unpredictable path changes, especially with leased facilities, and data interfaces (modems, 56/64 kbps).

22.4.6.2 Dependability

The likelihood of failures in both the equipment and media should be assessed considering backup facility operation. This should be compared with the operational requirements.

It is important to understand that the real probability of inadvertent data crosses and loopbacks in digital systems requires that dependable channels must include unique addressing mechanisms.

22.4.6.3 Security

This term is used to describe the freedom from unwanted operations (e.g. false trips). An assessment of the likelihood of data corruption, such as error bursts and data crosses, with the susceptibility of the teleprotection receivers must be made.

22.4.6.4 Electromagnetic Susceptibility

Equipment should meet the IEEE surge withstand capability (SWC) standard. Since each application is location dependent, equipment proximity to high voltage and neutral conductors, switching power sources, and other stationary and mobile communications equipment should be examined carefully. This is becoming increasing difficult with new GHz frequency bandwidth allocations.

23. Substation Automation and SCADA

23.1 Overview of EMS/SCADA Communications

Electrical power system SCADA and the Load Dispatch Centre’s Energy Management platform are some of the most important and well established applications of Ethernet communications in the operational environment of the Electrical Power Utility.

EMS/SCADA protocols have been subject of dedicated technical documents and their brief coverage here is only for the purpose of better understanding of the context of use, and the related constraints of the underlying Ethernet infrastructure.

Several levels of local and wide area Ethernet connections can be distinguished across the network, as presented in Figure 122, with different inter-networking strategies related to security and data exchange constraints. It should be noted that depending upon the adopted architectures and technologies, some of the described levels can be merged together.

- **Substation RTU to the SCADA Platform** – A first level that is developing quite fast is related to TCP/IP based connection of the substation RTU to the SCADA platform in the control center. The RTU may be natively operating with a TCP/IP protocol stack and interfaced to the network through an Ethernet connection (IEC60870-5-104) or through a Serial Server encapsulating Serial data from legacy RTU as further discussed in *Section 18.4 Serial Server – Serial to TCP Protocol Converter*.
- **Front-end LAN** – This level allows the connection of all substation RTU communication channels to communication front-end servers. It is generally a local network confined to the control center but can also be distributed among a number of SCADA access points, particularly when a back-up control center exists in the network.
- **SCADA LAN** – This level allows the Energy Management Systems (EMS) servers to access to the different substations through the communication front-end machines and the dedicated workstations to access the servers. It is generally localized in the control center but can also be extended to a back-up control center or to a remote workstation across the network.
- **Inter-Control Center Interconnections** – Individual Servers in the control center or the platform as a whole require direct high speed connections to back-up facilities (e.g. for database synchronization), to other control centers (e.g. for dispatch coordination), or to other platforms (e.g. for market management applications). These Ethernet based links are generally used to carry traffic through the Inter-Control Center Protocol (ICCP) standardized as IEC 60870-6 and Telecontrol Application Service Element (TASE-2) protocol. TASE-2 is used internationally for communications between control centers and often for communications between SCADA systems and other engineering systems within control centers.
- **Control Center Office LAN** – This level concerns non-real-time traffic such as the access of engineering workstations to synthetic data generated or processed in the EMS/SCADA platform. It carries normal office environment data exchange protocols.
- **Public Zone (DMZ)** – This level concerns the processed data that is made available to the outside world by the Control center through web-service and must therefore be well separated from the critical operational world. The data traffic across this network is exchanged using web-oriented protocols.

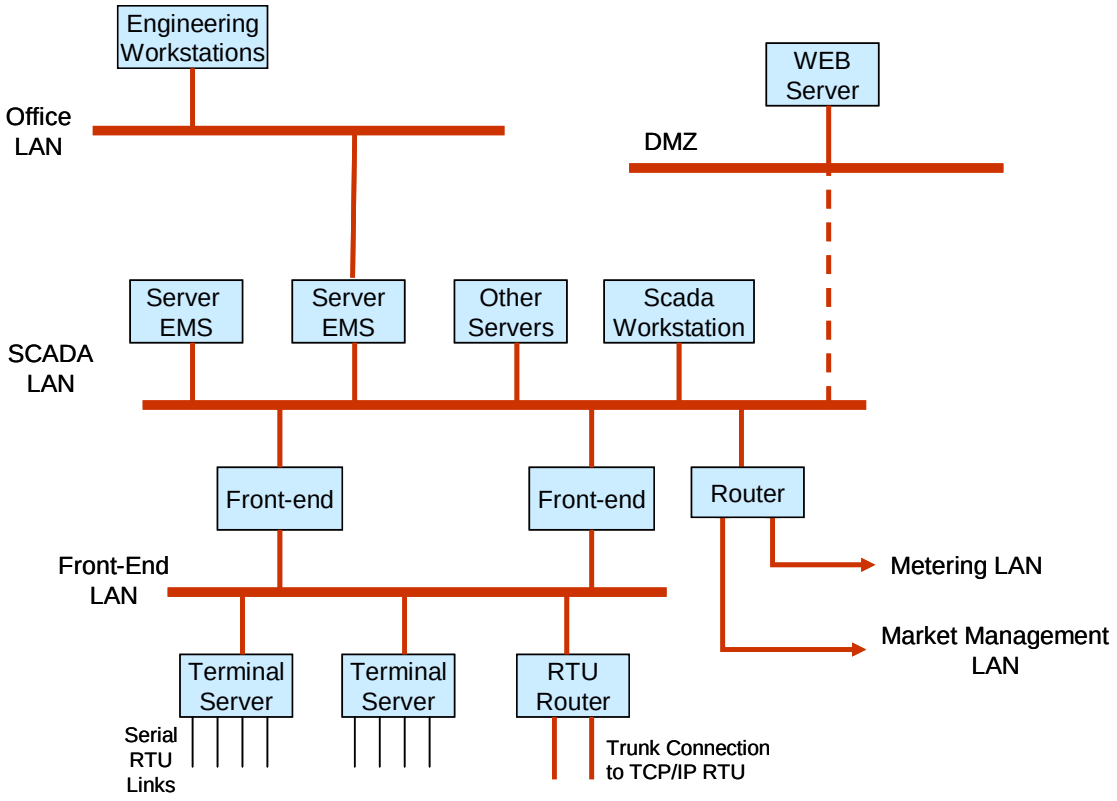


Figure 122 – Control Center Platform Communications

23.2 SCADA RTU to Control Center Communications

Still today, the widest employed communication mode for the substation RTU remains the Asynchronous Serial link through an RS-232 interface. The communication protocol associated to this mode has been standardized as IEC 60870-5-101 (IEC101), although many other protocols are still in use in legacy systems. It is suitable for multiple configurations such as point-to-point, star, multi-drop, etc.

The great advantage of Serial link SCADA is its conceptual simplicity when associated to a circuit-based communication system: RTUs have independent circuits and can be backed-up by another circuit with fully separate routing across the network. The major drawback to serial communication for SCADA is indeed its lack of flexibility and the large quantity of independent serial circuits that must be terminated and connected to a Front-end in the control center. This implicates hundreds of RS-232 interface points, associated interface hardware and a great amount of cabling and connectors. Moreover, any change in the organization of the SCADA system, such as the transfer of the control center to a new geographical location or the implementation of a Back-up control center, shall require tremendous change and a great number of ancillary equipment such as fall-back switches, interface splitters, etc., reducing considerably the overall reliability of the system.

In the late 80s, packet switching protocols were applied to SCADA services essentially to save leased bandwidth in the aggregate links to the control center and also to enhance the flexibility of

the system. RTU information was assembled into ITU-T X25 packets at designated switching nodes using a PAD (Packet Assembler Disassembler) and routed to the Control platform through Virtual Circuits established across multiple packet switches. Similar implementations were made in early 90s using Frame Relay systems.

The principle of replacing end-to-end serial SCADA circuits by packet communication received considerable support with the advent of IP networking leading to TCP/IP based SCADA protocol IEC 60870-5-104, generally called IEC104. The high capacity optical network with modern SDH transmission provides the adequate infrastructure to deploy the required wide area Ethernet connections.

The IEC104 protocol was developed as an extension of IEC101, adapted for use in a TCP/IP environment through an Ethernet LAN interface at 10 or 100Mbps, although the bandwidth allocated to each RTU communications remains often around 10kbps.

The application layer remaining largely unchanged, the amount of process-oriented data to be exchanged does not significantly increase through the use of IEC 104, even if new applications such as RTU-management and SW-updates may punctually consume more bandwidth than in IEC101.

Moving from Serial link to TCP/IP SCADA communications raises a number of issues that must be taken into account:

- **Latency** – RTU communication is time sensitive and high latency can degrade the overall performance of the SCADA system or even render the protocol completely inoperable through the time-out of the communication servers. Latency problems due to switching and routing infrastructure may be avoided through an appropriate design. It should be noted that the “real-time” requirements of RTU-cycles are generally in the range of seconds, as compared to order of magnitude smaller transmission times across a thoroughly designed SCADA Ethernet/IP infrastructure. The main issue here is therefore the number of intermediate nodes in the routing of SCADA information as well as the time for any encapsulation and concatenation.
- **Path Redundancy and Resilience** – SCADA RTU communications generally require independent normal and back-up communication routes. In an Ethernet/IP network environment, the problem of resilience is generally overcome through inherent IP routing mechanisms (e.g. OSPF routing), and/or through the protection mechanisms of the underlying SDH network (e.g. SDH ring protection). Adequate planning of OSPF-routing areas, which helps avoid unwanted management traffic and increased re-routing times, and appropriate predefined alternative routes in the SDH infrastructure provide for high reliability and limited transmission times. Duplicate RTU routing independent of network resilience mechanisms is indeed possible, but should be performed keeping in mind the independence of normal and back-up routes dictates there be no common points of failure.
- **Restoration time** – Restoration times in case of failure may be higher than with serial transmission, depending on the selected protection schemes. The original restoration mechanism of Ethernet, the Spanning Tree Protocol (STP) has a convergence time which depends upon the complexity of the Ethernet mesh and which may be too long for a

SCADA system. More elaborate options such as Rapid Spanning Tree (RSTP) reduce this time, and as a general rule, the restoration time must be taken into consideration in the design of the Scada Ethernet infrastructure. This subject is further discussed in the relevant section of the document.

- **Multi-service integration** – IP networking is generally considered as a multi-service network technology. However, it should be noted that migrating SCADA to TC/IP does not necessarily allow the integration of additional services (office communications or IP voice services) within the same IP network. To provide the required QoS for a TCP/IP SCADA system, it is recommended to implement specific VLANs with dedicated bandwidth-allocation.

The use of TCP/IP in SCADA RTU communications offers some advantages when compared with serial communications:

- Ethernet simplifies the communications network architecture. Only a few Ethernet interfaces are required at the control center to access multiple remote RTUs or gateways, as compared with numerous modem-connections at front-end computer.
- Only few (redundant) LAN-connections are needed and the RTUs or gateways are addressed via their IP-address.

Moreover, the use of TCP/IP enhances considerably the flexibility of the SCADA communication system, facilitating the relocation of an RTU or a complete Front-end.

The migration process for a large installed base from existing serial communications to TCP/IP is a major concern in many SCADA systems. This process may be extended over many years, and does not necessarily cover at the same time the replacement of the RTU, its communication interface, the telecommunication infrastructure and the control center Front-end facilities. Moreover, new RTUs dispersed across the network may be TCP/IP while the existing may remain serial linked, up to their programmed end-of-life.

Different implementation strategies using Serial Servers across the network allow a mixture of serial and TCP/IP SCADA in the same network; this provides a gradual migration scheme as addressed in detail in *Section 18 Serial to Ethernet Conversion*.

23.3 Inter-Control Center Communications

Communications between control centers is necessary for connection to back-up facilities (e.g. for database synchronization), to other control centers (e.g. for dispatch coordination), or to other platforms (e.g. for market management applications). These interconnections have been assured through the Inter-Control Centre Protocol (ICCP) standardized as IEC 60870-6 and Telecontrol Application Service Element (TASE-2) protocol, although earlier protocols such as ELCOM-90 and its multiple adaptations may still be in use in certain older systems.

The primary purpose of Telecontrol Application Service Element (TASE-2) is to transfer data between control systems and to initiate control actions. Data is represented by object instances. The object models and services that are specific to control center operation and applications are

found in the IEC 870-6-503. Additional models and services may be defined according to particular requirements.

ICCP uses an underlying transport-service, normally TCP/IP over Ethernet. The required bandwidth for an ICCP link is generally around 2Mbps (E1) provisioned over an SDH network, although lower capacity links (64-128 kbps or even lower) have been in use in implementations where no fiber and SDH capacity is available.

The time constraint for an ICCP connection is of the order of hundreds of milliseconds, which rarely constitutes a constraint in an Ethernet/IP infrastructure over a digital communication network.

Security is the fundamental issue in implementing ICCP connections. An inadequately protected ICCP connection may form an open door to the control of the nation-wide energy network. Although an in-depth discussion of IT-security is not within the scope of this document, few important standards and their relationship are mentioned in the following paragraph.

23.4 SCADA System Security

Even if Security is a topic treated in dedicated technical documents [14], it is useful here to make a particular note concerning SCADA system security.

The IEC TC_57 / WG15 has undertaken the development of security standards for various communication protocols such as IEC 60870-5, its derivative DNP, IEC 60870-6 (ICCP), and IEC 61850. These security standards must meet different security objectives for the different protocols, which vary depending upon how they are used. Some of the security standards can be used across a few of the protocols, while others are very specific to a particular profile. The different security objectives include authentication of entities through digital signatures, ensuring only authorized access, prevention of eavesdropping, prevention of playback and spoofing, and some degree of intrusion detection. For some profiles, all of these objectives are important; for others, only some are feasible given the computation constraints of certain field devices, the media speed constraints, the rapid response requirements for protective relaying, and the need to allow both secure and non-secured devices on the same network.

This work is published by the IEC as IEC 62351, Parts 3-6, titled:

- **IEC 62351-3: Data and Communication Security – Profiles Including TCP/IP** (these security standards cover those profiles used by ICCP, IEC 60870-5 Part 104, DNP 3.0 over TCP/IP, and IEC 61850 over TCP/IP)
- **IEC 62351-4: Data and Communication Security – Profiles Including MMS** (these security standards cover those profiles used by ICCP and IEC 61850)
- **IEC 62351-5: Data and Communication Security – Security for IEC 60870-5 and Derivatives (i.e. DNP 3.0)** (these security standards cover both serial and networked profiles used by IEC 60870-5 and DNP)

- **IEC 62351-6: Data and Communication Security – Security for IEC 61850 Peer-to-Peer Profiles** (these security standards cover those profiles in IEC 61850 that are not based on TCP/IP – GOOSE, GSSE, and SMV)

The interrelationship of these security standards and the protocols are illustrated in Figure 123.

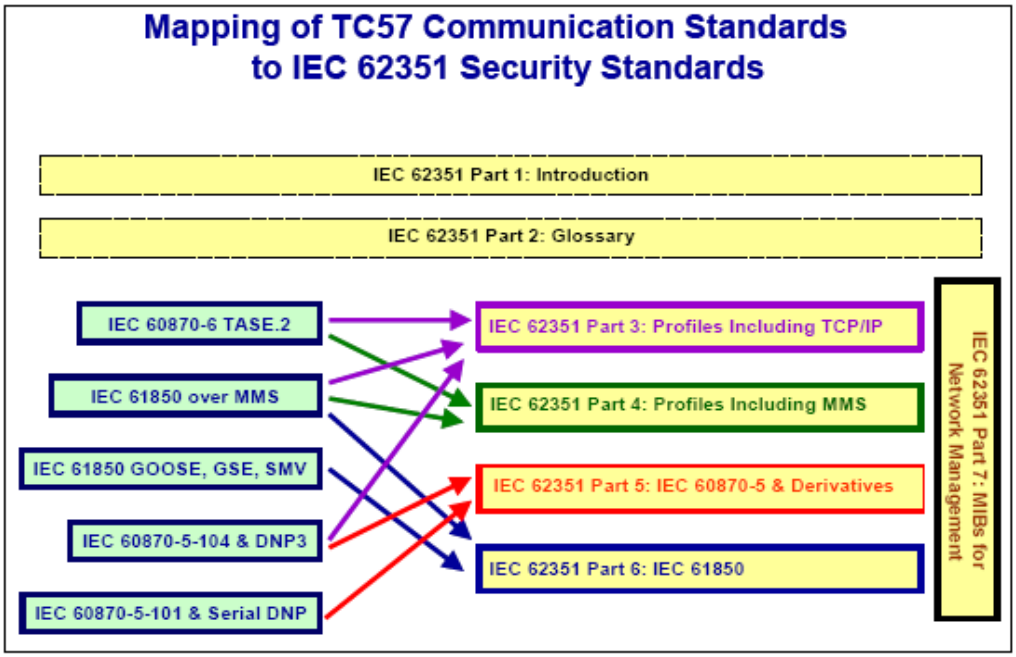


Figure 123 – Mapping of communication standards to IEC 62351-xx

24. Setting Changes via Telecommunication Channels

Telecommunication channels are not normally used to change settings to microprocessor relays. Most utilities prefer and recommend being on site when changing settings on relays that are in service, by taking the relay out of service while making setting changes. This reduces the risk of inadvertently tripping a circuit breaker.

The most common method of changing relay settings is to connect directly from a laptop computer to an RS-232 or RS-485 port on the relay, and using proprietary vender software to communicate with the relay. If the relay has an Ethernet port, then the laptop is connected to the LAN (Local Area Network), which then connects to an individual relay with its own unique IP (Internet Protocol) address. Some relays also can communicate through non-proprietary communications software, such as HyperTerminal.

25. Fault Recorder

Fault recorders store digital and analog data for post-disturbance analysis, and, like relays, are typically located in substations. The recorders can be set to call in data to a master station whenever an event is recorded, or the master station can automatically poll each recorder

periodically and extract new data. Telecommunications equipment plays a critical role in getting the information in a timely fashion. Typical event file size ranges from 20 kB (kilobytes) to several MB (megabytes), and are stored in vendor-proprietary or COMTRADE (Common format for Transient Data Exchange) format.

Fault recorders use vendor-proprietary software to extract the data, and typically communicate by telephone or Ethernet.

26. Fault Location

Having relays calculate the locations and types of faults can be invaluable in a Power Company's ability to quickly isolate the fault and restore service to the affected customers. The information includes the calculated fault distance from the substation, what phases were involved (A, B, C or G), along with a date and time stamp. The relays communicate this information in several ways:

- Traditionally a Technician or Engineer travels to the substation and extracted the information locally from the relay itself. The person then communicates that information to Operations and Maintenance personnel.
- If remote access to the relay is possible, then a traditional phone line or Ethernet connection is used to communicate with the relay, and the fault record is extracted.
- The relay sends the data directly to the local RTU (Remote Terminal Unit), or to a transducer that converts signals from digital to analog. The RTU then transmits the data to the Operations Center.
- Newer, microprocessor-based RTUs can now talk to the relays directly using a variety of protocols, and get the information.

Present communications technology allows two-terminal fault location methods, which are able to eliminate the effects of fault resistance and loading current. Two-terminal fault location methods require the following communications and information:

- Measurement of three-phase voltages and currents or sequence components at each end with a time stamp.
- Modems and other communications equipment to transfer data to the other relay at the end of the line or a central device.
- Correlation of time stamps or power system status/configuration information to perform fault location calculations on data from both ends.

Internet and Web-based technologies allow an enhanced handling of fault data for fault location calculations. Web-based distributed server-client technology can be applied to access fault data and calculate fault location simply.

Furthermore, recent improvements in data acquisition, GPS time synchronization, and communication systems have increased the interest in traveling wave fault location methods. Traveling wave fault location methods require the following communication equipment:

- A very accurate time stamping device on both ends of the line.
- A communications circuit to transmit the time stamped data to a central device.

27. Wide Area Protection including Synchrophasor Applications

27.1 Synchrophasor Systems

A well-designed, successful synchrophasor system has many varied components. By its nature, such a system is most likely geographically diverse. Hardware and software devices must work together, as must field and back-office components. Typical components are shown in the Figure 124 below:

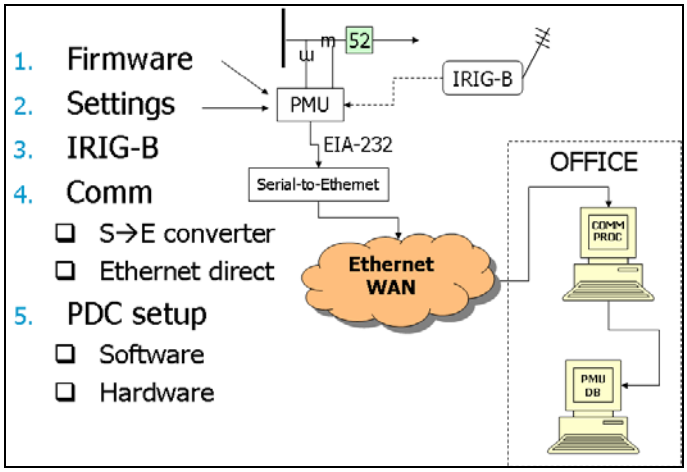


Figure 124 – Synchrophasor System Components

Foremost among these components is the Phasor Measurement Unit (PMU) itself. The PMU can take many forms and the PMUs on a given system may be of many different vintages. Older PMUs are generally stand-alone devices, designed for that dedicated purpose. They may communicate over leased-line modem connections or other low-bandwidth mediums. Those units designed and built before the IEEE Std C37.118-2005 "Standard for Synchrophasors for Power Systems", may support the older IEEE P1344-1995 format or a proprietary, vendor-specific format.

Today, as a result of the C37.118 standard, many different vendors can support this functionality in a wide range of products. In a post C37.118 world, these products stand a much higher likelihood of being integrated together. PMUs can now be imbedded within microprocessor-based protective relays. This offers tremendous cost savings because protective relays are already installed in key locations on the grid. All that needs to be done is to add a "hook" into the relay to retrieve the data.

Aside from the adoption of the C37.118 standard, another significant advancement in this field is the deployment of high-speed Ethernet based communications infrastructure. Most utilities now have the ability to send synchrophasor data from the field to the office in a standard format via TCP/IP or UDP over a corporate Wide Area Network (WAN) to a central Phasor Data

Concentrator (PDC). This capability has made widespread data gathering virtually "plug and play" and no longer requires dedicated, maintenance-intensive communication circuits for synchrophasor data. If a direct Ethernet output is unavailable on a particular relay or device, a separate EIA-232 serial-to-Ethernet converter can be utilized to immediately convert the serial output to Ethernet. Special attention must be paid to WAN firewall settings as well as which ports are being used for sending data and control signals from PMU to PDC.

Other PDC topology considerations involve distributed, master-slave PDC approaches versus a centralized PDC. A distributed PDC approach – where a PDC is installed in the field, at a receiving station for example – is ideal for sites where many individual PMUs are located. The distributed PDC (likely a hardware-based PDC) can collect data from multiple PMUs on-site over a simple serial (or Ethernet) data connection and can then aggregate the data and send it back to a master PDC via Ethernet. A centralized PDC approach is better for gathering data from multiple, widely dispersed stations that may only have a single PMU in each of them. The centralized approach involves higher communication costs while the master-slave approach involves higher PDC costs. Ultimately, the topology of your system will dictate your approach and, once again, a hybrid approach may be the overall best route.

Note that once synchrophasor applications progress beyond merely monitoring the electric system to actually controlling aspects of the system in near real-time in response to received data, communication requirement can change dramatically. Most notably, communication speed, availability, and bandwidth requirements all increase.

Once a synchrophasor system has been designed and deployed, it comes time to operate it. Various challenges await the operator. Distributed systems that depend on many diverse components, such as a quality IRIG-B time signal, a continuous communications channel, PMU hardware, PDC software, etc can be prone to failure.

The first step is becoming aware of such a problem. For this reason, it is important to build into your system alarms and annunciation for all the different failure modes such as IRIG-B failure, communication channel failure, PMU failure, and PDC software failure. If a system is successfully deployed it will have customers, and those customers will come to depend on the applications supported by the PMU synchrophasor data. Without the data, the applications will fail and the customers (likely other departments at your same utility) will have problems operating or analyzing the electric system.

Ultimately, these issues will need to be resolved by the utility industry before synchrophasor applications can become robust and trusted enough to enter the mainstream utility environment. Some resolutions depend on vendor involvement and cooperation, while others are problems internal to and unique to each utility.

28. Event Recorder

The role of telecommunications in Event Recorders is the same as for Fault Recorders, as discussed above.

Appendix 1

Glossary of terms

The following definitions are representative of how these terms are used in the telecommunications industry.

AU-N - Administrative Unit-N; a discrete unit of the SDH payload carrying one or more VC-N

adaptive relaying - a protection philosophy that permits and seeks to make automatic or semi-automatic adjustments to various protection functions in order to make them more attuned to prevailing power system conditions.

asynchronous - A communication practice where the transmitting and receiving units are not timing the received data via some common clock. EIA 232 is a common asynchronous communications scheme.

bandwidth - In an analog communications system, bandwidth refers to the amount of spectrum occupied by the communications signal. In a digital system, it is used to refer to the data rate. i.e. "OC3 is a higher bandwidth channel than OC1."

bit stuffing - A technique used to synchronize signals to a common rate before multiplexing. In asynchronous systems, the number of bits stuffed varies according to the difference between the outgoing synchronous data rate and the incoming asynchronous rate.

BITS Clock – Stratum 1 Building Integrated Timing Supply clock.

bps- bits per second is a unit of measure of the speed of data transmission when there are only two signal levels (e.g. 0 and 1). The term Baud is commonly misused to mean bps.

byte interleaved - a process used in time division multiplexing where individual bytes from different lower speed channel sources are combined into one continuous higher speed bit stream.

CDMA – Code Division Multiple Access

communication protocol - A formal set of conventions governing the format and relative timing devices and other of message exchange parameters between two communications terminals.

data crosses (crosstalk) - Unwanted transfer of energy from one adequate circuit to another.

DACS - Digital Access Crossconnect System - A device that can rearrange the lower speed logical paths in a multiplexed signal for retransmission at the higher rate.

digital cross connect - Any device used to connect electrical or logical signals between devices. Electrically this refers to a patch panel. See DACS.

dynamic range - The difference, in decibels, between the overload level and the minimum acceptable signal level in a communications system.

error bursts - A burst of incorrect data bits in a communications system. Error bursts usually occur during resynchronization or bit slippage. Error bursts are more typical than steady state errors in digital communications.

ES - Errored Second; measure of network or equipment performance

FSK - frequency-shift keying. The form of frequency modulation in which the modulating signal shifts the output frequency between predetermined frequency values.

FIFO - First-In First-Out; a type of data buffer

GPS - Global Positioning Satellite, a source of reference timing traceable to Universal Co-ordinated Time (UTC), internationally-managed reference time

Hello Packets - A special packet (message) that is sent out periodically from a router to establish and confirm network adjacency relationships.

IED – Intelligent Electronic Device

ISI - Inter-Symbol Interference; jitter caused by mis-equalization

ISL - Inter-Switch Link is a Cisco Systems proprietary protocol that maintains VLAN information in Ethernet frames as traffic flows between switches and routers, or switches and switches.

IP – Internet Protocol

index of refraction - The ratio of the phase velocity in free space to that in the medium.

I/O – Input Output

LED - Light-Emitting Diode

MTIE - Maximum Time Interval Error; a measure of wander

multipath fading - The propagation phenomenon that results in signals reaching the receiving antenna by two or more paths. When two or more signals arrive simultaneously, wave interference results causing distortion.

multiplexer - a device allowing two or more signals to pass over and share a common transmission path simultaneously.

NTP - The Network Time Protocol is a protocol and software implementation for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks. It is one of the oldest Internet protocols.

overhead bits - Bits in a serial data stream assigned for the use of the communication equipment and not available for payload. Overhead bits are used for functions associated with transporting the payload such as switching and network management.

OCXOs - Oven-Controlled Crystal Oscillators. High performance crystal oscillators employ temperature control circuitry to hold the crystal and critical circuitry at a precise, constant temperature.

OPC Server - Software application that acts as an API (Application Programming Interface) or protocol converter. An OPC Server will connect to a device such as a PLC, DCS, RTU, or a data source such as a database or User interface, and translate the data into a standard-based OPC format.

packet - an ordered group of data and control signals transmitted through a network, as a subset of a larger message.

packet switching - A data transmission technique, which divides user information into discrete envelopes called packets, and sends information packet by packet.

PCMCIA Card - Personal Computer Memory Card International Association is the form factor of a peripheral interface designed for laptop computers.

PDH - Plesiochronous Digital Hierarchy; historical transmission system (also a tributary of SDH)

phasor - a complex number representation of a fundamental frequency component of a waveform. A phasor includes amplitude and phase angle information

PLL - Phase-Locked Loop; method of timing recovery

ppTIE - Peak-to-Peak Time Interval Error , a measure of wander

RAS - Remote Access Services refers to any combination of hardware and software to enable the remote access tools or information that typically reside on a network of IT devices

RaW Socket - In computer networking, a RaW socket is an internet socket that allows direct sending and receiving of raw network packets.

RFC - In computer network engineering, a Request for Comments (RFC) is a memorandum published by the Internet Engineering Task Force (IETF) describing methods, behaviors, research, or innovations applicable to the working of the Internet and Internet-connected systems.

RIP – Routing Information Protocol is a distance-vector routing protocol, which employs the hop count as a routing metric. RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from the source to a destination. The maximum number of hops allowed for RIP is 15.

RIP II - RIP version 2 was developed in 1993 and last standardized in 1998 to overcome the deficiencies of the original RIP specification. It included the ability to carry subnet information, thus supporting Classless Inter-Domain Routing (CIDR). To maintain backward compatibility, the hop count limit of 15 remained.

rms - Root Mean Square; calculation often applied to power and noise measurements

SDH - Synchronous Digital Hierarchy

SES - Severely Errored Second; measure of network performance

SMPP - Short Message Peer-to-Peer protocol is a telecommunications industry protocol for exchanging SMS messages between SMS peer entities such as short message service centers and/or External Short Messaging Entities. It is often used to allow third parties (e.g. value-added service providers like news organizations) to submit messages, often in bulk.

SMS - Short Message Service (SMS) is a text messaging service component of phone, web, or mobile communication systems, using standardized communications protocols that allow the exchange of short text messages between fixed line or mobile phone devices.

SNTP - Simple Network Time Protocol is a less complex implementation of NTP, using the same protocol but without requiring the storage of state over extended periods of time.

Synchronous - A mode of transmission in which the sending and receiving terminal equipment are operating continuously at the same rate and are maintained in a desired phase relationship by an appropriate means. This means can be an external clock or a clock accompanying the data.

TCP – Transmission Control Protocol

TDEV - Time Deviation; a measure of wander

TDMA – Time Division Multiple Access

Teleprotection - A type of communication terminal equipment used by the relaying industry for sending discrete contact logic signals from point to point with a high degree of security and dependability.

TIE - Time Interval Error; a measure of wander

time division multiplexing. Sharing a communication channel among several users by allowing each to use the channel for a given period of time in a defined repeated sequence.

trunked radio - a system that allows multichannel radios to communicate via a central radio backbone. The radios are assigned to a unique channel at the time a connection is made.

UART - Universal Asynchronous Receiver / Transmitter

UI - Unit Interval; a measure of jitter

UIpp - Unit Interval Peak-to-Peak; a common measure of jitter

UIrms - Unit Interval rms; a measure of jitter in line systems

Unix - Officially trademarked as UNIX, sometimes also written as UNIX, is a multitasking, multi-user computer operating system originally developed in 1969.

VCSEL - Vertical Cavity Surface Emitting Laser

XLR connector - is a style of electrical connector, primarily found on professional audio, video, and stage lighting equipment. The connectors are circular in design and have between 3 and 7 pins.

Appendix 2

Acronyms

4WIF	4 Wire voice channel InterFace
A/D	Analog to Digital
ACK	Acknowledgement
ACPW	AC Pilot Wire
ACSI	Abstract Communication Service Interface
ADCCP	Advanced Data Communication Control Protocol
ADU	Application Data unit
AGC	Automatic Gain Control
AIS	Alarm Indication Signal
AMI	Alternate Mark Inversion
ANSI	American National Standards Institute
APDU	Application Protocol Data Unit
API	Application Programming Interface
ARP	Address Resolution Protocol
ARQ	Automatic Repeat-Request
ASCII	American Standard Code for Information Interchange
ASDU	Application Service Data Unit
ASK	Amplitude Shift Keying
AT	Audio Tone
ATM	Asynchronous Transfer Mode
B8ZS	Bipolar 8-Zero Substitution
BER	Bit Error Rate
BITS	Building Integrated Timing Supply
BLSR	Bidirectional Line Switched Ring
BPDU	Bridge Protocol Data Unit
BRP	Beacon Redundancy Protocol
CAT	Category
CATV	Cable TV
CC	Coupling Capacitor
CCITT	International Telegraph and Telephone Consultative Committee
CD	Collision Detection
CDM	Code Division Multiplexing
CDMA	Code Division Multiple Access
CFI	canonical Format Indicator
CID	Configured IED Description
CIDR	Classless Inter-Domain Routing
Coax	Co-Axial
COMTRADE	COMmon format for TRAnsient Data Exchange
CoS	Class of Service
COT	Cause of Data Transmission
CR	ASCII Carriage Return – refers to a control character or mechanism

	used to reset a device's position to the beginning
CR/LF	ASCII Carriage Return / line feed (new line) character combination
CRC	Cyclic Redundancy Check
CRLF	Carrier Return / Line Feed Character - MS-DOS style
CRP	Cross-network Redundancy Protocol
CSMA	Carrier Sense Multiple Access
DANC	Doubly-attached Nodes
DANH	Doubly Attached Node with HSR protocol
DARPA	Defense Advanced research Projects Agency
DCB	Direct Comparison Blocking
DCE	Data circuit-terminating Equipment
DCU	Directional Comparison Unblocking
DCUB	Directional comparison UnBlocking
DEC	Digital Equipment Corp.
DHCP	Dynamic Host Configuration Protocol
DIF	Digital Interface
DIFF	Differential (relay)
DIG	Digital
DMZ	Demilitarized Zones
DNP	Distributed Network Protocol
DOS	Disk Operating System
DPLC	Digital Power Line Carrier
DRP	Distributed Redundant Protocol
DS	Digital Signal
DSCP	Differentiated Service Control Point
DSL	Digital Subscriber Line
DSP	Digital Signal Processing
DT	Direct Transfer
DTE	Data Terminal Equipment
DTT	Direct Transfer Trip
DTT	Direct Transfer trip
DWDM	Dense Wavelength Division Multiplexing
EBCIDIC	Extended Binary Coded Decimal Interchange Code
ECC	Error Correcting Code
ECSA	Exchange Carriers Standards Association
EIA	Electronic Industry Association
EMI	Electro Magnetic Interference
EMS	Energy Management System
eRSTP	Enhanced Rapid Spanning Tree Protocol
*ETSI	European Telecommunication Standards Institute
FCC	Federal Communications Commission
FC-PC	FC connector may be designated "FC/PC" (for physical contact)
FDM	Frequency Division Multiplexing
FEC	Forward Error Correction
FSK	Frequency Shift Keying
FTP	Foiled Twisted Pair

ftype	function type
GOOSE	Generic Object Oriented Substation Events
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global System for Mobile
GUI	Graphical User Interface
GSE	Generic Substation Events
GSSE	Generic Substation State Events
HDB	High Density Bipolar
HDB3	High-Density Bipolar 3
HDLC	High-Level Data Link Control
HFC	Hybrid Fiber Coax
HMI	Human Machine Interface
HSR	High-availability Seamless Redundancy
ICCP	Inter-Control Centre Protocol
ICD	IED Capability Description
ICMP	Internet Control Message Protocol
ICT	Information and Communication Technologies
IEC	International Electro-mechanical Commission
IED	Intelligent Electronic Device
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IRIG-B	Inter-Range Instrumentation Group time code type B
ISA	Industry Standard Architecture
ISDN	Integrated Services Digital Network
ISL	Inter-Switch Link
ISO	International Standards Organization
IT	Information Technology
ITU	International Telecommunication Union
LACP	Link Aggregation Control Protocol
LAN	Local Area Network
LC	Inductance/Capacitance
LCx	Logical Connection
LLC	Logical Link Control
LNx	Logical Node
LF	Line Feed (New Line) ASCII Character
LTU	xxx Line Tuning Unit
MAC	Media Access Control
MAS	Multiple-Address System
MB	Mega Bytes
MBAP	Modbus Application Protocol
MMS	Multimedia Messaging Service
MRM	Media Redundancy Manager
MRP	Media Redundancy Protocol

MS-DOS	Microsoft Disc Operating System
MS-SPRing	2- or 4-fiber Multiplex Section Shared Protection Ring
MSTP	Multiple Spanning Treee Protocol
MTIE	Maximum Time Interval Error
MTTF	Mean Time To Failure
MTTR	Mean Time To Repair
MUX	Multiplexer
NCO	Numerical Control Oscillator
NCP	network Control Program
NE	Network Element
NMS	Network Management System
NRZ	Non return To Zero
NTP	Network Time Protocol
OC	Optical Carrier
OCXO	Reference Oscillator
OFDM	Orthogonal Frequency Division Multiplexing
OFIF	Optical Fiber InterFace
OS	Operating System
OSI	Open Systems Interconnect
OSPF	Open Shortest Path First – Routing protocol
OUI	Organizational Unique Identifier
PAD	Packet Assembler Disasssembler
PAM	Pulse Amplitude Modulation
PC	Phase Comparison (relay)
PCI card	Peripheral Component Interconnect card
PCM	Pulse Code Modulation
PCMCIA	Personal Computer Memory Card International Association
PCS	Personal Digital Service
PDC	Phasor Data Concentrator
PDH	Plesiochronous Digital Hierarchy
PDU	Protocol Data Unit
PEP	Peak Envelope Power
PLC	Programmable Logic Controller
PLC	Power Line Carrier
PLCC	Power Line Carrier Communication
PLL	Phase Lock Loop
PMU	Phasor Measurement Unit
POTS	Plain Old Telephone System
POTT	Permissive Overreaching Transfer trip
PPP	Point-to-Point Protocol
PRC	Primary Reference Clock
PRP	Parallel Redundancy Protocol
PSK	Phase Shift Keying
PT	Precision Time
PTP	Precision Time Protocol
PTT	Permissive Transfer Trip

PUTT	Permissive Underreaching Transfer trip
PWIF	Pilot Wire Interface
PWIM	Pilot Wire Interface Module
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
RAS	Remote Access Service
RF	Radio Frequency
RFC	Request for Comments
RIP	Routing Information Protocol
RIP II	Routing Information Protocol Version 2
RJ-xx	Registered Jack - (telephone style) network connector
RSGB	Radio Society of Great Britain
RSTP	Rapid Spanning Tree Protocol
RTU	Remote Terminal Unit
Rx	Receive
S Format	supervisory function
SAS	Substation automation System
SCADA	Supervisory Control and Data Acquisition
SCD	Substation Configuration Description
SCL	Substation Configuration Description Language
SCSM	Specific Communication Service Mapping
SDH	Synchronous Digital Hierarchy
Sercos	**SE**rial **R**eal-time **CO**mmunication **S**ystem
SMPP	Short Message Peer-to-Peer protocol
SMS	Short Message Service
SNCP	2-fiber Sub-Nework Connection Protection Ring
SNR	Signal to Noise Ratio
SNTP	Simple Network Time Protocol
SONET	Synchronous Optical Network
SS	Spread Spectrum
SSB	Single Side Band
SSD	System Specific Description
SSM	Synchronization Status Message
STARTDT	Start Data Transfer
STM	Synchronous Transport Model
STOPDT	Stop Data Transfer
STP	Shielded Twisted Pair
STP	Spanning Tree Protocol
STS	Synchronous Transport Signal
SW	Software
TASE-2	Telecontrol Application Service Element
TCI	Tag Control Information
TCP	Transmission Control Protocol
TDEV	Time Deviation
TDM	Time Division Multiplexing
TDMA	Time Division Multiple Access

TESTFR	Test APDU
TIA	Telecommunication Industry Association
TIE	Time Interval Error
ToS	Type of Service
TPID	Tag Protocol Identifier
TSG	Timing Signal Generator
TTIF	Transfer Trip Interface
Tx	Transmit
U Format	Unnumbered Control Function
UART	Universal Asynchronous Receiver/Transmitter
UCA	Utility Communications Architecture
UDP	User Datagram Protocol
UHF	Ultra High Frequency
UI	Unit Intervals
UPSR	Unidirectional Path Switched Ring
UPSR	Unidirectional Path Switched Ring
UTC	Coordinated Universal Time
UTP	Unshielded Twisted Pair
VHF	Very High Frequency
VID	VLAN Identifier
VLAN	Virtual Local Area Network
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network
WDM	Wavelength Division Multiplexing
XML	eXtensible Markup Language

Appendix 3

List of Standards

IEC 101	Abbreviation for IEC 60870-5-101
IEC 103	Abbreviation for IEC 60870-5-103
IEC 104	Abbreviation for IEC 60870-5-104
IEC 60044-8	Instrument transformers – Part 8: Electronic current transformers
IEC 60870-5	IEC 60870 part 5 is one of the IEC 60870 set of standards which define systems used for telecontrol (supervisory control and data acquisition) in electrical engineering and power system automation applications. Five documents specify the base IEC 60870-5:
IEC 60870-5-1	Transmission Frame Formats
IEC 60870-5-2	Data Link Transmission Services
IEC 60870-5-3	General Structure of Application Data
IEC 60870-5-4	Definition and Coding of Information Elements
IEC 60870-5-5	Basic Application Functions
IEC 60870-5-101	Telecontrol equipment and systems - Part 5-101: Transmission protocols - Companion standard for basic telecontrol tasks
IEC 60870-5-102	Telecontrol equipment and systems - Part 5: Transmission protocols - Section 102: Companion standard for the transmission of integrated totals in electric power systems
IEC 60870-5-103	Telecontrol equipment and systems – Part 5-103: Transmission protocols – Companion standard for the informative interface of protection equipment
IEC 60870-5-104	Telecontrol equipment and systems – Part 5-104: Transmission protocols – Network access for IEC 60870-5-101 using standard transport profiles
IEC 60870-5-6	Guidelines for conformance testing for the IEC 60870-5 companion standards
IEC 61850	Communication Networks and Systems in Substation
IEC 61850-1	Communication networks and systems in substations - Part 1: Introduction and overview
IEC 61850-2	Communication networks and systems in substations - Part 2: Glossary
IEC 61850-3	Communication networks and systems in substations - Part 3: General requirements
IEC 61850-4	Communication networks and systems in substations - Part 4: System and project management
IEC 61850-5	Communication networks and systems in substations - Part 5: Communication requirements for functions and device models
IEC 61850-6	Communication networks and systems for power utility automation - Part 6: Configuration description language for

	communication in electrical substations related to IEDs
IEC 61850-7-1	Communication networks and systems in substations - Basic communication structure for substation and feeder equipment - Principles and models
IEC 61850-7-2	Communication networks and systems in substations - Basic communication structure for substation and feeder equipment - Abstract communication service interface (ACSI)
IEC 61850-7-3	Communication networks and systems in substations - Basic communication structure for substation and feeder equipment - Common Data Classes
IEC 61850-7-4	Communication networks and systems in substations - Basic communication structure for substation and feeder equipment - Compatible logical node classes and data classes
IEC 61850-8-1	Communication networks and systems in substations - Specific Communication Service Mapping (SCSM) - Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3
IEC 61850-9-1	Communication networks and systems in substations - Specific Communication Service Mapping (SCSM) - Sampled values over serial unidirectional multidrop point to point link
IEC 61850-9-2	Communication networks and systems in substations - Specific Communication Service Mapping (SCSM) - Sampled values over ISO/IEC 8802-3
IEC 62351-1	Power systems management and associated information exchange - Data and communications security - Part 1: Communication network and system security - Introduction to security issues
IEC 62351-2	Power systems management and associated information exchange - Data and communications security - Part 2: Glossary of terms
IEC 62351-3	Power systems management and associated information exchange - Data and communications security - Part 3: Communication network and system security - Profiles including TCP/IP
IEC 62351-4	Power systems management and associated information exchange - Data and communications security - Part 4: Profiles including MMS
IEC 62351-5	Power systems management and associated information exchange - Data and communications security - Part 5: Security for IEC 60870-5 and derivatives
IEC 62351-6	Power systems management and associated information exchange - Data and communications security - Part 6: Security for IEC 61850
IEC 62351-7	Power systems management and associated information exchange - Data and communications security - Part 7: Network and system management (NSM) data object models
IEC 62351-8	Power systems management and associated information exchange - Data and communications security - Part 8: Role-based access control
IEC 62439	Industrial communication networks - High availability

	automation networks - Part 2: Media Redundancy Protocol (MRP)
IEC 8802-3	Information technology -- Telecommunications and information exchange between systems -- Local and metropolitan area networks -- Specific requirements -- Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications
IEEE 643	IEEE Guide for Power-Line Carrier Applications
IEEE 802.3	IEEE Standard for Information technology-Specific requirements - Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications Corrigendum 1: Timing Considerations for PAUSE Operation
IEEE 802.1p	IEEE Standard for Local and metropolitan area networks Media Access Control (MAC) Bridges
IEEE 802.1q	IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks
IEEE 802.1w	IEEE Standard for Information Technology -Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Common Specifications - Part 3: Media Access Control (MAC) Bridges: Amendment 2 - Rapid Reconfiguration
IEEE 1379-2000	Superseded by WGC3.1379 - Recommended Practice for Data Communications Between RTUs & IEDs in a Substation
IEEE 1588	Precise Networked Clock Synchronization Working Group
IEEE C37.94-2002	IEEE Standard for N Times 64 Kilobit Per Second Optical Fiber Interfaces Between Teleprotection and Multiplexer Equipment
IEEE C37.238-2011	IEEE Standard Profile for Use of IEEE 1588 Precision Time Protocol in Power System Applications
IEEE P1613	Standard for Environmental and Testing Requirements for Communications Networking Devices Installed in Electric Power Facilities

References

[1] B. Lundqvist, “100 years of relay protection, the Swedish ABB relay history,” ABB Automation Products, Substation Automation Division, [Online]. Available: http://www05.abb.com/global/scot/scot296.nsf/veritydisplay/c1256d32004634bac1256e19006fd705/$File/PAPER_2001_08_en_100_Years_of_Relay_Protection__the_Swedish_ABB_Relay_History.pdf. [Accessed: June 10, 2010].

[2] “Telecommunications: the network’s nervous system,” published by AREVA T&D, Winter 2009-10, [Online]. Available: http://www.areva-td.com/home_tdmain/liblocal/docs/Think%20TD/Think%20TD_6%20EN%20II-1%20Telecom.pdf. [Accessed: June 10, 2010].

[3] ITU-T Recommendation G.810, Definitions and terminology for synchronization networks.

[4] R. Neil, “Understanding Jitter and Wander Measurements and Standards,” Agilent Technologies, Second Edition. February 1, 2003.

[5] Wikipedia contributors, “Universal asynchronous receiver/transmitter,” Wikipedia, The Free Encyclopedia, June 8, 2010, [Online]. Available: http://en.wikipedia.org/w/index.php?title=Universal_asynchronous_receiver/transmitter&oldid=366837008. [Accessed: June 10, 2010].

[6] ITU-T Recommendation V.11/X.27, Electrical characteristics for balanced double-current interchange circuits operating at data signaling rates up to 10 Mbit/s.

[7] IEEE/PSRC Working Group H2, “Using Spread Spectrum Radio Communication for Power System Protection Relaying Applications,” IEEE Power System Relaying Committee. July 5, 2005.

[8] D. Woodward, “Ethernet Networks Technology in Electrical Substations,” The Electricity Forum, [Online]. Available: http://www.electricity-today.com/et/Issue0802/i08_ethernet.htm. [Accessed: June 10, 2010].

[9] M. Pozzuoli, R. Moore, “Ethernet in the Substation,” Power Engineering Society General Meeting, Montreal, Quebec, October 16, 2006.

[10] W. Morgan, J. Read, R. Midence, “Providing High Speed Relay Fault Protection between Substations,” [Online]. Available: http://www.electricenergyonline.com/?page=show_article&mag=49&article=360. [Accessed: June 10, 2010].

[11] R. Moore, G. Allen, R. Midence, “Migrating from Serial to Ethernet Communications” presented at DistribuTECH 2008, January 2008

[12] Wikipedia contributors, “DNP3,” Wikipedia, The Free Encyclopedia, April 19, 2010, [Online]. Available: http://en.wikipedia.org/w/index.php?title=DNP3&oldid=356979410. [Accessed: June 10, 2010].

[13] Wikipedia contributors, “IEC 60870-5”, Wikipedia, The Free Encyclopedia, May 12, 2010, [Online]. Available: http://en.wikipedia.org/w/index.php?title=IEC_60870-5&oldid=361631593. [Accessed: June 10, 2010].

[14] CIGRE TB 317, “Security for Information Systems and Intranets in Electric Power Systems”, JWGD2/B3/C2.01, April 2007.

[15] IEEE C37.93, Guide for Power System Protective Relay Applications of Audio Tones Over Voice Grade Channels.

[16] IEEE PC37.236, Guide for Power System Protective Relay Applications over Digital Communication Channels.

[17] W. Pacino, “Principles & Metrics of Jitter and Wander,” March, [Online]. Available: http://users.rcn.com/wpacino/jitwtutr/jitwtutr.htm. [Accessed: June 10, 2010].

[18] ITU-T Recommendation O.171, Characteristics of synchronous digital hierarchy (SDH) equipment functional blocks.

[19] ITU-T Recommendation G.783, Characteristics of synchronous digital hierarchy (SDH) equipment functional blocks.

[20] ITU-T Recommendation G.811, Timing characteristics of primary reference clocks.

[21] CIGRE JWG 34/35.11, Protection using Telecommunications

[22] S. Ward, T. Dahlin, B. Ince, “Pilot Protection Communication Channel Requirements,” *RFL Electronics Inc.*, p. 50.

[23] “Synchronous Optical Network (SONET),” *IEC Web ProForum Tutorials*, p. 50, [Online]. Available: http://www.iec.org. [Accessed: June 10, 2010].

[24] “Synchronous Digital Hierarchy (SDH) ,” *IEC Web ProFurom Tutorials*, p. 50, [Online]. Available: http://www.iec.org. [Accessed: June 10, 2010].

[25] CIGRÉ Study Committee D2 Working Group 23, Brochure to assist utilities to plan, specify, design and implement Ethernet infrastructures necessary for the IP-based operational applications of the electrical power delivery system.

[26] “How Ethernet Works,” on the How Stuff Works website at http://computer.howstuffworks.com/ethernet3.htm.

[27] “Power Line Carrier Channel & Application Considerations For Transmission Line Relaying”, Miriam P. Sanders, Roger E. Ray, Pulsar Technologies, Inc.; Pulsar Document Number C045–P0597