315

COMMUNICATIONS TECHNOLOGY FUNDAMENTALS FOR THE DESIGN OF MODERN PROTECTION AND CONTROL SYSTEMS

Working Group
D2.16

April 2007

COMMUNICATIONS TECHNOLOGY FUNDAMENTALS FOR THE DESIGN OF MODERN PROTECTION AND CONTROL SYSTEMS

Working Group
D2.16

Active Members :

Andres Cadenas	(**Convener**)	**Spain**
Carlos Samitier		**Spain**
Chris Quirke	(**Secretary**)	**Ireland**
Dave Dolezilek		**USA**
John Fitch		**United Kingdom**

Corresponding Members :

Masakazu Koaizawa	**Japan**
Josep Maria Nadal	**Spain**
Rodolfo Pellizzoni	**Argentina**
Cuitlahuac Picasso	**Mexico**

n° ISBN : 978-2-85873-005-6

TABLE OF CONTENTS

RÉSUMÉ **2**

KEYWORDS **2**

FOREWORD **2**

1 INTRODUCTION **3**

1.1 SAS DEFINITION 3
1.2 SAS STRUCTURE AND FUNDAMENTALS 3
1.3 SAS DEVICE 4
1.4 SAS INTERFACES 5
1.5 SAS FUNCTIONS 6
1.6 SAS COMMUNICATIONS 6

2 DATA EXCHANGE REQUIREMENTS **8**

2.1 LEAD APPLICATIONS 8
2.2 IMPORTANCE LEVEL OF COMMUNICATIONS 11
2.3 COMMUNICATIONS SERVICE LEVEL CRITERIA 11

3 COMMUNICATIONS TECHNOLOGIES DESCRIPTION **12**

3.1 TRANSMISSION MEDIA OUTSIDE SUBSTATIONS 12
3.2 TRANSMISSION MEDIA INSIDE SUBSTATIONS 15
3.3 COMMUNICATIONS METHODS 16
3.4 COMMUNICATION TOPOLOGY 18
3.5 COMMUNICATION TECHNOLOGIES 19
3.6 BACKBONE TECHNOLOGY 20
3.7 DATA SECURITY 24

4 COMMUNICATIONS AND APPLICATIONS MATRIX **25**

4.1 METHODOLOGY 26

5 CROSS WORKING MATRICES. RESULT **26**

6 CONCLUSIONS **27**

7 REFERENCES **29**

ANNEXES **30**

A. MATRICES **30**

B. SECURITY ANNEX **39**

Résumé

This technical brochure analyses the advantages and disadvantages of both the use and impact of available communication technologies, inside and outside the substation, in protection and control systems for a Substation Automation System by means of a cross matrices methodology. The output matrix provides a relative assessment of communications technology performance for lead applications in substations.

Keywords

Communications technologies, Telecommunications, Control Systems, Protection Systems, Design

Foreword

Cigré Study Committee D2 created Working Group 16 at the end of 2001 to investigate and evaluate utility applications and the communication technologies available and their effects on the performance of substation automation systems.

Working Group 16 has been following technological advances in the environment of communications to study its potential impact in the power utilities.

1 Introduction

The aim of this technical brochure is to analyse the advantages and disadvantages of both the use and impact of available communication technologies, inside and outside the substation, in protection and control systems for a Substation Automation System by means of a cross matrices methodology. The output is a matrix which gives a relative assessment of technology performance; with communications technologies in rows and applications in columns.

This document is structured to facilitate consideration of the implications of using different communications technologies in protection and control systems design to different members within the Electrical Power Industry.

The first chapter describes a Substation Automation System in terms of structure, fundamentals, components, interfaces, functions and communications.

Chapter 2 concerns with the classification of data and information flows of applications in transmission and distribution substations used in Chapter 4. The data is classified in matrices in terms of lead applications and data application.

Chapter 3 provides a reference of modern communication technologies and explains the concepts used in the following chapter.

Chapter 4 shows a communications and applications matrix which crosses the criteria described in Chapter 2 with the communications technologies shown in Chapter 3. The methodology applied to produce the output of the chapter is also described here.

Chapter 5 has as its goal the multiplication of the matrices produced in Chapters 2 and 4 in order to produce the final matrix which shows the applicability of communication technologies.

Chapter 6 shows the conclusions and results achieved.

Chapter 7 includes the references used in this work.

For those wishing to know more details on the methodology followed, annexes with all the matrices have been included.

1.1 SAS Definition

A Substation Automation System is a set of inter-connected devices aiming at protecting, supervising and operating the electrical network.

In this brochure, the acronym SAS will be used. It stands for Substation Automation System.

1.2 SAS Structure and Fundamentals

A SAS consists of a given set of devices that protects, supervises and operates a part of the system, e.g., a busbar, a transformer, or a line. In almost all cases, this is associated with a breaker. The set of devices associated with a breaker is called a bay, and is associated with level 1, process level or by extension bay-level. It is in charge of the high voltage interface, for both acquisition and controls. Its operation is autonomous for many fast/automatic actions, especially the elimination of faults and power restoration. One SAS comprises several bays, approximately as many as the number of breakers in the substation (See Figure 1.1).

All bays interface with the substation-level SAS devices. This enables the SAS to provide a single interface to all bays, and is in charge of station-wide automation, local control as well as the interface with substation external applications.

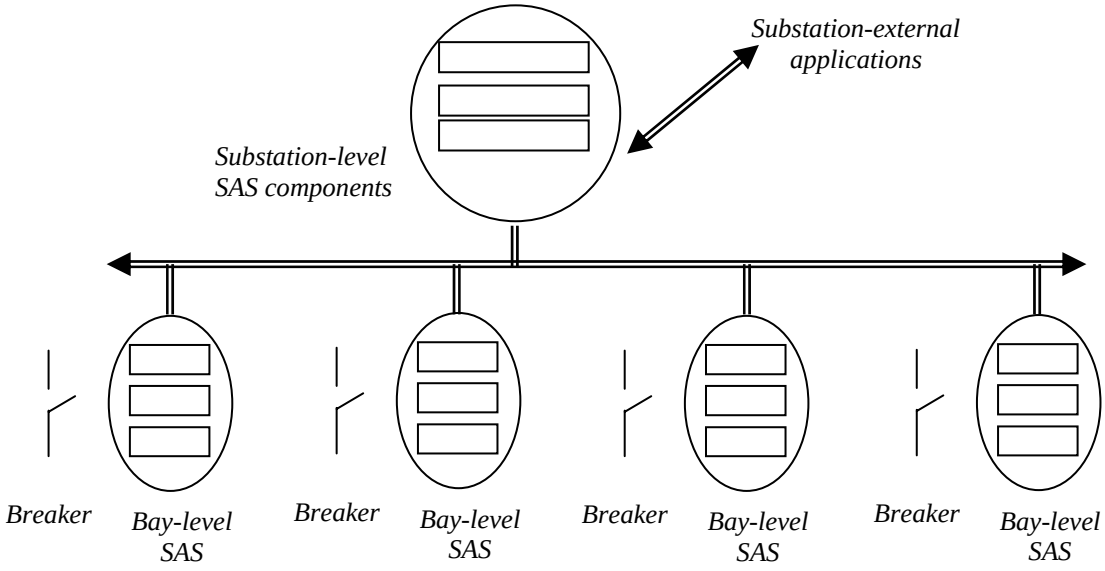


Figure 1.1 SAS

1.3 SAS Device

SAS components at bay-level include the following: protection, Input/Output controllers, automation computer, and communication computer. The last three items can be combined in one single device often called a Bay Computer.

SAS components at substation-level are substation computer, local control computer, telecontrol computer, and communication devices such as switches and routers.

An SAS comprises other components as well which are not critical for the performance of the system and are used for measurement or maintenance functions.

Protection Equipment

Usually called protective relays, these dynamically analyse currents and sometimes voltages on the high-voltage apparatus they protect: a line, a busbar or a transformer. Current and voltage signals are computed to decide whether or not the protection has to act to eliminate a fault. The protection operates mainly by issuing a trip command to the breaker. One bay comprises several protection relays of different types, each one to cope with a specific type of fault.

Input – Output Controllers

Controlling a substation is essentially controlling the switching apparatus. This indicates its position and associated mechanisms by means of binary voltage signals and some analogue signals. The switching apparatus can be controlled by switching low-voltage relays and applying a voltage to their closing or opening mechanism.

An SAS acquires all the station signals and is able to send all necessary commands. To enable the SAS to carry out this Input-Output computers are used. These are adapted to the substation by using the appropriate number and types of input and output boards.

Bay-level devices have to exchange data between themselves and also with the rest of the substation. Within the bay, communication is used for sharing data and is mainly used by the control and supervision functions. In the case where communication is used for automation, it supports some critical data exchanges.

The data exchanges with the rest of the substation are intended to gather data at substation level and in general it is not time critical. An important exception is the inter-bay signals for protections coordination: they are critical in time, dependability and reliability. Until recently these signals were only hard-wired, but new communication standards also address these signals and this is now achievable with digital communication.

Bay-level devices support one or two types of digital communications, although the trend is to one single bus in the substation. As most data handled by the Input-Output computer has to be transmitted to substation-level devices, the communication controller is usually an integral part of these devices.

Automation computer

The operation of a substation needs two types of automation:

- automatic actions, which cannot be carried out by a person (reaction in a few tens of ms)
- pre-defined sequences of actions, where it is desirable that the operational procedure is carried out automatically.

Automatic actions are carried out by the protection relays. These are the fastest actions in the SAS and are mission-critical, as their correct operation is directly linked to security of people, preventing damage which could occur to the high-voltage elements, and the safe and efficient operation of the complete network.

Other fast automatic functions which are not as critical would be the tripping of a breaker to clear a fault. Because many automatic sequences use the data acquired and sent by Input-Output computers, the automation computers and Input-Output computers are generally one single device. This situation is similar to the PLCs (Programmable Logic Controllers) used in other industrial processes, up to the point where PLCs are used by some manufacturers in their SASs.

Substation Computer

The substation computer is in charge of the whole coordination of the bay controllers' performance and other devices in the substation. The substation computer also provides a HMI for the local operation and a communication interface for control dispatching.

1.4 SAS Interfaces

Basically, the most important interfaces in an SAS are the following:

- High voltage devices
- Device to device
- External systems
- Operators
- Maintenance team

1.5 SAS Functions

The goal of an SAS is to control, monitor and protect the primary substation equipment. This task is performed by a number of coordinated functions that can be classified into the following categories:

- System support functions
    - Network management
    - Time synchronisation.
- System configuration and maintenance functions
    - Operator mode control of Logical Nodes
    - Settings
    - Test mode
    - System security management
- Operational and control functions
    - Access security management
    - Operational Control
    - Alarm management and event recording
    - Data retrieval and Disturbance/fault record retrieval
- Local process automation functions
    - Protection function
    - Interlocking
    - Synchronous switching (point-on-wave switching)
    - Measuring, metering and power quality monitoring
    - Breaker failure
    - Load shedding
    - Load restoration
    - Voltage and reactive power control
    - Feeder switchover and transformer tap change
    - Automatic switching sequences

In the IEC-61850 architecture, the SAS functions are implemented using different logical nodes (LN). Every LN represents a fundamental basic function. The LNs that form a function may reside in one or several physical devices.

1.6 SAS Communications

SAS have been traditionally implemented as either centralised or distributed architectures. Centralised systems are generally electrically hardwired or use serial communications to connect the data acquisition units. More recent SASs are implemented with dispersed IEDs which are connected using a proprietary communication network or a network based on an industry standard.

The SAS communication structure chosen has an impact on the performance and reliability of the overall substation. This brochure considers the options for communications technology and gives guidance on those available and which is more appropriate for the function being considered.

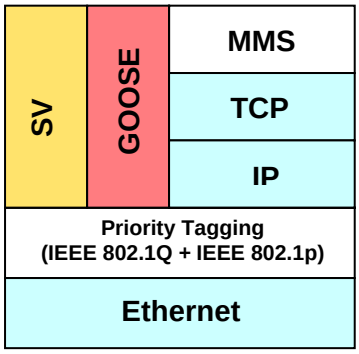
The current recommended standard for SAS communications is IEC 61850. However most utilities are faced with the extension and modification of SAS built to other practices and standards. Therefore choices need to be made on the most appropriate communication method of extending or updating the SAS. This can be carried out by:

- continuing the current SAS communications practice
- adding new bays to the SAS which meet current standards
- replacing the complete SAS

The IEC 61850 standard is focused on the SAS architecture, which considers the interconnection between IEDs at substation level, using standardised local area networks (LANs) and defines object models for substations and feeder equipment. This allows the standardisation of different devices and equipment at the substation, defining a new automation architecture.

The IEC 61850 standard supports the substation automation functions by the communication of sampled values (SVs) for CTs and VTs, fast exchange of I/O data for protection and control, control and trip signals, engineering and configuration, monitoring and supervision, control-center communication, time-synchronisation, etc.

Figure 1.2 shows the communication stack defined in the IEC 61850 standard.



i

Figure 1.2 - Communication Stack

The IEC 61850-7-xx parts explain how the abstract services and models are mapped to concrete communication protocols as defined in IEC 61850-8-1, as is shown in Figure 1.3.

The data transmission between IEDs are accomplished through different types of messages, such as GOOSE (Generic Object Oriented Substation Event) which are used for transmission of critical events in real time such as tripping, commands to operate, etc., and sampled values (SVs), which are encapsulated and transmitted over Ethernet. All other information within the substation is transmitted by means of communication messages between the logical nodes that constitute the functions. The messages are transmitted using the ACSI (Abstract Communication Service Interface) services, which are based on simple communication services provided by the MMS (Manufacturing Messaging Specification) protocol. Underlying the application level with MMS the model uses TCP/IP as transport and network protocols.

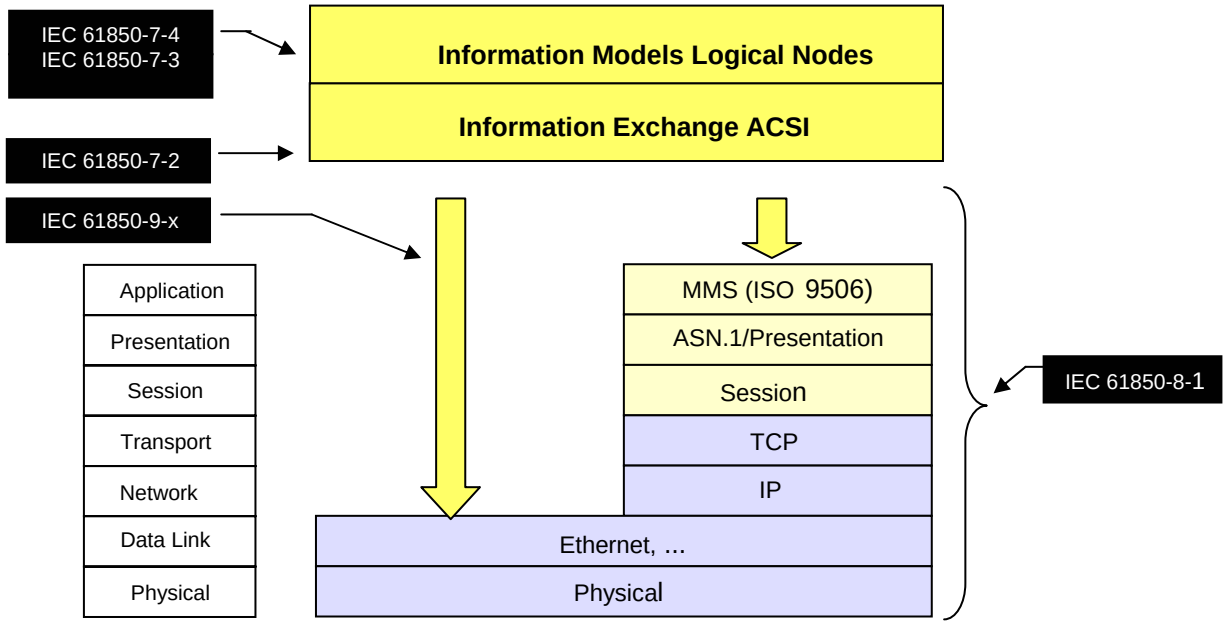


Figure 1.3 - Communication Mapping

IEC 61850-8-1 defines the use of the standard IEEE 802.1pq (VLAN, Priority Tagging). The priority tagging is used to separate the high priority and critical data traffic from the low priority, high volume traffic.

2 Data Exchange Requirements

Chapter 2 classifies Data and Information Flows in Transmission and Distribution Substations. It describes the requirements of source data and information, which has been identified as collected by various utilities in High Voltage Transmission and Distribution electrical substations. The data and information has been classified in a table, with various data type sub-groups, which are collectively defined in terms of a “Lead Application”. The “Lead Application” is the utility business driver for the data or information being collected, traditionally for a prime end user group or an application requirement within the utility business.

2.1 Lead applications

The **Lead Applications** which have been uniquely identified are as follows:

- Station Control
- Data Analysis
- Real Time Protection and Automation Functions
- Substation Automation System (SAS) Management
- Commercial
- Substation Management
- Site Working

- Security

Station Control

This is any control point (within or external to the substation) that provides access to substation "real time" operational data, operational metering data or provides a substation operational control facility. The data types identified are:

Time-stamped indications - These are event driven (spontaneous) changes of state (state of plant, equipment alarms and metering) which have an associated time synchronised time stamp giving the time at which the change occurred. The time stamp can be used to determine the sequence of events.

Non-time stamped indications – These are event driven (spontaneous) changes of state (plant states, equipment alarms and metering) generally used to drive displays and meters at the monitoring point.

Alarms – These are generally associated with abnormal plant and equipment states, which generate an audible warning requiring operator action

Measurements – Cyclic gathering of data, relating to physical or electrical quantities

Commands – Data sent to the substation to alter the state of the operational equipment

Data Analysis

This is data collected and used (generally off-line) either to evaluate events at the substation or to provide confirmation of device configuration. The data types identified are:

Event Reports – typically log files and reports generated by an event recorder or historical system which provide information on the change of state of operational equipment

Oscillograph File Transfer – typically event triggered fault records generated by a protection device or fault recorder. These may contain digital events and analogue waveforms.

Confirmation of Parameters/Setting uploading – data files uploaded to provide information on the actual configuration of a device.

Real Time Protection and Automation Functions

This is data which is transferred between devices in real time to ensure correct protection, operation and substation automation. The data types identified are:

Protection and Protection Initiated Automation – Data and signals used to initiate Circuit Breaker Tripping and high speed reclosure, operating in a timeframe of less than 100ms.

Low Speed Substation Automation – Data and signals used to initiate intra substation applications, which operate in a timeframe of more than 100ms. Management of outages on distribution networks in real time.

Teleprotection – Data and signals sent to remote substations to accelerate, release or block Circuit Breaker tripping. Usually covers the exchange of monitoring and command information to protect operational equipment.

Zone Automation – Data and signals required by automation systems that operate across zones of the transmission system on a wide area inter-substation basis.

Substation Automation System (SAS) Management
This is data required to manage the configuration and performance of the SAS itself. The data types identified are:

SAS Monitoring Data – Supervision data relating to the operational performance, health and condition of the SAS

Configuration downloading – File transfer of site specific application configuration data files or parameter settings

Commercial
This is data collected for the purpose of energy trading and billing or has an impact on the commercial operation of the utility business. The data types identified are:

Revenue Metering Data – This is time integrated Energy Data at a commercial interface or boundary used for energy charging and billing.

Energy Quality – This is data related to agreed quality of service criteria, where energy is transferred at commercial interfaces or boundaries, which could be subject to financial penalties.

Substation Management
This is data collected to monitor plant and equipment condition or relates to environmental factors. The data types identified are:

HV Apparatus Health and Performance – data relating to plant condition and performance, generally used to indicate maintenance requirements, its duty cycle, capability and loading ability

Weather and Environment – data relating to substation environmental factors such as temperature and pollution etc., which may be used to influence utility business decisions.

Site Working
This is data required by site personnel in the execution of site related duties. The data types identified are:

Safety Information – data used by site personnel to ensure that plant and equipment to be maintained is isolated, secured and earthed.

On-Line Documentation – data used by site personnel to carry out their tasks at the substation (e.g. maintenance manuals and schedules, drawings and plans)

Security
Data required to show and prevent threats to the physical substation and unauthorised access. The data types identified are:

Site Video Surveillance – data relating to security systems indicating unauthorised attempts to access or damage

Access Control – data relating to potential threats to the substation communication systems and general configuration data which must be prevented from disclosure, modification or destruction.

2.2 Importance level of communications

In order to identify the “best fit” communications to transport each data or information type from the substation to the user and/or application, certain “Criteria” were been defined. For each “Lead Application“ data type, the impact of the “Criteria” has been weighted according to the following scoring system:

++	High Impact
+	High/Medium Impact
=	Medium Impact
-	Medium/Low
--	Low Impact

2.3 Communications service level criteria

The communications service level “Criteria” which have been identified as having an impact on data and information are:

- Data Loss
- Data Corruption
- Data Disclosure
- Data Delayed
- Response Time
- Volume
- Data Flow
- Data Profile

Data Loss
This is the weighted impact of unintentional loss of data within the communication system for each specific data type.

Data Corruption
This is the weighted impact of data corruption though noisy channels and high Bit Error Rates within the communication system for each specific data type.

Data Disclosure
This the weighted impact of data being unintentionally made available by the communication system outside the utility business for each specific data type.

Data Delayed
This is the weighted impact of data being delayed by the communication system for each specific data type

Response Time
This is the estimated required response time of the communication system required for each specific data type.

Volume
This is an estimate of the amount of data which needs to be transferred for each specific data type.

Data Flow
This indicates the flow of data between substation levels, where 1 is the process or bay level, 2 is the substation level and 3 is remote from the substation “n” indicates that data flows to all levels

Data Profile
This indicates the type or format of the data, which can be:

Event driven (Spontaneously generated and transmitted)
Periodic (Cyclic scanning of data by a master station))
Burst (Record of data generated about a trigger point)
On Demand (User requests data)

Figure 2.1 summarizes Chapter 2, showing the interrelationship between Telecommunications Services Criteria and Lead Applications by means of a matrix.

	Lead Applications		
Telecommunications Services Criteria	+	=	=
	-	+	-
	--	++	-
	++	=	+

Figure 2.1- Lead Applications Matrix

3 Communications Technologies Description

In order to understand the matrices and the methodology followed a reference of modern communication technologies is provided in this chapter for a better comprehension of the next chapter. The concepts explained here appear in the matrices of the following chapters.

3.1 Transmission Media Outside Substations

Fibre

Fibre is the favourite medium to use for high capacity networks. In addition to the huge bandwidth, optical fibres also provide perfect electrical isolation and immunity against electromagnetic interference (EMC) and so are ideally suited to being used as a communications medium serving substations.

The traditional single mode fibres according to ITU-T G.652 recommendation are being replaced more and more by G.655 fibres that are more suited for WDM (Wavelength Division Multiplexing).

Typical applications of G.652 fibres are SDH transport networks working on STM-16 or STM-64 level, while on G.655 fibres DWDM of four to sixteen SDH networks are used.

The investments in optical fibre networks will clearly go on in the future.

More information on the selection of optical fibre cables is found in Cigré Brochure 132 “Optical fibre cable selection for electricity utilities”.

Copper

Copper can take the form of leased line from a public telecommunications operator or be privately owned by the utility.

Copper cables are becoming again attractive to use, thanks to recent techniques like ADSL and SDSL modems. ADSL offers data transfer rates of up to 2 Mbit/s for download and up to 256 kbit/s for upload, and SDSL even promises a symmetrical 2 Mbit/s transfer rate.

Latest development in DSL modem technology is the SHDSL technique based on a new modulation principle called TC-PAM (Trellis Coded Pulse Amplitude Modulation) which promises even higher speeds up to 4.6 Mbit/s over longer distances.

SHDSL looks like to have a bright future on existing copper networks. Also known as G.991.2, G.SHDSL is an international standard for symmetric DSL developed by the ITU. G.SHDSL provides for sending and receiving high-speed symmetrical data streams over a single pair of copper wires at rates between 192 kbps and 2.31 Mbit/s. G.SHDSL was developed to incorporate the features of other DSL technologies, such as ADSL and SDSL and will transport T1,E1, ISDN, ATM and IP signals. This is the first DSL technology to be developed from the ground up as an international standard. G.SHDSL was ratified by the ITU in February 2001.

With copper there is always a strong dependence between speed (data rate) and distance which limits their potential use in Wide-Area Networks. It is important to notice that the theoretical distance may not be achieved in practice due to interference, noise and crosstalk. The application of high-speed copper technologies in the harsh electromagnetic environment of power stations and substations requires most careful engineering, in particular when such systems are expected to operate during faults in the primary system as might be the case for protection applications.

Where a service is leased from a public telecommunications operator, the capacity of the copper will be limited by the fact that the operator will insist on isolation as the cable enters the substation. This is to protect the public equipment from high voltage faults which may occur within the substation. Also the capacity is limited by the equipment installed at the public operator's exchange.

Where the copper is privately owned by the utility then there is a lot more freedom in choosing the terminal equipment and consequently the data carrying capacity can be greater.

When copper cable is used as a communications medium serving substations the issues of isolation of high induced voltages has to be addressed. This isolation requirement seriously impacts the bandwidth that can be provided into a substation.

Radio

Radio links use unguided electromagnetic waves to propagate, thus wireless transport of signals. Recent developments concern both public and private networks. Radio is well suited to being used a communications medium into substations since it can provide high bandwidth and doesn't have the disadvantage of requiring isolation.

Point-to-Point Microwave Radio

Point-to-point microwave radio has been used for many years to provide communications services to transmission stations. Initially analogue system were used but now digital microwave is standard for many applications. Radio still provides a solution where there may be difficulty in providing other infrastructure e.g. fibre or in remote areas where the public telecommunications infrastructure is inadequate. Often radio uses PDH offering bandwidths of 2, 4, 8 or 34 Mbit/s. In more recent times microwave radio systems follow the SDH standards and so can easily be integrated into modern broadband digital networks.

Public Mobile Radio (GSM, GPRS, GSM data)

Normal GSM can provide relatively narrowband data e.g. 9.6 kbits/s. Some networks use multiple frequencies to enable data rates of up to 44 kbits/s to be transmitted. More recently

public operators are currently offering a variety of ‘high bandwidth’ data communication possibilities (up to 56 kbits/s) like high-speed data and GPRS on existing GSM networks. These networks are being rolled out in Europe and many of them give the possibility of roaming facilities between operators or between different countries.

UMTS networks are now being constructed which promise more bandwidth (up to 2Mbits/s but 512kbits/s is more realistic). These networks will enable applications to provide multimedia i.e. voice, data and video services.

Point-to-Multipoint

Recently, to bypass the last mile of the incumbent operators, a technology called point to multipoint radio was introduced; better know as wireless local loop. Here, the operator splits a 2 Mbit/s stream to different clients. The bandwidth is shared by multiple users .

Spread Spectrum

Spread spectrum is a form of wireless communications in which the frequency of the transmitted signal is deliberately varied. This results in a much greater bandwidth than the signal would have if its frequency were not varied. The frequency of the transmitted signal can be deliberately varied over a comparatively large segment of the spectrum. This variation is done according to a specific, but complicated mathematical function. In order to intercept the signal, a receiver must be tuned to frequencies that vary precisely according to this function. The receiver must "know" the frequency-versus-time function employed by the transmitter, and must also "know" the starting-time point at which the function begins. If someone wants to jam a spread-spectrum signal, that person must have a transmitter that "knows" the function and its starting-time point. Most spread-spectrum signals use a digital scheme called frequency hopping. The transmitter frequency changes abruptly, many times each second. Between "hops," the transmitter frequency is stable. The length of time that the transmitter remains on a given frequency between "hops" is known as the dwell time. A few spread-spectrum circuits employ continuous frequency variation, which is an analogue scheme.

Satellite

Using satellites as communication medium is still a niche market for utility applications. Either it is used as a backup to GSM networks, or where GSM networks give no coverage, or when there is no access to the fixed wire network. Many satellite operators offer up to 2 Mbit/s access to the Internet or to VPN LAN’s.

Depending on the application, the use of satellite communication may be prohibited by the inherent signal propagation delay (up/down link) and/or by high cost in case of permanent connections.
Non-stationary low orbit satellites (LEOs) have lower signal propagation delays, however roaming between satellites ascending and descending on the horizon may introduce undesired signal interruptions.

In some cases satellite communication is used for the access of very remote substations for SCADA. Normally special ground terminals are used for this niche application (polling of RTUs).

VSAT (Very Small Aperture Terminal) is a satellite communications system that can serve utilities. Each substation is interconnected with the hub station via the satellite in a star topology. For one substation to communicate with another, each transmission has to first go to the hub station which retransmits it via the satellite to the other end user's VSAT. VSAT handles data, voice, and video signals. Service can be via a service provider who has signed up for a bulk service or by private companies that operate or lease their own VSAT systems.

Satellite telephony. Dedicated satellite rented data and telephony services whether between private user’s groups or to establish connection with public telephony operator worldwide.

Power Line Carrier (PLC)

Power Line Carrier (PLC) systems have traditionally been used for more than 60 years for the transmission of control data (SCADA), protection commands and telephony. PLC systems can bridge very long distances over high-voltage AC or DC transmission lines. Due to the limited transmission capacity and need for more communication, PLC has gradually been complemented or substituted by broadband systems since the availability of long-haul fibre-optic technology

Emerging Digital PLC (DPLC) with increased transmission capacity and advanced networking capabilities opens however new perspectives which will extend the range of PLC applications and facilitates the integration of PLC into modern digital networks.

PLC over high-voltage lines is continued to be used by most electric utilities worldwide, either as a backup system for vital services (protection and control), or where the installation of broadband solutions (fibre, radio) is economically not justified.

3.2 Transmission Media Inside Substations

Multimode Fibre

In optical fibre technology, multimode fibre is optical fibre that is designed to carry multiple light rays or modes concurrently, each at a slightly different reflection angle within the optical fibre core. Multimode fibre has a larger core than single mode multimode fibre transmission is used for relatively short distances because the modes tend to disperse over longer lengths (this is called modal dispersion). Hence it is used within the substation.

The electrical isolation and immunity against electromagnetic interference (EMC) makes fibre ideally suited to being used as a communications medium within substations For longer distances, single mode fibre (sometimes called monomode) fibre is used.

Copper Twisted Pair

Twisted pair is the ordinary copper wire that connects telecom equipment. To reduce crosstalk or electromagnetic induction between pairs of wires, two insulated copper wires are twisted around each other. Normally multiple twisted pairs are contained within the same cable. For some business locations, twisted pair is enclosed in a shield that functions as a ground. This is known as shielded twisted pair (STP). Ordinary wire to the home is unshielded twisted pair (UTP).

Twisted pair comes with each pair uniquely colour coded when it is packaged in multiple pairs. Different uses such as analogue, digital, and Ethernet require different pair multiples. Within substations twisted pair cabling has many uses e.g. telephony for network operational purposes, control wiring between bays and the control building and also within the control building. Due to the noisy electrical environment, electromagnetic interference can occur and balanced interfaces e.g. X.21 are being used to help minimise these effects.

Although twisted pair is often associated with telephony use, a higher grade of twisted pair is often used for horizontal wiring in LAN installations. In recent time cabling such as CAT 5 is used to provide high speed (up to Gigabit/s) LAN access.

Wireless

DECT (Digital Enhanced Cordless Telecommunications) is a digital wireless telephone technology. Formerly called the Digital European Cordless Telecommunications standard because it was developed by European companies, DECT's new name reflects its global

acceptance. DECT uses time division multiple access (TDMA) to transmit radio signals to phones. Whereas GSM is optimized for mobile travel over large areas, DECT is designed especially for a smaller area with users who are mobile within this area e.g. a substation. Dual mode phones are available which are equipped for both GSM and DECT. These can operate seamlessly between the two networks. Consideration needs to be given to the use of DECT equipment within close proximity to high voltage equipment where interference can occur.

Wireless LAN

Wireless LAN is one in which a mobile user can connect to a local area network (LAN) through a wireless (radio) connection. A standard, IEEE 802.11, specifies the technologies for wireless LANs. The standard includes an encryption method, the Wired Equivalent Privacy algorithm. There are currently four specifications in the family: 802.11, 802.11a, 802.11b, and 802.11g. All four use the Ethernet protocol and CSMA/CA (carrier sense multiple access with collision avoidance) for path sharing. The most recently approved standard, 802.11g, offers wireless transmission over relatively short distances at up to 54 Mbits/s compared with the 11 Mbits/s of the 802.11b standard. Like 802.11b, 802.11g operates in the 2.4 GHz range and is thus compatible with it.

The 802.11b standard - often called Wi-Fi - is backward compatible with 802.11. The modulation used in 802.11 has historically been phase-shift keying (PSK). The modulation method selected for 802.11b is known as complementary code keying (CCK), which allows higher data speeds and is less susceptible to interference.

Using modern technology wireless LAN adapters are now available which can fit on a Personal Computer Memory Card Industry Association (PCMCIA) card for a laptop or notebook computer.

Within substations wireless LAN can be deployed, however consideration needs to be given to the location of the receivers since the physical equipment (switchgear, transformers etc.) may lead to propagation difficulties.

Bluetooth

Bluetooth is a computing and telecommunications industry specification that describes how mobile phones, computers, and personal digital assistants (PDAs) can easily interconnect with each other and with business phones and computers using a short-range wireless connection. Using this technology, users of cellular phones, pagers, and personal digital assistants will be able to get quickly synchronized with information in a desktop or notebook computer, initiate the sending or receiving of a fax, initiate a print-out, and, in general, have all mobile and fixed computer devices be totally coordinated.

Bluetooth requires that a low-cost transceiver chip be included in each device. The tranceiver transmits and receives in a previously unused frequency band of 2.45 GHz that is available globally. In addition to data, up to three voice channels are available. Each device has a unique 48-bit address from the IEEE 802 standard. Connections can be point-to-point or multipoint. The maximum range is 10 meters. Data can be exchanged at a rate of up to 2 Mbit/s in the second generation of the technology. A frequency hop scheme allows devices to communicate even in areas with a great deal of electromagnetic interference such as substations. Built-in encryption and verification is provided.

3.3 Communications Methods

Peer to Peer

Peer-to-peer is a communications model in which each party has the same capabilities and either party can initiate a communication session. In some cases, peer-to-peer communications is implemented by giving each communication node both server and client

capabilities. In recent usage, peer-to-peer has come to describe applications in which the Internet is used to exchange files directly or through a mediating server. The number of simultaneous member connections and which files are to be shared or password protected can be specified.

The peer to peer communication environment opens up new opportunities for protection applications in the electrical plant. Traditional protection schemes used hard wires and wired logic to implement the various protection schemes. Peer to Peer communications now allows for information transfer through the use of Remote Inputs and Remote Outputs. Any device can define a Remote Input that is linked to an object in another IED (either local or anywhere on the network). Linkage would be specified by IED address, object name, object type, and security. The requesting device gets access to the desired object either on request, on change of state (or deadband), or periodically. Since plant control requires a high degree of reliability, provision is made to implement redundant communications from the IEDs and subsequently, support for a redundant LAN. In the same way peer-to-peer communications provides opportunities for Bay-to-Bay communications within a substation.

On the Internet, peer-to-peer (referred to as P2P) is a type of transient Internet network that allows groups of computer users with the same networking programs to connect with each other and directly access files from one another's hard drives. This has advantages for SAS to SAS communications, in that relevant information stored at one SAS is easily accessible to another SAS, without the expense and complication of maintaining a centralized server. In this way information is exchanged other directly form SAS to SAS or from SAS to a remote controller.

Master/Slave

In computer networking, master/slave is a model for a communication protocol in which one device or process known as the master controls one or more other devices or processes known as slaves. Only the master can initiate a transaction. - the slaves respond by supplying the requested data to the master, or by taking the action requested. Once the master/slave relationship is established, the direction of control is always from the master to the slaves.

The master controls all activity by selectively polling the slave devices. Some protocols provide for a number of slave devices on a common line. Each device is assigned an address to distinguish it from all other connected devices. The master can address individual slaves or some protocols allow the master to initiate a broadcast message to all slaves. Slaves return a response to messages that are addressed to them individually. Responses are not returned to broadcasts e.g. clock synchronisation from the master.

The master/slave method of communication can be used for hierarchical communications e.g. between the Control Centre and RTUs. In the same way this can be used for Control Centre to SAS and Engineering Office to IED communications. Within the substation the SAS can be the master and the IED the slave.

Client/Server

Client/server describes the relationship between two computer programs in which one, the client, makes a service request from another, the server. The server then fulfils the request. In a network, the client/server model provides a convenient way to interconnect systems that are distributed efficiently across different locations.

The client/server model has become one of the central ideas of network computing. Most business applications being written today use the client/server model. So does the Internet's main program, TCP/IP.

In the usual client/server model one server is activated and awaits client requests. Typically, multiple client programs and PCs share the services of a common server program. Both client programs and server programs are often part of a larger program or application. Requests can in turn be forwarded to its own client program that sends a request to a database server

at another location. This enables remote communications from multiple locations to a single database.

Relative to the Internet, a Web browser is a client program that requests services (the sending of Web pages or files) from a Web server elsewhere on the Internet. Similarly, your computer with TCP/IP installed allows you to make client requests for files from File Transfer Protocol (FTP) servers in other computers on the Internet.

Publish/Subscribe

In a publish/subscribe domain, a single sending application, or publisher, broadcasts a single message to several receiving applications, or subscribers.

Publish/subscribe messaging is useful when you want to broadcast the same information to a wide audience. Sample implementations include stock price tickers, notification of promotional offers, and requests for bids or proposals.

SNMP (Simple Network Management Protocol) Traps are event notifications that SNMP agents send to the management software. The management system records these events so that an overview of the network devices is obtained. Management systems are required for a complex network with many devices, since a large amount of information will be delivered via all the traps that SNMP delivers from the various network devices.

3.4 Communication topology

Point-to-point

This topology connects only two stations by each communication channel or communication link and is the simplest possible.

Figure 3.1 – Point-to-Point

Bus

All stations are attached, through appropriate hardware interfacing, directly to a linear transmission medium, or a bus. A transmission from any station propagates the length of the medium in both directions and can be received by all other stations.

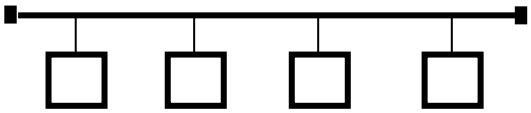


Figure 3.2 – Bus

Star

In this topology each station is connected by point-to-point links to a common central node. There are two alternatives for the operation. One mode is for the central node to operate in broadcast mode. The other is for the central node to act as a switching device.

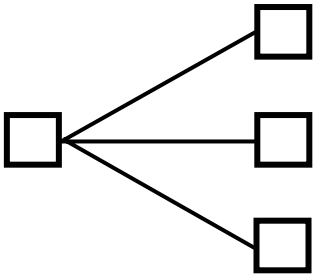


Figure 3.3 – Star

Ring

The communication path between all stations forms a ring. This is a preferred method to improve the availability of the communication path. If the path is interrupted in some location, full communication is maintained, since every station can be reached from two sides of the ring.

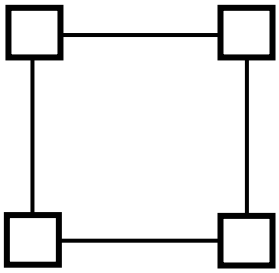


Figure 3.3 – Ring

3.5 Communication technologies

Serial

Serial means one event at a time. In data transmission, the techniques of time division and space division are used, where time separates the transmission of individual bits of information sent serially and space (on multiple lines or paths) can be used to have multiple bits sent in parallel.

In the context of computer hardware and data transmission: serial connection, operation, and media usually indicate a simpler, slower operation and parallel indicates a faster operation. This indication doesn't always hold since a serial medium (for example, fibre optic cable) can be much faster than a slower medium that carries multiple signals in parallel.

Serial communication between equipment and modem or other serial devices adheres to defined standards. An example is the use of RS232C for relatively low speed applications. The actual interface provided by substation equipment manufacturers can vary widely depending on the function of the equipment etc. As examples these interfaces can range from 9600 bits/s on an RS232C interface to 10 Mbits/s on Ethernet connected devices.

Ethernet

Ethernet has become the predominant standard for the Logical Link Control (LLC) and Media Access Control (MAC) in Local Area Networks (LAN).

Although there are several LAN technologies, Ethernet is predominantly being used in the substation environment. With the advent of the UCA (Utility Communications Architecture), 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.

Ethernet, which was developed in the 1970s, was the technological basis for IEEE 802.3 specification, which was initially released in 1980. The differences between Ethernet and IEEE 802.3 LANs are subtle. Today, the term "Ethernet" is often used to refer to all carrier sense multiple access/collision detection (CSMA/CD) LANs that generally conform to Ethernet specifications, including IEEE 802.3.

The most relevant physical interfaces used in the substation environment are:
10/100BASE-TX that uses a 2 pairs UTP (Unshielded Twisted Pairs) category 5 cable in a point-to-point arrangement (star topology)
100BASE-FX that uses an optical fibre (2 strands) in a point-to-point arrangement (star topology)
Gigabit Ethernet, 1000BASE-LX a transmission technology based on the Ethernet frame format and protocol used in local area networks (LANs), provides a data rate of 1 billion bits per second (one gigabit). Gigabit Ethernet is defined in the IEEE 802.3 standard and is currently being used as the backbone in many enterprise networks.

Gigabit Ethernet is carried on optical fibre or on CAT5 cabling using 4 pairs. Existing Ethernet LANs with 10 and 100 Mbps cards can feed into a Gigabit Ethernet backbone. A newer standard, 10-Gigabit Ethernet, is also becoming available.

3.6 Backbone technology

Backbone technology concerns with a high capacity network linking substations and substations with control centres, i.e., it is for communications outside substations.

IP

IP is the protocol used in the Internet. It is not a new technology since it was designed more than 20 years ago but is the most extended and experienced network protocol. In contrast to connection-oriented networks, IP is based on the Datagram connectionless principle.

Connection-oriented networks are based on the circuit-switched approach. Each connection is associated to a circuit that has resources allocated for its exclusive use along a path. There is no uncertainty about the bandwidth or delay along this path so the Quality of Service in terms of Bandwidth and Delay can be guaranteed.

Datagram networks introduced a very different mode of operation. Network resources (bandwidth, buffers, etc.) are statistically shared among their users. This presents many advantages for computer communication applications since data traffic tends to be bursty so that resource reservation would lead to low utilisation levels. In datagram networks, data packets are delivered to the Network without any resource being allocated, and the Network exerts its “best effort” to serve the packets.

In addition to the connectionless working mode, datagram networks are based on the End-to-End paradigm. The responsibilities of maintaining a session are shared between the network and its users. The Network is responsible for the routing whereas the users are responsible for the control of the communication. Thanks to this approach, the Datagram networks present an unmatchable resilience level as well as the best resource optimisation. These

characteristics make them suitable for mission-critical applications such the ones that can be found in Power Utilities Control Networks.

The plain Internet protocol suite cannot guarantee the specific QoS as the network presents a non-deterministic transmission delay. Consequently it cannot be applied to delay sensitive applications unless some specific mechanisms were added in order to guaranty bandwidth and/or delay.

The great flexibility of this type of networks makes them suitable for service integration. Although they cannot intrinsically offer a constant bit-rate service, thanks to the new application protocol that has been defined, it is possible to achieve this functionality at the application level.

IP is a mature technology used in almost every device or service providing connectivity whether in LANs, WAN, the Internet and in the new set of protocols which are under the standardisation process in the TC57 of the IEC.

IP Address

In the most widely installed level (IP V4) of the Internet Protocol (IP) today, an IP address is a 32-bit number that identifies each sender or receiver of information that is sent in packets across the Internet. When you request an HTML page or send e-mail, the Internet Protocol part of TCP/IP includes your IP address in the message (actually, in each of the packets if more than one is required) and sends it to the IP address that is obtained by looking up the domain name in the Uniform Resource Locator you requested or in the e-mail address you're sending a note to. At the other end, the recipient can see the IP address of the Web page requestor or the e-mail sender and can respond by sending another message using the IP address it received.

An IP address has two parts: the identifier of a particular network on the Internet and an identifier of the particular device (which can be a server or a workstation) within that network. On the Internet itself - that is, between the routers that move packets from one point to another along the route - only the network part of the address is looked at.

TCP

TCP (Transmission Control Protocol) is a protocol used along with 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 packets that a message is divided into for efficient routing through the Internet.

For example, when an HTML file is sent from a Web server the Transmission Control Protocol (TCP) program layer in that server divides the file into packets, numbers the packets, and then forwards them individually to the IP program layer. Although each packet has the same destination IP address, it may get routed differently through the network. At the client end TCP reassembles the individual packets and waits until they have arrived to forward them as a single file.

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.

UDP

UDP (User Datagram Protocol) is a communications protocol that offers a limited amount of service when messages are exchanged on a network that uses IP. UDP is an alternative to TCP and, together with IP, is sometimes referred to as UDP/IP. Like TCP, UDP uses the

Internet Protocol to actually get a datagram or data unit from one system to another. Unlike TCP, however, UDP does not provide the service of dividing a message into packets 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.

IP version 6

IP version 6 (IPv6) is the new version of the Internet Protocol, designed as a successor to IP version 4 (IPv4) [RFC-791]. The changes from IPv4 to IPv6 fall primarily into the following categories:

Expanded Addressing Capabilities
IPv6 increases the IP address size from 32 bits to 128 bits, to support more levels of addressing hierarchy, a much greater number of addressable nodes and simpler auto-configuration of addresses.

Header Format Structure
The structure of the header has been redefined to make it more regular which is easier to decode but longer than IPv4.

Improved Support for Extensions and Options
Changes in the way IP header options are encoded allows for more efficient forwarding, less stringent limits on the length of options, and greater flexibility for introducing new options in the future.

Flow Labelling Capability
A new capability is added to enable the labelling of packets belonging to particular traffic "flows" for which the sender requests special handling, such as non-default quality of service or "real-time" service.

Authentication and Privacy Capabilities
Extensions to support authentication, data integrity, and (optional) data confidentiality are specified for IPv6.

Although IPv6 was specified back in 1992 it has not been widely deployed in the Internet due to its total incompatibility with the existing IPv4. Despite the fact that there is a lack of address space in the Internet, a number of auxiliary mechanisms have been developed to cope with these drawbacks.

ATM

Asynchronous Transfer Mode is a means of digital communication that is capable of very high speeds. It is used for the transport of voice, video, data and images as well as for providing broadband advanced services.

The ATM technology was formerly standardise by the ATM Forum working in a coordinated way with the IETF (Internet Engineering Task Force) and later adopted by the ITU-T as the base for the Broadband ISDN network. Although ATM could be used in every part of the network, from the access to the core, it is in the backbone where it is mostly used. 80% of the service providers in the world have ATM backbones. One of the reasons for this situation in

the capacity of ATM of accommodating different classes of services, the resource optimisation achieved thanks to the use of statistical multiplexing and the QoS guarantees that can be provided.

ATM can be considered where high speed and capacity are required e.g. for communication between the substation and the Control Centre.

Frame Relay

Frame relay is a telecommunication service designed for cost-efficient data transmission for intermittent traffic between local area networks (LANs) and between end-points in a wide area network (WAN). Frame relay puts data in a variable-size unit called a frame and leaves any necessary error correction (retransmission of data) up to the end-points, which speeds up overall data transmission. For most services, the network provides a permanent virtual circuit (PVC), which means that there is continuous, dedicated connection. An enterprise can select a level of service quality - prioritizing some frames and making others less important. Frame relay is generally offered by service providers.

Frame relay is a fast packet technology, which means that the protocol does not attempt to correct errors. When an error is detected in a frame, it is simply "dropped." (thrown away). The end points are responsible for detecting and retransmitting dropped frames.

Frame relay is often used to connect local area networks with major backbones as well as on public wide area networks and also in private network environments with leased lines over leased lines. It requires a dedicated connection during the transmission period.

Frame relay relays packets at the Data Link layer of the Open Systems Interconnection (OSI) model rather than at the Network layer. A frame can incorporate packets from different protocols such as Ethernet. It is variable in size and can be as large as a thousand bytes or more.

Frame relay is suitable where mid to high capacity bandwidth is required across a wide area network e.g. from the substation to the maintenance centre.

SDH / SONET

The rapid growth of digital networks and the integration of high-speed data services have enforced the development of new standards, which would facilitate the deployment of large networks with comprehensive network management facilities. The new standard appeared first as SONET (Synchronous Optical Network) in the United States. Subsequently, the ITU-T (former CCITT) was approached with the goal of developing this proposal into a worldwide standard. This goal was finally achieved in 1988 with the adoption of the SDH (Synchronous Digital Hierarchy) standards.
While there are commonalties between SDH and SONET, particularly at the higher rates, there are significant differences at the lower multiplexing levels.

The ITU-T recommendations define a number of basic transmission rates within the SDH and SONET, see table below, with further levels proposed for study.

SDH		SONET			
Synchronous Transport Module level	***Aggregate Rate***	***Optical Carrier level***	***Synchronous Transport Signal level***	***Aggregate Rate***	***Max. number of simultaneous voice channels***
		OC-1	STS-1	51.840 Mbit/s	783
STM-1	155.520 Mbit/s	OC-3	STS-3	155.520 Mbit/s	2'349
STM-4	622.080 Mbit/s	OC-12	STS-12	622.080 Mbit/s	9'396
STM-16	2’488.320 Mbit/s	OC-48	STS-48	2’488.320 Mbit/s	37'584
STM-64	9’953.280 Mbit/s	OC-192	STS-192	9’953.280 Mbit/s	150'336

Table 3.1 – SDH/SONET

The recommendations also define a multiplexing structure whereby an STM-N (Synchronous Transport Module level N in SDH terminology) or STS-N (Synchronous Transport Signal level N in SONET terminology) aggregate can carry a number of lower bitrate signals as payload to facilitate the transport of legacy PDH tributaries.

SDH is expected to dominate backbone transmission networks for years to come. It offers carrier-class reliability, short restoration times of < 50 ms in case of path failures and provides transport for different types of traffic and services.

Modern SDH platforms pave the way to transform a rigid, voice-oriented network to a universal transport mechanism for voice and data, allowing operators to increase capacity as needed and to adopt a highly flexible investment strategy.

Since its introduction, SDH has been adopted worldwide by many Electric Utilities for both fiber and microwave radio systems. It is today considered the standard technology for transport networks, offering the requested Quality of Service for demanding real-time applications and mission critical services.

MPLS

Multiprotocol Label Switching (MPLS) provides a mechanism for engineering network traffic patterns that is independent of routing tables. MPLS assigns short labels to network packets that describe how to forward them through the network. MPLS is independent of any Layer 3 network protocol and can be used for unicast packets, although is mostly used with IP.

In the traditional Level 3 forwarding paradigm, as a packet travels from one router to the next, an independent forwarding decision is made at each hop. The IP network layer header is analyzed, and the next-hop is chosen based on this analysis and on the information in the routing table. In an MPLS environment, the analysis of the packet header is performed just once, when a packet enters the MPLS cloud. The packet then is assigned to a stream, which is identified by a label, which is a short (20-bit), fixed-length value at the front of the packet. Labels are used as lookup indexes into the label forwarding table. For each label, this table stores forwarding information. You can associate additional information with a label—such as class-of-service (CoS) values—that can be used to prioritize packet forwarding.

3.7 Data Security

Data security mechanisms are required to prevent security threats such as data disclosure, data corruption, and denial of service. Annex B describes security threats and the available technologies to prevent these attacks. The following paragraphs describe the preventive methods which can be used to control security threats.

Encryption

Encryption is the conversion of data into a form, called a ciphertext, that cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it can be understood.
Simple ciphers include the substitution of letters for numbers, the rotation of letters in the alphabet, and the "scrambling" of voice signals by inverting the sideband frequencies. More complex ciphers work according to sophisticated computer algorithms that rearrange the data bits in digital signals.
In order to easily recover the contents of an encrypted signal, the correct decryption key is required. The key is an algorithm that "undoes" the work of the encryption algorithm. Alternatively, a computer can be used in an attempt to "break" the cipher. The more complex the encryption algorithm, the more difficult it becomes to eavesdrop on the communications without access to the key.
Encryption/decryption is especially important in wireless communications. This is because wireless circuits are easier to "tap" than their hard-wired counterparts. The stronger the cipher -- that is, the harder it is for unauthorized people to break it -- the better, in general. However, as the strength of encryption/decryption increases, so does the cost.

Authentication

It is the process of determining whether someone or something is, in fact, who or what it is declared to be. In private and public computer networks (including the Internet), authentication is commonly done through the use of logon passwords. Knowledge of the password is assumed to guarantee that the user is authentic. Each user registers initially (or is registered by someone else), using an assigned or self-declared password. On each subsequent use, the user must know and use the previously declared password. The weakness in this system for transactions that are significant (such as the exchange of money) is that passwords can often be stolen, accidentally revealed, or forgotten.
For this reason, Internet business and many other transactions require a more stringent authentication process. The use of digital certificates issued and verified by a Certificate Authority as part of a public key infrastructure is considered likely to become the standard way to perform authentication on the Internet.
Logically, authentication precedes authorization (although they may often seem to be combined).

4 Communications and Applications Matrix

This chapter analyses the impact of each technology described in the previous chapter over criteria described in Chapter 2: positive, negative or special comments. Figure 4.1 shows the interrelationship between Communications Technologies and Telecommunications Service criteria by means of a matrix.

	Telecommunications Service Criteria		
Communications Technologies	P	P	P
	N	C	C
	P	P	N
	N	N	N

Figure 4.1 – Communications and Applications Matrix

4.1 Methodology

The methodology used to produce the output matrix is based on the categorisation of the elements in the data flow matrix to show their relative importance. The matrix elements are weighted according to their relevance to the application. Each element is converted to a number according to the following table:

IMPACT		RESPONSE TIME		VOLUME		DATA FLOW		PROFILE	
WEIGHTED VALUE	**GRADE**	**WV**	**GRADE**	**WV**	**GRADE**	**WV**	**TYPE**	**WV**	**TYPE**
10	++	10	milliseconds	10	several Mbytes	10	Multidir p-t-p	10	event-driven
8	+	5	seconds	7	hundreds of kbytes	8	Unidir p-t-p	8	periodic or event driven
6	=	2	minutes	5	several kbytes	3	Multidir p-t-mp	5	burst or on demand
4	-	1	hours	2	a hundred bytes	1	Unidir p-t-mp	3	periodic
1	--			1	a few bytes			1	on demand
1	P								
-1	N								
0	C								
0	---								

Table 4.2 – Conversion Matrix

5 Cross Working Matrices. Result

The next step is to multiply both matrices cell by cell and add all the elements of each row to obtain the final classification.

	Telecommunications Services Criteria		
Communications Technologies	P	P	P
	N	C	C
	P	P	N
	N	N	N

X

	Lead Applications		
Telecommunications Services Criteria	+	=	=
	-	+	-
	--	++	-
	++	=	+

=

	Lead Applications
Communications Technologies	Results

Figure 5.1 – Cross Working Matrices

Having done this process, the average value for every lead application is calculated. Then the most and least appropriate technology is chosen for each lead application.

6 Conclusions

The following table summarises the result of the process and provides a comparison of the recommended communication technology for every lead application.

	STATION CONTROL	DATA ANALYSIS	REAL TIME PROTECTION & AUTOMATION	SAS MANAGEMENT
Transmission Media outside Substations				
RECOMMENDED	FIBRE	FIBRE	FIBRE	FIBRE
NOT RECOMMENDED	SATELLITE	GSM	SATELLITE	SATELLITE
Transmission Media inside Substations				
RECOMMENDED	FIBRE	FIBRE	FIBRE	FIBRE
NOT RECOMMENDED	TWISTED PAIR	DECT	TWISTED PAIR	T. P. & DECT
Communication Methods				
RECOMMENDED	PUBLISH/SUBSC.	MASTER/SLAVE	PUBLISH/SUBSC.	MS & PS
NOT RECOMMENDED	CLIENT/SERVER	PEER-TO-PEER	CLIENT/SERVER	CLIENT/SERVER
Communication Topology				
RECOMMENDED	BUS	BUS	BUS	BUS
NOT RECOMMENDED	RING	RING & STAR	RING	RING
Communication Technologies				
RECOMMENDED	ETHERNET	ETHERNET	ETHERNET	ETHERNET
NOT RECOMMENDED	SERIAL	SERIAL	SERIAL	SERIAL
Backbone technology				
RECOMMENDED	TCP/IP&ATM&SDH	ATM & SDH	ATM & SDH	ATM & SDH
NOT RECOMMENDED	UDP	FRAME RELAY	FRAME RELAY	FRAME RELAY
Security				
MOST EFFECTIVE	DATA ENCRIPTION	DATA ENCRIPTION	DATA ENCRIPTION	DATA ENCRIPTION
LEAST EFFECTIVE	AUTHENTICATION	AUTHENTICATION	AUTHENTICATION	AUTHENTICATION

	COMMERCIAL	S/S MANAGEMENT	SITE WORKING	SECURITY
Transmission Media outside Substations				
RECOMMENDED	FIBRE	FIBRE	FIBRE	FIBRE
NOT RECOMMENDED	GSM	GSM	GSM	SATELLITE & GSM
Transmission Media inside Substations				
RECOMMENDED	FIBRE	FIBRE	FIBRE	FIBRE
NOT RECOMMENDED	DECT	BLUETOOTH	T. P. & DECT	T. P. & DECT
Communication Methods				
RECOMMENDED	MS & PS	PUBLISH/SUBSC.	MS & PS	MASTER/SLAVE
NOT RECOMMENDED	C/S & P-T-P	C/S & P-T-P	PEER-TO-PEER	C/S & P-T-P
Communication Topology				
RECOMMENDED	BUS	BUS	BUS	BUS
NOT RECOMMENDED	RING & STAR	RING	STAR	STAR
Communication Technologies				
RECOMMENDED	ETHERNET	ETHERNET	ETHERNET	ETHERNET
NOT RECOMMENDED	SERIAL	SERIAL	SERIAL	SERIAL
Backbone technology				
RECOMMENDED	ATM & SDH	ATM & SDH	ATM & SDH	ATM & SDH
NOT RECOMMENDED	FRAME RELAY	FRAME RELAY	FRAME RELAY	FR & UDP
Security				
MOST EFFECTIVE	DATA ENCRIPTION	DATA ENCRIPTION	DATA ENCRIPTION	DATA ENCRIPTION
LEAST EFFECTIVE	AUTHENTICATION	AUTHENTICATION	AUTHENTICATION	AUTHENTICATION

Table 6.1 – Methodology result and comparison of communication technologies for lead applications

To summarise the output of the table, the state of the art for communication technologies for supporting SAS applications is fibre, Ethernet, bus topology, ATM/SDH using publish/subscribe or master/slave communication methods.

The table shows that fibre is the recommended medium both outside and inside the substation. However this does not take cost into account, which may be a consideration in substation deployment. If a more cost effective medium is chosen, its performance can be evaluated from the data in the more detailed matrix in Annex A. However radio or copper are not recommended as transmission medium e.g. Satellite is not recommended for long haul and twisted pair is not recommended for short haul communications.

Inside the substation a bus topology implemented via Ethernet is the recommended option. Compared with bus/Ethernet topology, serial and ring do not give the same performance within the substation.

For the backbone ATM/SDH is the recommended technology. Generally Frame Relay is not the preferred approach.

Nowadays security is an important consideration in substation design. Data encryption appears to be the most effective single measure. Authentication on its own is not as effective and it is recommended that both be used. Implementation of security measures has negative performance implications for substation operation because of the increased communication overhead.

The methodology used in this work is flexible and extendable and allows new technologies to be introduced and compared with the current communications options. This is a powerful approach to assess the new communication technologies prior to adoption. The detail in the matrices allows alternative communication technologies to be assessed against the recommendations for a specific utility application.

Future work could consider relative costs of communication technologies to widen the scope of the work. This would enable utilities to make choices on the most cost effective and appropriate technology for a particular application.

7 References

[1 International Electrotechnical Commission *"IEC 61850-3. Communications networks and systems in substations – Part 3 General requirements"*, January 2002.

[2] Misha Schwartz, "*Telecommunication Networks: Protocols, Modeling, and Analysis*", Reading, MA: Addison-Wesley, 1987.

[3] Cisco Systems, "*Internetworking Technologies Handbook*", Cisco Press, 2004.

[4] D. Awduche, J. Malcolm, M. O'Dell and J. McManus. RFC 2702, "*Requirements for Traffic Engineering Over MPLS*", September 1999.

Annexes

A. MATRICES

This matrix characterises the data flows for each of the lead applications against specific criteria e.g. response time for time-stamped applications.

Characterization of data flows : data types & criteria

Application	Station Control (Note a)					Data analysis		
Criteria / Data Type	Time-stamped indications	Non Time-stamped indications (Note b)	Alarms	Measurements	Commands	Event reports	Oscillography file transfer	Configuration / Parameters / Settings uploading
Impact of data loss [1]	-	+	+	-	+	-		
Impact of data corruption [1]	=	+	+	+	++	+		
Impact of data disclosure	++	++	-	-	+	-		
Impact of data delayed [1]	--	-	=	-	+	--		
Response time	1 to 3s	1 to 3s	1 to 3s	1 to 10s [2]	0.5 to 3s	on demand a few minutes automatic: hours acceptable		
Volume	100 events configured per bay	10 to 20 per bay	15 to 50 alarms configured for a feeder bay	2 to 5 measurements configured for a feeder bay	a few bytes	up to a hundred infos per fault and 1 info < 80 bytes	1 to 3 files per fault 1 file = several 10 kbytes	Around 100 kbytes per bay
Data flow [5]	1 -> 2, 2 -> 3 1 -> 3	1 -> 2, 2 -> 3 1 -> 3	1 -> 2, 2 -> 3 1 -> 3	1 -> 2, 2 -> 3 1 -> 3	3 -> 1,2 2 -> 1	1 -> 2,3 2 -> 3	1 -> 2, 3	1 -> 2,3
Data profile [6]	event-driven	event-driven	event-driven	periodic every 10s [2]	event-driven	burst or on demand		

[1] not considering if it is the result of an intentional attack or a malfunction
[2] depending on the time interval between reports
[3] even slower for earth-resistant protections
[4] whether the automaton is time-critical (single phase recloser) or not (slow station-level automaton for switchgear interlocking)
[5] 1 is bay level, 2 is station level, 3 is remote level
[6] data profile : burst / periodical / event-driven / on-demand

[7] for a typical feeder bay : 2 measurements (P active and Q reactive power) with a report every 10s
[8] a few infos for a bay-level automaton - up to hundreds of infos for a station-wide automaton

Note a: Station control applies to any point that controls all the substation, irrespective of where it is (in or out of the substation)

Note b: Non-time stamped indications are indications presented through a mimic board or any type of graphic form

Note c: Load sheddind, Power shedding, System stability Control

Safety information: exchange of procedure progress to de-energize a circuit

Application	Real-time protection & automation functions (tripping, inter-locking, reclosing, …)				SAS Management	
Criteria / Data Type	Protection & Protection-initiated automation	Low-speed S/S automations	Teleprotection	Zone Automation (Note c)	SAS monitoring data	Configuration (downloading)
Impact of data loss [1]	++	+	++	+	+	-
Impact of data corruption [1]	++	+	++	+	+	++
Impact of data disclosure	+	=	--	-	=	+
Impact of data delayed [1]	++	+	++	=	--	--
Response time	5 to 50ms [3]	300ms to a few seconds [4]	1 to 100 ms	a few seconds	a few seconds	downloading : a few seconds activation : a few seconds
Volume	a few bytes	5 to tens bytes	a few bytes	a few kbytes	up to a hundred bytes for a complex failure	several kbytes
Data flow [5]	1 <-> 1, 2	1 <-> 1, 2, 3	1<->1	2 <-> 3	1,2 -> 3 1,2 -> 2	2,3 -> 1 3 -> 2
Data profile [6]	event-driven		event-driven	event-driven	event-driven	on demand

Application	Commercial		S/S management	
Criteria / Data Type	Revenue metering data	Energy quality	HV apparatus health & performance	Weather / Environment
Impact of data loss [1]	=	-	--	--
Impact of data corruption [1]	+	-	-	--
Impact of data disclosure	++	=	-	--
Impact of data delayed [1]	=	--	--	--
Response time	on request : a few minutes	up to half an hour	minutes	up to 1 hour
Volume	several kbytes	hundreds of kbytes	a few kbytes	a few kbytes
Data flow [5]	1 -> 3	1 -> 3	1->3	1->3
Data profile [6]	periodical	burst or on demand	periodical or event-driven	periodical or event-driven

Application	Site Working		Security	
Criteria / Data Type	Safety information	On-line documentation	Site video surveillance	Access Control
Impact of data loss [1]	+	-	+	+
Impact of data corruption [1]	++	-	+	++
Impact of data disclosure	-	=	-	++
Impact of data delayed [1]	=	--	=	-
Response time	1 minute	up to half an hour	up to 1 minute	up to 1 minute
Volume	several kbytes	several Mbytes	several Mbytes	a few bytes to 1 kbyte
Data flow [5]	2 <-> 2 2 <-> 3	3 -> 2	2 -> 3	3 <-> 2
Data profile [6]	on demand	on demand	on demand	on demand

This matrix describes the characteristics of the communications technologies in terms of positive, negative or neutral effect on the communication criteria. Specific concerns are also indicated.

	Data Loss	Data Corruption	Data Disclosure	Data Delay	Response Time	Volume	Data Flow	Data Profile
Transmission Media outside Substations								
Fiber	----	P	P	P	P	P	P	----
Copper	----	N	N	N	N	N	P	----
Radio								
Point-to-point Microwaves (PDH/SDH)	N	N	N	P	P	P	P	----
GSM, GPRS, GSM Data	N	N	N	C1	C1	N	N	C2
Point-to-Multipoint	N	N	N	C1	C1	----	P	----
Spread spectrum	N	N	P	C1	C1	N	----	----
Satellite	N	N	N	N	N	----	N	----
High Voltage PLC	N	N	P	N	N	N	N	----
Transmission Media inside Substations								
Fiber	----	P	P	P	P	P	P	----
Copper								
Twisted pair	----	N	----	N	N	N	P	----
Ethernet (UTP)	----	P	P	P	P	P	N	----
Wireless								
DECT telephony	N	N	N	P	P	N	P	----
Wireless LAN	P	N	N	C1	C1	P	P	----
Bluetooth	----	P	P	P	P	N	N	----
Communication Methods								
Peer-to-Peer	N	----	----	P	P	N	----	----
Master/Slave	P			N	N	P		
Client/Server	N	----	----	N	N	P		
Publish/Subscribe	N	----	----	P	P	P		
Communication Topology								
Point to Point	N	----	----	----	P	----	P	----
Bus	P	----	----	----	P	----	P	----
Star	N	----	----	----	P	----	N	----
Ring	----	----	----	----	N	----	N	----
Communication Technologies								
Serial	N	N	N	N	N	N	N	----
Ethernet	----	----	N	C1	----	P	P	----
Backbone technology								
TCP/IP	P	P	----	C1	C1	----	----	----
UDP/IP	N	----	----	C	P	----	----	----
MPLS	----	----	----	P	P	P	----	----
ATM	----	----	----	P	P	P	P	----
Frame Relay	P	P	----	N	N	N	N	----
SDH/SONET/DWDM	----	----	----	P	P	P	P	----
Security								
Data Encryption	----	----	P	N	N	N	----	----
Authentication	----	----	P	N	N	N	N	----

CONSIDERATIONS	
C1	Non-deterministic delay. It Could change for every connection
C2	Connection-oriented service does not match all data profiles

The following tables show the outputs for each of the lead applications, showing in green the highest values and in red the lowest values for each category.

	Station Control					AVERAGE STATION CONTROL
	Time-stamped indications	Non Time-stamped indications	Alarms	Measurements	Commands	
Transmission Media outside Substations						
Fiber	28	31	27	25	40	30,2
Copper	-26	-29	-25	-23	-24	-25,4
Radio						
Point-to-point Microwaves (PDH/SDH)	-8	-13	-5	-3	-4	-6,6
GSM, GPRS, GSM Data	-26	-30	-24	-20	-35	-27
Point-to-Multipoint	-19	-25	-19	-15	-18	-19,2
Spread spectrum	-5	-9	-15	-11	-11	-10,2
Satellite	-27	-36	-32	-26	-47	-33,6
High Voltage PLC	-12	-19	-27	-21	-32	-22,2
Transmission Media inside Substations						
Fiber	28	31	27	25	40	30,2
Copper						
Twisted pair	-16	-19	-21	-19	-16	-18,2
Ethernet (UTP)	26	29	25	23	24	25,4
Wireless						
DECT telephony	-18	-19	-11	-9	-6	-12,6
Wireless LAN	-6	-6	0	-4	-1	-3,4
Bluetooth	16	23	19	17	22	19,4
Communication Methods						
Peer-to-Peer	-3	-2	0	2	4	0,2
Master/Slave	3	2	0	-2	-4	-0,2
Client/Server	-5	-14	-16	-10	-20	-13
Publish/Subscribe	7	4	6	8	6	6,2
Communication Topology						
Point to Point	2	-2	-2	2	5	1
Bus	10	14	14	10	21	13,8
Star	0	-4	-4	0	-11	-3,8
Ring	-6	-6	-6	-6	-13	-7,4
Communication Technologies						
Serial	-32	-39	-35	-29	-48	-36,6
Ethernet	-4	-6	0	0	1	-1,8
Backbone technology						
TCP/IP	10	16	16	12	18	14,4
UDP/IP	1	-3	-3	1	-3	-1,4
MPLS	11	12	14	12	14	12,6
ATM	12	13	15	13	22	15
Frame Relay	-2	3	1	-1	-4	-0,6
SDH/SONET/DWDM	12	13	15	13	22	15
Security						
Data Encryption	-1	-2	-10	-8	-6	-5,4
Authentication	-2	-3	-11	-9	-14	-7,8

	Data analysis			AVERAGE DATA ANALYSIS
	Event reports	Oscillography file transfer	Configuration / Parameters / Settings uploading	
Transmission Media outside Substations				
Fiber	28	25	30	27,67
Copper	-12	-9	-14	-11,67
Radio				
Point-to-point Microwaves (PDH/SDH)	0	-3	2	-0,33
GSM, GPRS, GSM Data	-29	-26	-31	-28,67
Point-to-Multipoint	-8	-8	-8	-8,00
Spread spectrum	-13	-10	-15	-12,67
Satellite	-27	-27	-27	-27,00
High Voltage PLC	-24	-21	-26	-23,67
Transmission Media inside Substations				
Fiber	28	25	30	27,67
Copper				
Twisted pair	-8	-5	-10	-7,67
Ethernet (UTP)	12	9	14	11,67
Wireless				
DECT telephony	-10	-7	-12	-9,67
Wireless LAN	5	2	7	4,67
Bluetooth	2	5	0	2,33
Communication Methods				
Peer-to-Peer	-6	-3	-8	-5,67
Master/Slave	6	3	8	5,67
Client/Server	-2	-5	0	-2,33
Publish/Subscribe	4	1	6	3,67
Communication Topology				
Point to Point	6	6	6	6,00
Bus	14	14	14	14,00
Star	-10	-10	-10	-10,00
Ring	-10	-10	-10	-10,00
Communication Technologies				
Serial	-32	-29	-34	-31,67
Ethernet	9	6	11	8,67
Backbone technology				
TCP/IP	12	12	12	12,00
UDP/IP	-2	-2	-2	-2,00
MPLS	8	5	10	7,67
ATM	16	13	18	15,67
Frame Relay	-4	-1	-6	-3,67
SDH/SONET/DWDM	16	13	18	15,67
Security				
Data Encryption	-4	-1	-6	-3,67
Authentication	-12	-9	-14	-11,67

	Real-time protection & automation functions (tripping, inter-locking, reclosing, …)				AVERAGE R.T. PROT & AUT.
	Protection & Protection-initiated automation	Low-speed S/S automations	Teleprotection	Zone Automation (Note c)	
Transmission Media outside Substations					
Fiber	42	32	42	36	38,00
Copper	-36	-26	-22	-16	-25,00
Radio					
Point-to-point Microwaves (PDH/SDH)	-4	-4	10	4	1,50
GSM, GPRS, GSM Data	-32	-27	-32	-33	-31,00
Point-to-Multipoint	-25	-19	-11	-10	-16,25
Spread spectrum	-13	-12	-20	-15	-15,00
Satellite	-51	-38	-51	-41	-45,25
High Voltage PLC	-36	-28	-50	-36	-37,50
Transmission Media inside Substations					
Fiber	42	32	42	36	38,00
Copper					
Twisted pair	-28	-20	-21	-12	-20,25
Ethernet (UTP)	36	26	22	16	25,00
Wireless					
DECT telephony	-6	-8	8	-2	-2,00
Wireless LAN	-4	-1	10	9	3,50
Bluetooth	34	22	20	10	21,50
Communication Methods					
Peer-to-Peer	9	3	9	0	5,25
Master/Slave	-9	-3	-9	0	-5,25
Client/Server	-29	-19	-29	-16	-23,25
Publish/Subscribe	11	7	11	6	8,75
Communication Topology					
Point to Point	3	0	10	7	5,00
Bus	23	16	30	23	23,00
Star	-3	-6	-10	-13	-8,00
Ring	-13	-8	-20	-15	-14,00
Communication Technologies					
Serial	-52	-40	-52	-44	-47,00
Ethernet	-4	-1	10	9	3,50
Backbone technology					
TCP/IP	20	16	20	16	18,00
UDP/IP	0	-3	0	-3	-1,50
MPLS	21	15	21	14	17,75
ATM	24	18	31	24	24,25
Frame Relay	-4	-2	-11	-8	-6,25
SDH/SONET/DWDM	24	18	31	24	24,25
Security					
Data Encryption	-13	-9	-20	-10	-13,00
Authentication	-16	-12	-30	-20	-19,50

	SAS Management		AVERAGE SAS MANAGNT	Commercial		AVERAGE COMMERCIAL
	SAS monitoring data	Configuration (downloading)		Revenue metering data	Energy quality	
Transmission Media outside Substations						
Fiber	30	37	33,5	39	28	33,5
Copper	-14	-21	-17,5	-23	-12	-17,5
Radio						
Point-to-point Microwaves (PDH/SDH)	-6	-3	-4,5	-3	4	0,5
GSM, GPRS, GSM Data	-32	-35	-33,5	-37	-29	-33
Point-to-Multipoint	-14	-14	-14	-16	-6	-11
Spread spectrum	-12	-11	-11,5	-9	-9	-9
Satellite	-36	-36	-36	-40	-25	-32,5
High Voltage PLC	-26	-25	-25,5	-25	-20	-22,5
Transmission Media inside Substations						
Fiber	30	37	33,5	39	28	33,5
Copper						
Twisted pair	-8	-13	-10,5	-13	-6	-9,5
Ethernet (UTP)	14	21	17,5	23	12	17,5
Wireless						
DECT telephony	-10	-13	-11,5	-13	-10	-11,5
Wireless LAN	4	-1	1,5	1	9	5
Bluetooth	10	11	10,5	13	-2	5,5
Communication Methods						
Peer-to-Peer	-4	-3	-3,5	-3	-8	-5,5
Master/Slave	4	3	3,5	3	8	5,5
Client/Server	-12	-5	-8,5	-9	0	-4,5
Publish/Subscribe	0	7	3,5	7	6	6,5
Communication Topology						
Point to Point	5	9	7	4	6	5
Bus	21	17	19	16	14	15
Star	-11	-7	-9	-12	-10	-11
Ring	-13	-13	-13	-10	-10	-10
Communication Technologies						
Serial	-38	-41	-39,5	-45	-32	-38,5
Ethernet	4	5	4,5	3	9	6
Backbone technology						
TCP/IP	16	14	15	14	8	11
UDP/IP	-3	1	-1	-4	-2	-3
MPLS	8	11	9,5	13	10	11,5
ATM	16	19	17,5	21	18	19,5
Frame Relay	0	-5	-2,5	-7	-10	-8,5
SDH/SONET/DWDM	16	19	17,5	21	18	19,5
Security						
Data Encryption	-2	-3	-2,5	-3	-4	-3,5
Authentication	-10	-11	-10,5	-11	-12	-11,5

	S/S management		AVERAGE S/S MANAGEMNT	Site Working		AVERAGE SITE WORKING	Security		AVERAGE SECURITY
	HV apparatus health & perfomance	Weather / Environment		Safety information	On-line documentation		Site video surveillance	Access Control	
Transmission Media outside Substations									
Fiber	22	15	18,5	37	31	34	38	39	38,5
Copper	-6	1	-2,5	-17	-15	-16	-22	-19	-20,5
Radio									
Point-to-point Microwaves (PDH/SDH)	5	10	7,5	1	7	4	6	-9	-1,5
GSM, GPRS, GSM Data	-20	-14	-17	-37	-32	-34,5	-38	-41	-39,5
Point-to-Multipoint	-1	5	2	-12	-6	-9	-12	-18	-15
Spread spectrum	-4	-4	-4	-19	-12	-15,5	-22	-11	-16,5
Satellite	-20	-13	-16,5	-40	-25	-32,5	-36	-44	-40
High Voltage PLC	-15	-14	-14,5	-37	-23	-30	-38	-27	-32,5
Transmission Media inside Substations									
Fiber	22	15	18,5	37	31	34	38	39	38,5
Copper									
Twisted pair	-2	2	0	-13	-9	-11	-18	-9	-13,5
Ethernet (UTP)	6	-1	2,5	17	15	16	22	19	20,5
Wireless									
DECT telephony	-1	4	1,5	-9	-13	-11	-14	-15	-14,5
Wireless LAN	4	10	7	9	12	10,5	14	1	7,5
Bluetooth	0	-7	-3,5	7	-5	1	2	13	7,5
Communication Methods									
Peer-to-Peer	-1	-2	-1,5	-5	-11	-8	-10	-5	-7,5
Master/Slave	1	2	1,5	5	11	8	10	5	7,5
Client/Server	-1	0	-0,5	-11	3	-4	-6	-11	-8,5
Publish/Subscribe	5	4	4,5	5	9	7	10	1	5,5
Communication Topology									
Point to Point	9	8	8,5	4	6	5	2	4	3
Bus	11	10	10,5	20	14	17	18	20	19
Star	-7	-8	-7,5	-16	-10	-13	-14	-16	-15
Ring	-10	-9	-9,5	-12	-10	-11	-10	-12	-11
Communication Technologies									
Serial	-23	-16	-19,5	-45	-35	-40	-46	-47	-46,5
Ethernet	7	10	8,5	11	12	11,5	14	3	8,5
Backbone technology									
TCP/IP	5	2	3,5	18	8	13	16	18	17
UDP/IP	1	0	0,5	-6	-2	-4	-6	-6	-6
MPLS	6	5	5,5	13	13	13	18	9	13,5
ATM	14	13	13,5	23	21	22	26	19	22,5
Frame Relay	-9	-11	-10	-5	-13	-9	-10	-1	-5,5
SDH/SONET/DWDM	14	13	13,5	23	21	22	26	19	22,5
Security									
Data Encryption	-2	-4	-3	-9	-7	-8	-14	1	-6,5
Authentication	-10	-12	-11	-19	-15	-17	-22	-9	-15,5

	AVERAGE STATION CONTROL	AVERAGE DATA ANALYSIS	AVERAGE R.T. PROT & AUT.	AVERAGE SAS MANAGNT	AVERAGE COMMERCIAL	AVERAGE S/S MANAGEMNT	AVERAGE SITE WORKING	AVERAGE SECURITY
Transmission Media outside Substations								
Fiber	30,2	27,67	38,00	33,5	33,5	18,5	34	38,5
Copper	-25,4	-11,67	-25,00	-17,5	-17,5	-2,5	-16	-20,5
Radio								
Point-to-point Microwaves (PDH/SDH)	-6,6	-0,33	1,50	-4,5	0,5	7,5	4	-1,5
GSM, GPRS, GSM Data	-27	-28,67	-31,00	-33,5	-33	-17	-34,5	-39,5
Point-to-Multipoint	-19,2	-8,00	-16,25	-14	-11	2	-9	-15
Spread spectrum	-10,2	-12,67	-15,00	-11,5	-9	-4	-15,5	-16,5
Satellite	-33,6	-27,00	-45,25	-36	-32,5	-16,5	-32,5	-40
High Voltage PLC	-22,2	-23,67	-37,50	-25,5	-22,5	-14,5	-30	-32,5
Transmission Media inside Substations								
Fiber	30,2	27,67	38,00	33,5	33,5	18,5	34	38,5
Copper								
Twisted pair	-18,2	-7,67	-20,25	-10,5	-9,5	0	-11	-13,5
Ethernet (UTP)	25,4	11,67	25,00	17,5	17,5	2,5	16	20,5
Wireless								
DECT telephony	-12,6	-9,67	-2,00	-11,5	-11,5	1,5	-11	-14,5
Wireless LAN	-3,4	4,67	3,50	1,5	5	7	10,5	7,5
Bluetooth	19,4	2,33	21,50	10,5	5,5	-3,5	1	7,5
Communication Methods								
Peer-to-Peer	0,2	-5,67	5,25	-3,5	-5,5	-1,5	-8	-7,5
Master/Slave	-0,2	5,67	-5,25	3,5	5,5	1,5	8	7,5
Client/Server	-13	-2,33	-23,25	-8,5	-4,5	-0,5	-4	-8,5
Publish/Subscribe	6,2	3,67	8,75	3,5	6,5	4,5	7	5,5
Communication Topology								
Point to Point	1	6,00	5,00	7	5	8,5	5	3
Bus	13,8	14,00	23,00	19	15	10,5	17	19
Star	-3,8	-10,00	-8,00	-9	-11	-7,5	-13	-15
Ring	-7,4	-10,00	-14,00	-13	-10	-9,5	-11	-11
Communication Technologies								
Serial	-36,6	-31,67	-47,00	-39,5	-38,5	-19,5	-40	-46,5
Ethernet	-1,8	8,67	3,50	4,5	6	8,5	11,5	8,5
Backbone technology								
TCP/IP	14,4	12,00	18,00	15	11	3,5	13	17
UDP/IP	-1,4	-2,00	-1,50	-1	-3	0,5	-4	-6
MPLS	12,6	7,67	17,75	9,5	11,5	5,5	13	13,5
ATM	15	15,67	24,25	17,5	19,5	13,5	22	22,5
Frame Relay	-0,6	-3,67	-6,25	-2,5	-8,5	-10	-9	-5,5
SDH/SONET/DWDM	15	15,67	24,25	17,5	19,5	13,5	22	22,5
Security								
Data Encryption	-5,4	-3,67	-13,00	-2,5	-3,5	-3	-8	-6,5
Authentication	-7,8	-11,67	-19,50	-10,5	-11,5	-11	-17	-15,5

B. SECURITY ANNEX

The terminology relating with security aspects of communication technology, which are considered relevant to this work, are described in the following sections.

SSL

The Secure Socket Layer (SSL) is a commonly-used protocol for managing the security of a message transmission on the Internet. SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers. SSL is included as part of both the Microsoft and Netscape browsers and most Web server products. SSL has gained widespread support and so has become the de facto standard. The "sockets" part of the term refers to the sockets method of passing data back and forth between a client and a server program in a network or between program layers in the same computer. SSL uses the public-and-private key encryption system, which also includes the use of digital certificates. SSL is now being succeeded by Transport Layer Security (TLS), which is based on SSL
TLS and SSL are an integral part of most Web browsers (clients) and Web servers. If a Web site is on a server that supports SSL, SSL can be enabled and specific Web pages can be identified as requiring SSL access. TLS and SSL are not interoperable. However, a message sent with TLS can be handled by a client that handles SSL but not TLS.

HTTPS

HTTPS (Hypertext Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a Web protocol which is built into the browser. The protocol encrypts and decrypts user page requests as well as the pages that are returned by the Web server. HTTPS is really just the use SSL as a sublayer under its regular HTTP application layer. (HTTPS uses port 443 instead of HTTP port 80 in its interactions with the lower layer, TCP/IP).
HTTPS and SSL support the use of X.509 digital certificates from the server so that, if necessary, a user can authenticate the sender. SSL is an open, non-proprietary protocol.

Hacker

A hacker is someone who attempts to crack someone else's system or otherwise uses programming or expert knowledge to act maliciously. A cracker is someone who breaks into someone else's computer system, often on a network, bypasses passwords or licenses in computer programs, or in other ways intentionally breaches computer security. A cracker can be doing this for profit, maliciously, or because the challenge is there. Some breaking-and-entering has been done ostensibly to point out weaknesses in a site's security system.
Typically, this kind of hacker would be a proficient programmer or engineer with sufficient technical knowledge to understand the weak points in a security system.

Snooping

A snoop server is a server that uses a packet sniffer program to capture network traffic for analysis. Used to identify security risks and/or to monitor employees' activities (such as Web sites visited), a snoop program puts network interfaces into promiscuous mode. This mode allows the system to access all the data in each network packet - instead of only routing-related information - including those packets intended for other computers. Packet data is typically captured to a file for later analysis and reporting. Any computer on a network can use a snoop program, although - at least for administrative purposes - they are most often installed on servers. Snooping is also a popular means of illicitly collecting network data; sometimes an administrative snoop server finds a previously undetected node operating for this purpose.

Spoofing

On the Internet, "to spoof" can mean to deceive for the purpose of gaining access to someone else's resources (for example, to fake an Internet address so that one looks like a certain kind of Internet user). Spoofing can also mean to simulate a communications protocol by a program that is interjected into a normal sequence of processes for the purpose of adding some useful function

Hijacking

Hijacking is a type of network security attack in which the attacker takes control of a communication between two entities and masquerades as one of them. In one type of hijacking (also known as a man in the middle attack), the perpetrator takes control of an established connection while it is in progress. The attacker intercepts messages in a public key exchange and then retransmits them, substituting their own public key for the requested one, so that the two original parties still appear to be communicating with each other directly. The attacker uses a program that appears to be the server to the client and appears to be the client to the server. This attack may be used simply to gain access to the messages, or to enable the attacker to modify them before retransmitting them.
Hijacking is also used to make it appear that one or more Web sites have been taken over. There are two different types of domain name system (DNS) hijacking. In one, the attacker gains access to DNS records on a server and modifies them so that requests for the genuine Web page will be redirected elsewhere - usually to a fake page that the attacker has created. This gives the impression to the viewer that the Web site has been compromised, when in fact, only a server has been. This type of hijacking is difficult to prevent, because administrators control only their own DNS records, and have no control over upstream DNS servers. In the second type of DNS hijack, the attacker spoofs valid e-mail accounts and floods the inboxes of the technical and administrative contacts. This type of attack can be prevented by using authentication procedures.
In another type of Web site hijack, the perpetrator simply registers a domain name similar enough to a legitimate one that users are likely to type it, either by mistaking the actual name or through a typo.

Denial of Service

On the Internet, a denial of service (DoS) attack is an incident in which a user or organization is deprived of the services of a resource they would normally expect to have. Typically, the loss of service is the inability of a particular network service, such as e-mail, to be available or the temporary loss of all network connectivity and services. A denial of service attack can also destroy programming and files in a computer system. Although usually intentional and malicious, a denial of service attack can sometimes happen accidentally. A denial of service attack is a type of security breach to a computer system that does not usually result in the theft of information or other security loss. However, these attacks can cost the target company a great deal of time and money.