19

THE OVERALL IMPACT OF DIGITAL TECHNIQUES FOR TRANSMISSION SYSTEMS (SUBSTATION CONTROL)

Working Group 06
of
Study Committee 35
(Communication and Telecontrol)

1987

cigre

THE OVERALL IMPACT OF DIGITAL TECHNIQUES FOR TRANSMISSION SYSTEMS (SUBSTATION CONTROL)

Working Group 06
of
Study Committee 35 (Communication & Telecontrol)

R.A. Lilley, J. Xampeny (Conveners)
B. Magnusson (Secretary)

1987

CONTENTS

1 - Introduction

1.1 Aim and scope of the report

With the existing investment and infrastructure it is likely that the operation, control and protection of transmission networks will be carried out by conventional equipment for a number of years.

However, digital techniques, which are already in widespread use in some fields, are increasingly coming into use in coexistence with analogue equipment and make it possible to consider a complete digitalization of the system as a whole. This leads to a progressive change in the functions and performance, which requires both the operator and the manufacturer to adopt a different approach and attitude towards the problem met.

The purpose of this document is to draw general conclusions on the impact of digital techniques on transmission networks, especially for substations. It does not attempt to give precise descriptions of the possible solutions and it should be considered as a guide for persons dealing with this field rather than as a collection of defenitive recommendations. Whilst the report is confined to transmission applications, many of the techniques discussed are applicable to distribution systems also.

The main contributors to this report from CIGRE study Committee 35 Working Group 35-06 are as follows:-

1.2 Contributors

J Xampeny	(Spain)
A Casals	(Spain)
A Gustafsson	(Sweden)
T Lefebvre	(France)
R A Lilley	(England)
T H Lomas	(England)
B Magnusson	(Sweden)
S L Nilsson	(USA)
A Rein	(Denmark)
W Wimmer	(Austria)
W Wolfgarten	(Germany)
A Natale	(Italy)

1.3 General

Before examining the impact of digital techniques on control systems in greater detail, some of the characteristics of the integrated station that distinguish it from current designs are listed.

The term integrated, used throughout this document, is to be taken in a wide sense and does not imply all functions being carried out within one device or box but a close interaction within a total defined system. The term coordinated which is sometimes used is felt to be insufficient in that protection and control functions are already coordinated within existing systems.

1.3.1 Features of integrated substation control

- The electrical measurements are transmitted in the form of digital messages.

- The information exchanged between the kiosks and the control buildings is multiplexed on a few serial links (optical fibres, coaxial cables, etc).

- Each application has access to a great deal of information via a reliable data base.

- Part of the hardware may be shared by several functions (eg data-processing or communications systems).

- Self test and auto diagnosis functions are continually performed and alarms generated for maintenance purposes.

- The electrical measurements and the other data are processed by sophisticated algorithms (signal-processing algorithms, sorting operations or expert systems).

- All the information is precisely timed, in order to allow event analysis.

- It is possible to write, test and modify software remotely, and download settings.

- Most of the devices can be standard (mini or microcomputers with their peripherals, interfaces, communication links, etc).

- Life time will probably be shorter due to rapid advances in these technologies.

- The new systems are inherently more sensitive to interferance than existing electro-mechanical systems.

1.3.2 The advantages of digital techniques

1.3.2.1. The economic aspect

In a broad sense, this is the most important aspect.

The control and monitoring market is small and specific. The cost of all equipment is tending to grow as performance requirements change or new functions appear.

On the other hand, because the fields of application are more and more varied, the cost of data processing hardware is steadily decreasing.

The introduction of microcomputer systems requires a significant expenditure to provide the necessary interface protection and the introduction of the new transducer techniques eg using optical techniques.

While their functional characteristics are constantly being improved, microcomputers, their peripherals and interface devices (man-machine interfaces, CRT terminals) are becoming less expensive due to component integration, use of widespread products and standardisation efforts.

In addition, unlike conventional equipment, several functions can take place in a single computer. This reduces not only the number of units, but also the number of physical links between the different modules and within the general infrastructure of substations.

On the other hand, the software development is expensive. Fortunately, it can be amortized over a large number of units and adapted to different types of hardware.

The same comments can be made with regard to the contribution of digital techniques to communications. However the substation is structured, the wiring at present used represents a large investment. Multiplexing and the high data rates offered by modern transmission techniques reduce communication within the station to a few links only. For example, in the field of local area communication networks, a great deal of work has been done by standards organisation (ISO, CCITT, IEC, etc) and be very large companies (MAP project from GENERAL MOTORS for instance), and there are reasonable hopes that these efforts will generate savings.

In addition to these direct gains there is the benefit of new functions and of better exploitation of existing functions which can help to improve the quality of supply. For example they will facilitate the tasks of operators hence improving their efficiency. Digital equipment can also test itself or be tested remotely, so reducing the cost of preventive maintenance.

1.3.2.2 Availability, reliability

Today, a device is very often dedicated to a particular function. With the use of data processing equipment this concept has changed because several functions are performed in the same processing unit. Moreoever, these functions are becoming more and more numerous and complex.

New kinds of architectures must be studied to avoid, as far as possible, common mode failure points. Some of these like data bases cannot be completely removed. However, these may be considered as relatively reliable provided they are periodically refreshed and checked. Nevertheless, many factors will allow an increase in the availability and the reliability of every function and of the whole system.

The self test capabilities of the digital techniques increase the availability of the system by detecting problems as soon as they occur. This is not the case with present equipment, ie. it is only possible to know if they are working by using them or when they perform an unwanted operation.

The reliability of an elementaty function is also improved by the use of VLSI circuits; these are becoming more and more reliable and are consuming less and less energy. The possibility of using error-detecting and correcting codes is also helping to improve the reliability of communications systems, and especially with long-distance links.

Transmission safety can be improved by using standardised protocols and media like optical fibres which give a better immunity against electromagnetic interference.

To cope with the growing complexity and number of functions, special care must be paid to software development. Modern methods of software engineering minimise mistakes as early as in the first design stages and lead to well structured system with a clear partitioning of functional unit.

1.3.2.3 Performance

In the long term, the major improvement will be to the required performance.

Some new objectives can be reached with conventional equipment but digital techniques can provide further sophistication for a reasonable cost. For example digital processing of signals increase the quantity and quality of the information that can be extracted from the same electrical values. This makes it possible to be either more precise or faster as in the case of system protections.

Other requirements such as real-time modelling of the thermal loading capability of lines and equipment can only be realistically achieved by digital means.

The concept of memory, which is a natural function of data-processing systems, constitutes another aspect that is interesting for multiple applications: oscillo-perturbography or simple storage for later processing

permits better use of equipment resources (central processing units, communications systems).

However, we must avoid the possibility of this leading to a large increase in the quantity of information to be processed by the operator, making the system more difficult to manage.

1.3.2.4 Flexibility & Compatability

At present, a modification can only be considered if requirements change significantly, and in all cases equipment has to be changed. When this happens, we generally prefer to wait for the next stage of development, or to accelerate its adoption.

Data-processing can make modifications or simple updatings easier. It can also facilitate the interconnection of sub-systems which communicate via a data base. Nevertheless, whenever a partial change is made to the software used for a function the greatest care must be taken to avoid disturbing the applications that use the same equipment. In this context, modern methods of software development demonstrate their importance, while they offer the additional advantage of placing the implementation of an application on a more functional level.

Most of the equipment can come from the vast market for industrial data-processing and be adapted to different configurations, thus reducing the development effort and also spares for maintenance purposes. Standard conformance (ISO, IEEC, IEC) improves the flexibility and compatibility by offering suitable interfaces.

1.3.2.5 New Functions

The new digital techniques applied to the control and monitoring of energy networks offer various facilities to operators such as sorting operations (alarms, data), combinations of elementary functions (sequence switching), greater possibilities for the storage of events or for setting points command etc. Many of these functions are already provided by conventional systems, which use mini-computers for a part of systems management. Complete digitalisation of the control functions opens up new possibilities such as:

- remote maintenance and remote diagnosis,
- down loading of programs, data instructions data bases,
- remote checking of information in protection, etc,
- calculation of load transfer before tripping a circuit-breaker.
- teleprotection.

In a second stage, the use of modern techniques like artificial intelligence and expert systems will complete these new possibilities inherent in data-processing systems, by making operational a number of functions that are very useful for the operator like reliable estimation of system state, aid in fault finding summarising information, analysing complex faults, or rapid and automatic return of installations to service after a serious breaksown. Most of these new developments will appear first in control centres.

2 - Functions

2.1 Introduction

This chapter presents a list of functions. Not many entirely new functions will be found in the list but many will be enhanced by digital techniques. The use of these in substations will open up possibilities for new ways of distributing functions (or sub-functions) between control centres and substations. The net result could be the decentralising of today's control centre functions. The document does not include any discussion of this topic.

2.2 Control and protection functions.

Protection Functions

Line Fault Protection

Detect a fault in the protected zone and initiate high-speed tripping of circuit breakers. The protection scheme can be pilot or non-pilot and produce three-phase tripping or selective-pole tripping output.

Transformer Fault Protection

Detect and initiate high-speed tripping of circuit breakers to isolate transformer or transformer bank for any fault within the protected zone. It must discriminate between internal faults and through faults and detect overload.

Bus Fault Protection

Detect and initiate high-speed tripping of circuit breakers to isolate the protected bus-bar section for any fault in the protected zone.

Shunt Reactor Protection

Detect faults in line-connected reactors in order to trip locally and to transfer-trip remotely. Detect faults in tertiary reactor bank to disconnect it from transformer.

Transfer tripping

Provide a common control facility for all functions which transfer-trip to a specific remote location. Supervise received transfer-trip signals and monitor false outputs.

Breaker Failure and Fault Protection

Direct that a fault identified by some relaying system has not been cleared by the protecting breaker, and initiate tripping of adjacent backup breakers to isolate the fault and malfunctioning breaker.

Automatic Control Functions

Automatic Reclosing

Attempts to reclose the breaker a short time after the fault has been cleared.

Automatic Switching Sequences

Executes sequences opening and closing breakers and disconnect-switches.

These sequences could be initiated automatically in the station from other stations or controlled from the Control Centre either by down-loading the full sequence or under an automatic step by step procedure.

Two types of functions are:

Automatic network restoration.
Used to restore the network after a major disturbance or after an unsucessful reclosing operation. The automatic network restoration requires the use of the synchronising function when closing the circuit breakers.

Switching of high voltage components.
Used as an aid to simplify the task of the operating personnel and to ensure that switching operations are performed rapidly and safely.

Synchronising

Used as an aid to the automatically initiated closing of circuit breakers which is prevented if the conditions for synchronising are not satisfied. Execute a breaker-closing order after adjusting voltage difference across the open breaker; operating tap changers and phase-angle regulators.

Load shedding

Used to prevent a breakdown of the power network if the frequency should drop significantly. When the frequency is dropping, different parts of the load will be disconnected successively at predetermined limits of frequency or rates of change of frequency. When the frequency starts to rise again, the load can be automatically reconnected successively as frequency reaches certain present values. Similar functions are network splitting and ripple control.

Automatic Voltage Control

Includes the control of tap changers and connection and disconnection of reactor banks. These functions can be performed based on the substation voltage or estimating the voltage at a remote point.

Network Automation

Reactive power control, ie. adapting MVAR production to network and consumption needs.

Tie Tripping

Used to trip the breaker when the transmission tie to a neighbouring utility shows sustained heavy power flow in conjunction with system frequency a specified amount below normal. The tripping can be produced based on load flows versus time without frequency supervision or based on the rate of frequency change.

Out-of-step Protection

Implement a splitting or islanding of the system which separates out-of-step machines and which balances the load and generation within each island.

<u>Monotoring Functions</u>

Fault Location

Measures the distance to a fault on line, based on information from the faulty line or from other lines and from other substations.

Interlocking (safety interlocking and operational interlocking).

Used to prevent a disconnector from breaking load current or connecting systems that are not connected in the station. Also prevents the closing of switches/earthing in dangerous combinations.

Pilot and Transfer - Trip channel Monitoring

By means of periodically executed hand shaking or check back tests determine the status of the communication channel.

Load Monitoring

Monitor the apparent impedance associated with load flow at the line terminal.

Distinguish between symmetric and unbalanced fault protection during swings. Detect line current overload.

Monitoring and Control of Breakers and Switches.

Monitor position of breakers and switches based an auxiliary contacts, and current and voltage data. Check timing, pole disagreement and flashover of open devices. Prevent false tripping and closing commands.

Inferential Measurement Check

Check the calibration of the transducers and the consistency of the measurements.

Overload Monitoring

Monitor temperature and current in a transformer, cable or overload line to estimate hot-spot temperature. Keep a historical record of "loss-of-life". Calculate the additional loading capability or predict the remaining time before exceeding safety margins.

<u>System Interfaces</u>

Local Man/machine subsystem

Enables the local operator to perform either at station or bay level, the following functions:

Data display, data entry, manual control operation, diagnostic and maintenance functions, and training procedures.

Remote Control Interfacing

Facilities communication between the substation and the control centre. Processing requests received from control centre and generating information for the control centre.

Alarm Functions

Include the supervision of the power system and the control equipment, performing checks of the data received against high and low limits and detect unauthorised change of status. Time-tag, store and display all the alarms.

Data Logging

Format and output all information which is to be printed locally and prepare information to be transmitted for print out at control centres.

Energy measurement

Obtain measurements of voltage and current, active and reactive power. Integrate these values to obtain, store and display measurements.

Oscillography-Disturbance recording

Collecting, storing and delivery of raw a.c. measurements samples and tripping signals collected immediately prior to and during a disturbance.

2.3 Maintenance Functions

The aim of the maintenance functions integrated in the control system is to support the maintenance staff in their work both for fault tracing and preventive maintenance. The functions can be divided in the following groups.

- control system maintenance

- primary equipment maintenance

These two categories of functions have different users. For instance maintenance people working with control equipment are, or will be in the near future, very familiar with handling computer system while on the other hand maintenance people working with the primary equipment will be handling computerised tools very seldom.

Maintenance functions for the control system include:-

- fault tracing

- self supervision

- statistics

- supervision of trends

- tele maintenance

2.3.2 Primary equipment

For planning of preventive maintenance and also to predict the remaining life time it could be very useful to store operating conditions for a very long time and provide a stastical database of the primary equipment.

An example of a function like this is monitoring the breaking current for a breaker at every tripping and give a signal when it is time to recondition the breaker. Another example is to monitor the winding temperature of a transformer and present the remaining life time for the isolation or the possibilities to overload the transformer.

2.4 Commissioning and installation functions

The intergrated control should in various ways include means to facilitate commissioning and installation, reducing the need for specialist programming assistance.

For example

- Self documentation
This means a presentation of software and data-base contents in a form that is useful for the commissioning staff (Program lists are not sufficient).

- Test interfaces
Possibilities to isolate input/output of function modules in order to operate with simulated data without disturbing other parts of an intergrated system.

- Expansion routines

Well prepared and documented standard routines for the expansion of a system with one or more item. (Meter value, signal, command, complete bay etc).

3 - Requirements

3.1 Introduction

In general an integrated control system must be an effective replacement for existing technology and show a cost and/or technical benefit to allow its implementation to be justified. Integration can be pursued to varying degrees. Complete integration could mean that all of the substation control and protection functions are performed in one computer. A distributed processor system may, on the other hand, have functions segregated and allocated to specific function modules that are interconnected by means of a number of communication links/systems.

The possibility of layered structures, the distribution of functions among the subsystems, the improvement of the interfacing capabilities due to the existence of standards, etc, are aspects influencing the requirements for the new generation of control systems.

The equipment used in the telecontrol and local control of the electric power systems and plants has been developed over several decades to a state of considerable refinement, but so far the concept adopted has been one of segregation between the local and the remote control.

Fuelled by the advances in digital techniques and other related technologies, and by the electricity authorities desire to reduce their operating costs via better electricity system and plant utilisation, considerable interest is now being shown in the idea of an integrated system approach to both electric power system telecontrol and local controls in substations.

Naturally, various strategies have been proposed throughout the world yielding different detailed methods to achieve the objective. It is foreseen that the differences of opinion will resolve as conclusive experiments and trials are performed, allowing the practical implications of each strategy to be clarified.

In this context, one important task is to lay down a set of requirements which must be satisfied. This section considers these requirements which have been grouped under the following headings.

Commercial Considerations

Cost

Performance

Applicability

These groups are interelated: The better the "Applicability" a system has the lower its "Cost" will be. However, in the case of "Performances" the "Cost" consequences cannot be correlated so easily, better "Performances" could extend the life term of the system, but clearly the initial investment would be higher with higher quality requirements.

3.2 Commercial considerations

3.2.1 Reduced costs are, especially in the hardware side, believed to be a strong, motivating force acting and encouraging the development of new control centre telecontrol, communications and local-control equipment. Consequently, market forces are likely to dictate that for equivalent performance, the cost of the new equipment be less than that of conventional equipment.

Costs break down into a number of areas and include items other than the initial purchasing cost, as detailed in the next section. For example, users are justified in considering the cost of installation, commissioning, spare parts, operation and maintenance, personnel training etc. Just as important is the cost and ease of expanding the system at a later date.

3.2.2 <u>Vendor Independance</u>

To comply with the existing commercial practise in telecontrol and substation control equipment, it is preferable that the complete system should be capable of being broken down into a logical set of sub-systems. Each sub-system should then be defined to such an extent that it becomes a multi-sourced item, ie it is commercially available from several manufactures.

This demands the evolution or international standards (software and hardware) that prove to be relevent to both users and manufacturers of such equipment.

3.2.3 <u>Compatibility</u>

Where the design of equipment is updated either to make use of the later technology or overcome the lack of availablity of an obsolescent part, then it is preferable that a policy of "upwards compatibility" is adopted.

This implies that upgraded hardware modules are both hardware and software fully compatible with the older design.

3.3 Cost

3.3.1 Investment

For the same performance, the cost of the new equipment must not be higher than the cost for a conventional control equipment. Additional functions will be judged on a cost/benefit basis. The comparison of cost should be done by comparing the life cycle cost, which will take into account not only the initial investment cost, but also the maintenance cost and other related costs.

3.3.2 Installation, Commissioning and Testing Cost

The system design should lower the special infrastructure requirements.

The remote terminals should be specially adapted so that it can be plugged directly into the sub-station system, without the need for costly interfaces.

Automatic data base generation and documentation production, at the overall system level, should be possible with the appropriate tools.

Instruments and tools, especially those on the software side, should be provided to speed up the commissioning and testing procedures.

3.3.3 Cost of Emergency Operation and Training

The system should be provided with backup facilities for degraded operation in case of an emergency in the control centre. The system should preferably be equiped with self instruction operational procedures and training simulators. This requirement will be of greater interest when applied to the integrated control systems for unmanned stations because it will reduce the cost of training.

3.3.4 Cost of Modifications and maintenance

The control system, in all its subsystems, should be provided with tools, utilities or other facilities, in order to modify the software with the growth of the electrical system.

Easy to use software tools, should be provided for the system maintenance and diagnosis.

In order to lower the cost of visits of personnel to the unmanned stations for testing and modifications, the modification and maintenance functions should as far as possible be done remotely with the appropriate tools. This includes equipment self-test, such procedures possibly being carried out on line.

3.3.5 Expandability Cost

The initial cost of the system should preferably be in direct proportion to the size and complexity of the electrical electric system and the dimension of the substations and power stations.

3.4 Performance

3.4.1 Man/Machine Interface

The man-machine interface is one of the essential parts of a control system because it can be the key point for its acceptance by the operators.

In control centres, full graphic displays with advanced operator interface capabilities and provided with local processing power, should increase the efficiency and performance of the man-machine communications.

In the substation the provision of a man/machine interface would undoubtedly assist the engineer in confirming the healthy operation of the secondary control system. The need for such assistance is directly linked to the overall complexity of the scheme and the need to deal quickly with emergencies. Under such circumstances, it is likely that the benefits rapidly outweigh the costs of the extra equipment.

A major requirement of such an interface is that it must be user friendly, probably by being menu driven, offering the user assistance in a number of important areas including:

a Commissioning.

b Operation.

c Routine testing.

d Diagnostic Assistance.

e Examination of present data.

f Archived store of part events.

g Alteration of settings.

h Operator training.

i Substation diagrams.

j User software development.

3.4.2 Reliability, Availability

The reliability and availability requirements should be referred to the overall system on a per function basis. This should include control centre communications and the local - telecontrol equipment at the stations.

The reliability figures have a relative value only. The main concept is total availability including equipment availability, maintainability, support procedures and maintenance and support effectiveness. The redundancy and/or the functional capabilities should be allocated in order to increase the availability to the overall system.

It is well-known that the limiting availability of a system is directly dependent on its repair time and in this way dependent on the formation and organisational aspects of the maintenence staff. It is important to note that external aspects of the system affect its availability.

The internal factors that affect the reliability of a system are:

a The reliability of the equipment and the software.

b The configuration of the system components.

The new control system should be at least as reliable as the conventional control equipment.

3.4.3 Security, Dependability

The standard ANSI/IEEE C37.1.1979 divides security of operation into three areas:

1. Operating practice procedures.

2. Communications security.

3. Hardware, software and firmware design.

At the overall level, the consequence of a system failure depends on the state of the electric power system. Assuming independence in occurrence, the probability of a dangerous situation is the product of the probability of the failure of a function of the control system and the probability of the occurrence of an emergency situation in the electric system when this function is needed.

One possible application of such criteria on the overall control local system could be:

Operating practice and procedures

An alarm should be generated whenever an event or function has automatically or manually been disabled.

An alarm shall be generated when a device fails.

Select-before-execute man/machine sequence and checkback-before-operate communication sequence will normally be provided as part of the overall control system.

Communication security.

An error in a message shall not result in a critical influence to the power system.

A positive indication should be available when a part of the system does not receive or respond to a valid message.

Hardware, software and firmware design.

The design could include:

A single component failure must not produce a critical system failure.

Safety power failure

Safety automatic restart and power restoration

Initialisation and reinitialisation

Equipment self-check capability with alarm.

Automatic switchover with alarm

Fail-safe operation

Non volatile address at remote equipment.

Local interlock in control devices.

With regard to dependability, the psychological effects of a rapid response to an order should be taken into account thus avoiding operator's doubts following the issue of a command.

3.4.4 Response Time

At the control centre level, the required response time is related to the system functions. The conventional and more common are:

1 to 3 second	Each step in the common procedure Status change and alarm presentation.
3 to 10 seconds	Load frequency control
10 to 30 seconds	Measurement update
30 seconds to 10 minutes	State estimation
5 minutes to 60 minutes	Energy reports

The time response of the local control systems should be classified due to the functional requirements in the following three groups.

up to 20 milli-seconds	Protection, event recording time descrimination,
up to 200 milli-seconds	Synchronising, "snap shot" measurements.

up to 1 second	Remote control, event information.

3.4.5 Accuracy and Range

High accuracy is required for some functions. The most demanding in this regard may by the interchange or revenue metering function, which must function within very narrow error boundaries. A typical amplitude error between 10 and 100 to 200% of the rated imput for a current value may be less than 0.2%. Voltage values may have to be available with similar accuracy up to 110 - 130% of rated value. Phase angle errors of fundamental frequency components for this function must also be very small. Typically less than 15 minute errors are allowed.

The accuracy requirements for protective relaying type functions are less demanding, but the dynamic range requirements are very high. Typically, it is required that the relay quantities be reproduced by the sensors up to 20 p.u. fully offest. The smallest quantity to be resolved depends on what kind of protection function is involved. A transformer differential protection is required to be fairly sensitive in order to detect turn-to-turn failures involving few turns. A typical requirement is to have a resolution that is better than 0.01 p.u. leading to a requirement for at least a 12 bit range of the analog-to-digital converters. In some systems covering the whole spectrum of applications, a 16 bit analogue word has been chosen.

Time skew between samples can also have a detrimental effects for the relaying functions. While some correcting algorithms can be deployed for systems where the time skew is known, this requires more processing power of the computers and is therefore, not desireable. Therefore, the data acquisition system shall operate with a small time skew to permit sample comparisons for any two data items within a substation. A maximum time skew between samples of one half of an electrical degree, or about 25 microseconds for a 60 Hz system, seems acceptable for most relaying algorithms.

It should be understood that the accuracy question cannot be entirely separated from the signal processing algorithms. Thus, for each specific signal processing algorithm, a check of the effects of errors in the digital data sampling system must be made. There is, in general, a bandwidth-accuracy product for the required processed data. Metering for instance, has very high accuracy requirements but does not have to have a large bandwidth. Oscillographic type data records have rather high bandwidth requirements but a high accuracy is not needed.

3.4.6 Interfacing capabilities

At the overall system level there are four interfaces:

- Control centre operators. Overall system presentation should be available at the control centres. Alarm reduction algorithms are necessary to reduce the information sent to the control centres. The operator's interface should be able to cope with the extra rate of information during emergencies.

- Maintenance personnel outside the control centres. The specific information for maintenance purposes and station performance analysis, should be directly accessible from the specialised staff offices.

- Remote terminals. Intergrated telecontrol-local systems at the station, should perform a set of layered functions either locally or as remote terminals in the overall control system.

- Other control centres. Due to the hierarchy of control centres and the electric systems interconnection, a reliable and powerful computer network should connect the different control centres.

There are four interfacng points for the local control equipment, which have different requirements.

- Local operator interface: it should be borne in mind that in many cases the stations are not locally manned, so efficient instructions for the operational facilities should be provided. The system responses to an operator demand should start in less than 15 seconds and be completed in less than 2 seconds.

- Electric system: the IEC standards or other applicable standards should be met (IEC 60 and IEC 68).

- Remote control: the same functions that are performed by the conventional equipment, must be performed by the new one.

- Other equipment: in spite of the variety of the equipment, standards should be agreed upon for the other equipment interface (eg IEEE 488 and MAP).

3.4.7 Distribution of Functions

The concentrations of functions, both on the software and hardware sides, should be avoided as far as possible. This means that functions that only need information from one level, should be performed at that level.

Some of the maintenance functions could be fulfilled from offices other than the Control Centres.

3.4.8 Operating modes

The most obvious and by far the most frequent operating state of a power system is the normal healthy operating state. During such times the power system operators should do little other than dispatch routine control instructions to the power stations and the substations from their central control room. The development of telecontrol has provided a tool for the electricity authorities to perform these control tasks remotely with a high degree of automation. As a direct consequence, the need for human intervention, particularly at substation level, has drastically reduced to the point where demanning of the substation is technically possible and economically desireable.
Within the substation, the secondary control equipment will likewise operate in its normal healthy state for the vast majority of the time devoid of any direct interface with personnel. However, there are situations to consider when engineers will be present within the substation. These include:

a Initial commissioning

b Routine maintenance

c Switching of primary plant, in and out of service.

d Emergency conditions.

- Fault finding, isolation and repair.

- Manual operation.

e Extensions to primary and/or secondary control equipment.

f Substation refurbishment

g Power system testing

The definition of emergency conditions would include failure of any item including high voltage plant, secondary control equipment, communication lines or possibly the central control room. Other emergencies can occur as a result of accidents, major fires and industrial action. Lastly, the recovery of a power system after a major collapse must be considered.

Users will demand a fast return to service of any failed part of the secondary control equipment, especially if there are implications for the high voltage equipment. It is anticipated that this will create a need for hardware and/or software tools to assist engineers in their duties.

3.5 Application

3.5.1 Modularity: Flexibility, Expandability

It is important to maintain a high degree of functional modularity in order that existing computer base equipment can be utilised with minor modifications and that individual functions can be amended, maintained and checked without affecting the remainder of the system. The system must also be capable of being extended to incorporate additional functions as dictated by future system and substation control developments.

3.5.2 Capability to fit existing stations

The system should be capable of being applied to existing substations with the minimum outages and modifications. It will not always be possible to have a greenfield site for such applications.
The system must be upgraded to allow future generations of equipment from various manufacturers to be incorporated into the same system.

3.5.3 The substation environment is hostile and the equipment must be capable of operating in this environment. It is normally undesirable to use such techniques as air conditioning in what are normally unattended situations and the equipment should be sufficiently rugged to operate without such supporting equipment.

3.5.4 Operation

The system must be fundamentally simple and user friendly so that it can be easily understood by all levels of staff and must have sufficient flexibility such that when the functions or the substation itself are modified then the appropriate modifications can be made to the system and the total integrity of the new system checked without major disturbance to existing functions or equipment.
The system must be self-supporting in diagnostic and system information. Such information will replace the normal installation and operation manuals traditionally supplied. Diagnosis should be possible remotely together with the down line loading of settings. It is possible that the down line loading of the data will also be required.
The system should not require the need for special hardware development except in cases where the substation environment makes this essential. These should be kept to the absolute minimum and where possible industrial standards should be adopted. These standards should have substantial manufacturers support on an international basis.

4 - Architecture

4.1 Introduction

Comparing the many proposals that have been made for the integrated system architecture or organisation it can be seen that there is, in a general sense, good agreement between them. In most cases the architecture is based on a hierarchical arrangement of disturbed computer based units interconnected by serial communications networks. The differences between the various arrangements that emerge from more detailed study are due largely to "evolutionary" factors: whether aimed at current implementation or the longer term: what functions are included within the scope of the systems: whether conventional relays can be used; the primary plant layout eg double bus or breaker-and-a-half etc; the availability of system elements and techniques, particulary in respect of the communications aspects. To some extent differences occur due to different preferences for the physical locations of the various subsystems within the substation and the extent to which multicore cable saving is considered important eg in refurbished substations. Certainly all approaches have in common a desire to demonstrate economic and operational benefits, whilst achieving appropriate degrees of reliability, security, flexibility, maintainability etc.

4.2 Structure

In general terms the architecture may be represented by figure 4.1 It consists of three levels of equipment, numbered 0, 1 and 2, generally interconnected by two communication networks.

Each level is characterised by a group of functions associated with this level.

Level 0 covers the interface of control-and-protection-equipment to the HV equipment. It consists of several data acquisition units, associated with the sensors, transducers and actuators usually of one or two bays. These units can be located near to them and HV equipment of Level 1 in serial mode.

Level 1 includes all the protection and control functions which can be solved autonomously for each bay or protection zone. The equipment of this level consists of separate units (figure 4.7) or of combined units (figure 4.6) for control and protection for each bay or protection zone. It may be located at the central control house or at the switchyard, seperated from or integrated into the equipment at the respective level.

All control and protection functions not solvable at bay or protection zone level and all functions associated with the sub-station as a whole including telecontrol and central man-machine interface are solved at level 2. The equipment at this level may consist of a central computer (either duplicated or independent) (figure 4.2) or a group of computers, each solving only one or a few certain functions (figure 4.3). The equipment at level 2 is located in the central control house.

The equipment of the different levels is interconnected by serial communications network, ussually two separated ones.

In some important variants, shown in figure 4.4 and 4.8, two levels are effectively incorporated into the same physical equipment. Consequently there may be no serial communication network interconnected either by only one communication network or by two (or more) communication networks, separated for different groups or functions (control, protection, interlocking,.....), independant of levels.

4.3 Functions of Equipment Levels

The functions of the equipment at the three equipment levels are as follows:-

4.3.1 Level 0:

(a) Provide an internal environment adequately protected against the external electrical and physical environment.

(b) Acquire in digital form (preconditioning where necessary) the analogue values (currents, voltages) with appropriate speed or bandwidth, accuracy and dynamic range and the status of breakers, switches and alarms. Time tag status signals in some systems.

(c) Send the acquired data to level 1.
In general an individual data acquisition unit may send data to one or more relays at level 1.

(d) Receive control command signals from level 1 and output them to the plant actuators.

4.3.2 Level 1

(a) Receiving analogue and status data from level 0.

In general an individual level 1 unit may receive data from one or more level 0 units.

(b) Time tag event data received if not time tagged at level 0.

(c) Implement protection, control and measurement functions associated with the bay or protection zone.

(d) Send data sampling commands and circuit operation commands to level 0.

(e) Receive command information from level 2 and retransmit to level 1 where necessary.

4.3.3 Levels 0 and Combined.

The functions are as above for levels 0 and 1 individually with the exception of those associated with the communication network.

4.3.4 Level 2

(a) Receive analogue and status from level 1.

(b) Implement the overall substation functions associated with telecontrol and the man-machine interface.

(c) Control the manual interface peripherals: visual displays, printers, recorders.

(d) Service the telecontrol link to the remote control centre.

(e) Send control commands to level 1.

4.3.5 Common Functions

It is assumed that equipment at each level will provide, in addition to the functions tested above, control and supervision of its communications links as well as self-test and diagnostic functions.

4.4 Reliability

Comparing the integrated system with the conventional system from the reliability point of view, some new considerations arise. The integrated system may have less equipment overall to perform the same function and, all other things being equal, may consequently have improved reliability in terms of lower overall failure rate. However the basic architecture also contains the possibility of common failure modes, for example because of its use of multiplexed communication links. On the other hand very comprehensive failure detection mechanisms can be included which can detect failures very rapidly. If mean time to repair is short such periods of non-availability may be tolerated for some functions. However, for critical functions such as protection no single failure shall cause the non-availability of the function. To meet this criteria some degree of reduncancy must be included both in the equipment and in the communication networks. The most obvious form of reduncancy is duplication. All level 0 units and units of levels 1 and 2 executing critical functions would have to be duplicated, as would the critical communication links.

An alternative approach which would have a lower hardware overhead may become acceptable. Units at levels 0 and 1 associated with their own bay or protection zone, in addition to performing the fuctions for their own bay or protect zone also perform back-up functions for an adjacent bay or protection zone. Any single failure need not then lead to non-availability of essential fuctions.

4.5 Forms of Equipmemt

There is a presumption that the individual items of equipment which make up the integrated system will be based on digital technology. This is largely already the case for equipment at level 2. However, for levels 0 and 1 this represents a change from the present form of analogue and electromechanical protection relays.

During the transition phase therefore, the integrated system must allow both analogue and digital relays to coexist.

The move to digital technology encourages an aim to achieve more uniformity of hardware across the equipment levels on the basis that the actual functionality of the equipment is determined by software. This being the case there are apparent benefits in adopting widely compatible hardware systems.

In general, the modules used in individual equipments will use microprocessors or multiple microprocessors with appropriate input/output interface units for handling analogue, status, control and communication signals. Each unit should also support a local manual interface (which could be removable in order to be used with other similar units).

Level 0 units, in particular, require special attention in as much as they provide the interface to the plant. They must continue to function perfectly during all system disturbances and must therefore provide a very high level of electricity environmental withstand.

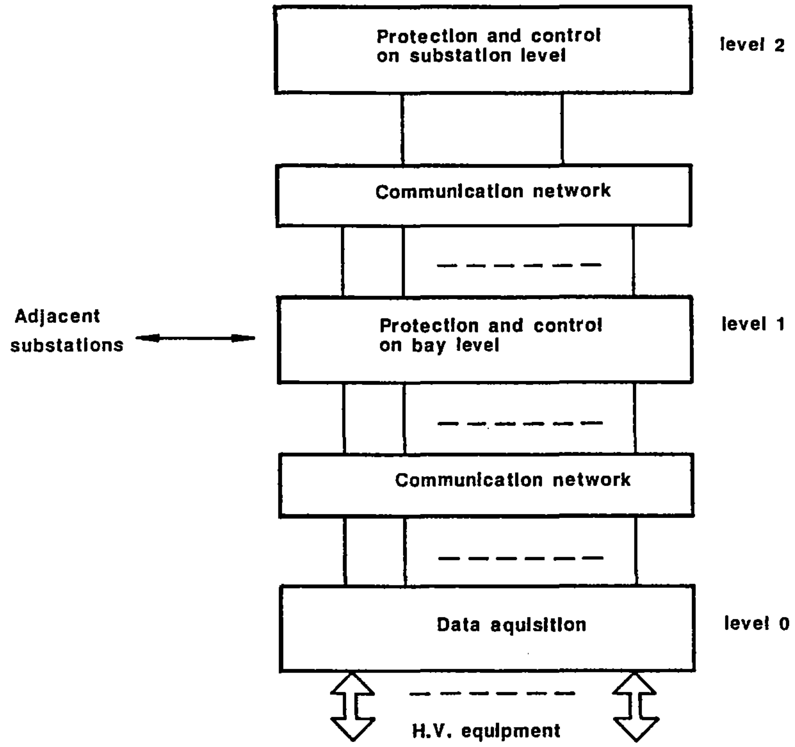

FIGURE 4.1 GENERAL ARCHITECTURE
OF INTEGRATED SUBSTATION

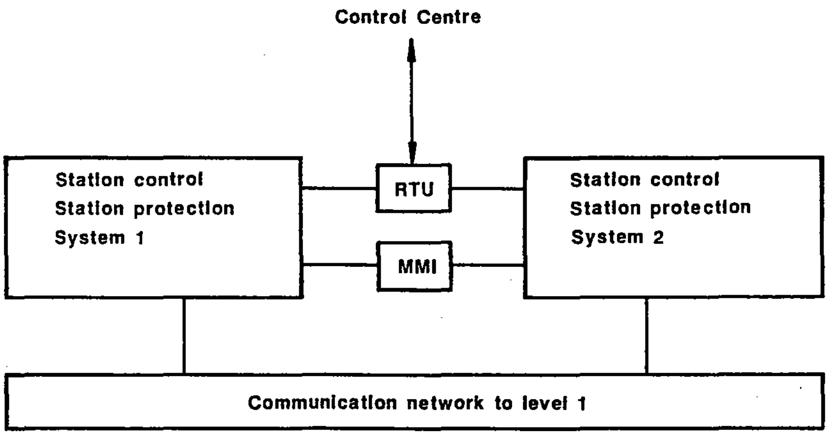

FIGURE 4.2 CENTRALISED LEVEL 2 ARCHITECTURE WITH SOME REDUNDANCY

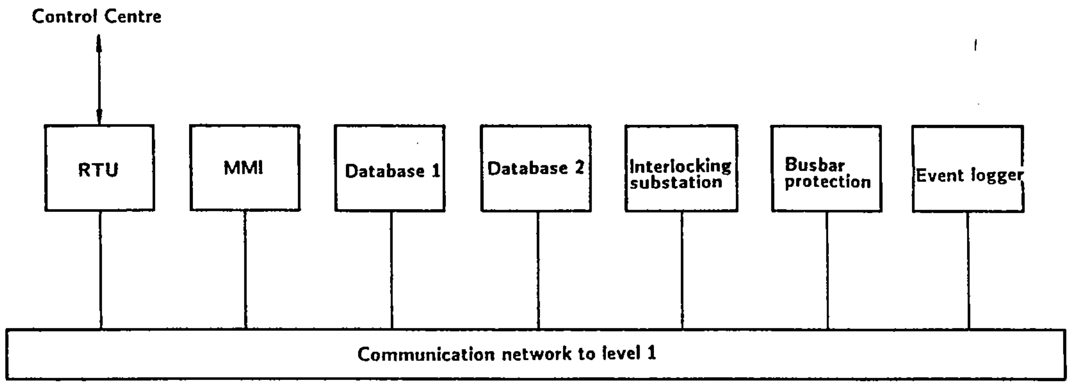

FIGURE 4.3 DECENTRALISED LEVEL 2 FUNCTIONAL ARCHITECTURE WITH DUPLICATED DATABASES

Note : Busbar protection may be at bay level

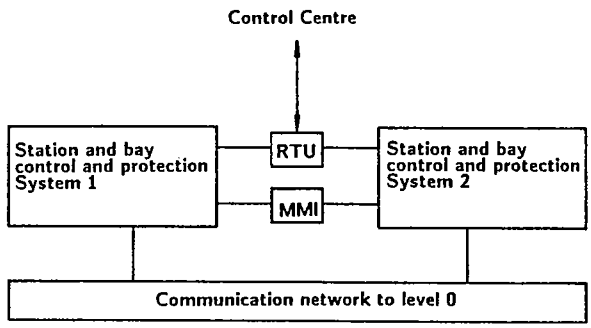

FIGURE 4.4 CENTRALISED ARCHITECTURE OF COMBINED LEVEL 2 AND LEVEL 1-SYSTEM

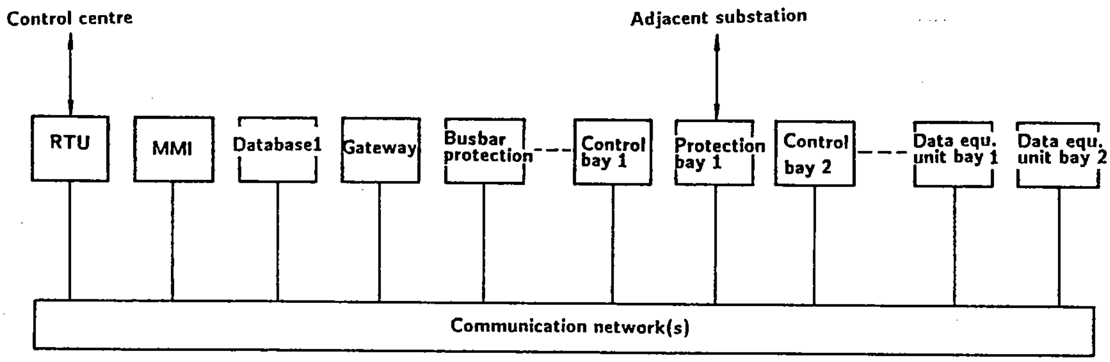

FIGURE 4.5 ARCHITECTURE OF DECENTRALISED AND NON-HIERARCHIAL SUBSTATION SYSTEM

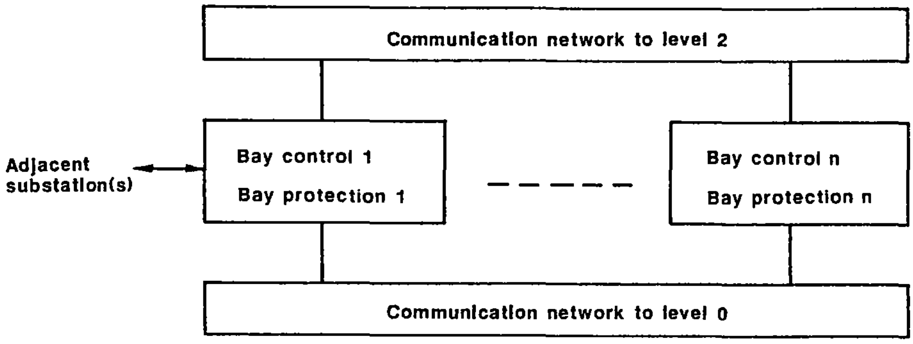

Figure 4.6 LEVEL 1 -ARCHITECTURE WITH COMBINED CONTROL - AND PROTECTION - EQUIPMENT AT BAY LEVEL

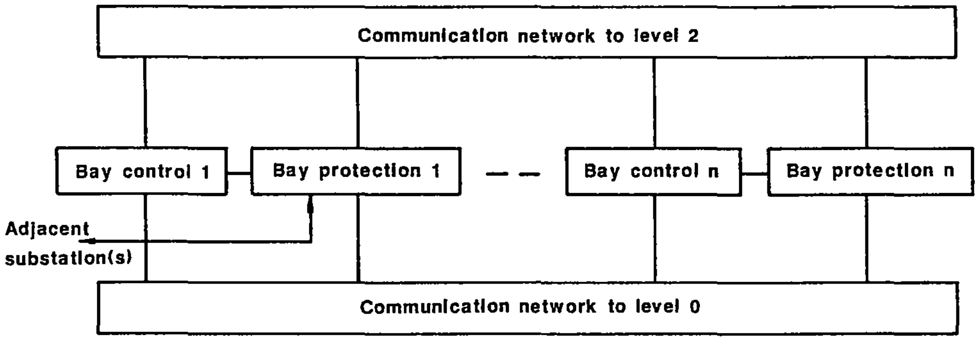

Figure 4.7 LEVEL 1 – ARCHITECTURE WITH SEPERATED CONTROL – AND PROTECTION – EQUIPMENT AT BAY LEVEL

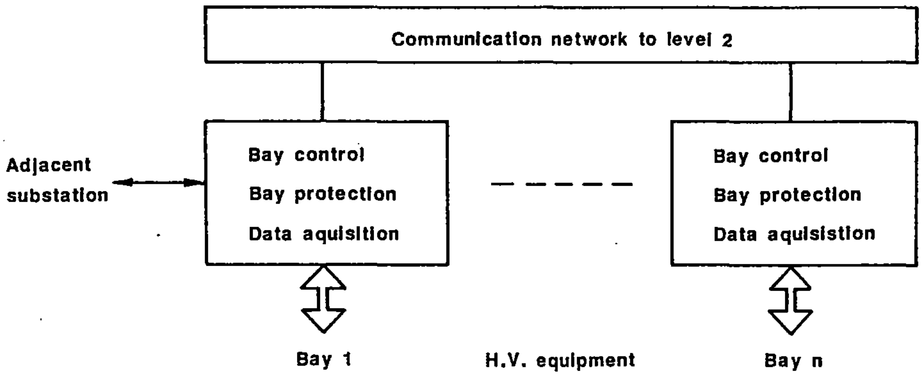

Figure 4.8 COMBINED LEVEL 1 AND LEVEL 0 EQUIPMENT

5 - System Database

5.1 Introduction

Computers applied in substations can be configured to serve different sets of functions from among those listed in Chapter 2. Simple systems can be built to handle limited data acquisition functions such as event recording, whereas more complex systems can serve the entire instrumentation, control and protection needs of a substation. While the data base needs of the simpler systems are non-trivial, those of a fully integrated control and protection system are rather complex. The simpler systems can be considered as a subject of the integrated system: therefore, they will not be discussed separately in this document.

5.2 Data Structures

5.2.1 Data Types

The data base of a substation control and protection system will have data types that are typically found in many other real-time control systems. The listing below may not be complete but represents the different types of data items that should be considered.

- Data items representing samples of measured or computed analogue quantities such as instantaneous current values or computed rms equivalent values of the same currents.

- Data items representing the logic states of substation equipment, such as breakers that can be an open, closed, intermediate or "dont know" state.

- Data items that represent counts such as time and date.

- Data items representing an address giving the location of an input (system module, card and point identification), an output, the name of a control point or the name of a variable used in the system.

- Data items representing operational parameters for functions such as the impedance setting of a distance relay, the lock-out states for a protection zone computed by a protective relaying function, or a local versus remote control authorisation entered by an operator.

- Data items representing parameters for operation of the control and protection system itself such as a test versus operate input for a hardware module, a disable versus enable operator entry for a software module, or an input to a hardware module.

- Time series data representing changes in the operational environment such as a state change of the substation, including data logs, event and oscillographic data files.

- Character strings associated with inputs/outputs.

The format of the data items must be understood by all of the users of the data, that is all of the function modules connected to the same communication subsystem. Some data items are settings, which have varying needs for on-line access. Those that are changed infrequently may not even need on-line access, they can be permanently entered when the system is built or is undergoing major changes. Thus, it is permissible to store some data in read-only memories (ROMs). If data items stored in ROMs need to be changed on-line, the data has to be read into RAM. The ROM data items can then be used as default values for use in a recovery-after-fault sequence. This could be the case for an adaptive setting of a protective relay function or for default report generation formats. Of course, the ROM will have to be revised to make any change permanent.

Some data, such as settings for relaying functions, must not be damaged by a temporary loss of auxiliary power. However, an unexpected trip command stored in a section of the data base containing the output queue for a control output devices has to be verified before its execution upon recovery from a power failure. Thus it may be beneficial to store control output queues in volatile memory because that would prevent old breaker trip commands from being executed upon recovery from a power failure. Volatile memories are acceptable only if there is a way to reconstruct the data base for each function module from segments available in other function modules. In general disc and other rotating forms of memory are not considered satisfactory for substation systems.

5.2.2 Combined Data Formats

Depending on the application, data may be combined to form larger blocks for the following reasons:-

- Improvement of transmission efficiency of a communication link.

- Summary of measured values of one

function module for a specific time slice (e.g. for checking of all currents of one busbar according to Kirchhoff's laws).

- Interrogation of all switch statuses, measured and counted values of a function module.

Standardisation of these combined data formats is needed to limit the range of variety. The problem is to do this while at the same time ensuring adequate scope for future developments and the desired degree of freedom in distributing the functions appropriately within a decentralised automation and control system for substations. If one or two preceding bytes are defined for the "data type" and thus for identifying these individual combinations, standardisation could be implemented as follows:

1st step:
Definition of, for instance, 10 or 20 basic combinations, definition of task-specific free area (which will remain free in the future) as well as definition of an area, which at first is "prohibited".

2nd step:
As soon as empirical values are available, extension of the defined aread by reducing the "prohibited" area.

5.2.3 Identification (addressing)

Based on the preceding information. Two associated elements of information can already be presented:

- Element 1: Data Type

- Element 2: Combined Data

Data type, in its broader sense, also includes the definition of transmission causes such as:

Event (process-related)
Cycle
Selective interrogation
General interrogation
Feedback after control operation

However, it would be advisable to define another byte for this purpose. The information thus represented can only be processed further, if it is possible to clearly identify them within the whole system. In the higher-level control systems (e.g. load dispatching centres, regional control centres), this will be implemented on a topology-orientated basis. This means that the address structure utility network is as follows:-

Station identification
Busbar section and/or voltage level
Cubicle
Item of equipment

For reasons of costs, most of today's telecontrol systems use a hardware-orientated address structure, which, for example, incorporates the following components within the substations:

Function module identification
Subassembly identification
Card identification
Terminated point identification

Conversion of such hardware-orientated address structures into the topology-orientated form optimised for high-level data processing can be performed in the telecommunication modules of the system. Frequently, however, it is done in the front end processor of the higher-order function module itself. This is the reason for the extreme variations of the contents in the telecommunication lines. The following compromise suggests itself for a future-orientated decentralisation concept of automation and control in substations:

- Topology-orientated addressing between higher layers of the integrated control system hierarchy within the substation and in the communications between substation and control centres.

- Hardware-orientated addressing (because of the advantages as regards price and easy verification) within the lowest level function modules within a substation. The conversion of hardware-orientated addressing into topology-orientated addressing must be assigned to one layer of processors of the integrated system.

5.3 Data Base

5.3.1 Assumptions

While the data base system to some degree can be discussed without considering the target hardware, there are some constraints imposed on data base implementation by the hardware. These constraints are:

- The hardware system installed in the substations may not contain the peripheral equipment needed for the software development because it increases the system cost and reduces its availability.

- If the system must continue to perform critical functions, such as the protection functions, for any single component failure then the entire system cannot be shut down for modifications or the necessary validation tests after a change.

- It must be possible to modify the entire data base segments without requiring a complete retest of the system.

The hardware implementation for a substation control and protection system has been discussed in Chapter 4.

Although a common data base is a possibility for a distributed processing system, the speed of response requirements of the protective relaying functions cannot be satisfied with present technologies in such a system. Thus, for such systems, the data base will be distributed but it may not be hierarchical in nature. This will depend on the functional distribution of the software and whether the data base modules are the same type or different (see Figure 5.1 and 5.2). Because a substation evolves over a long time period, its safe assumption that even if a system uses similar modules at the beginning of its useful life, it will evolve into a system with different modules. Therefore, it is probably better to assume different data base module types from the outset.

5.3.2 Data Storage Requirements

The data base management must consider the storage requirements of an integrated system. The different data types listed in section 5.2.1 above, will have to be considered individually. A lost data item that can be quickly recovered by making a new measurement can be stored in a volatile storage media whereas, a setting may have to be re-entered by an operator, who may not even be in the station. This type of data item must not be easily destroyed, which may require a non-volatile storage media (or redundant data items must exist).

5.3.3 Data Base Design Approaches

The assumptions given above directly lead to the conclusion that at least in the short term, conventional, general-purpose, type data base maintenance programs will not be available for control and protection systems. Hence, the data base function is assumed to be in two parts. One is the program for building the on-line data base and for rebuilding it after a system change. The other is the update of the on-line data base, but will not include expansion of the data base.

5.3.3.1 Data Base Builder

Assuming a system (Figure 5.2), with different data base modules there must be a data base builder for each unique family of system modules. Only the similar parts of the system can have the same data base building program. The alternative is to have a translator for each unique data base, which would result in a general program design as shown in Figure 5.3.

The inputs for the data base building program, which can serve as the system configuration program, include a list of all the system inputs and outputs. A list defining the control and protection system is also a needed input, because the inputs need to be mapped onto the different hardware modules. In addition, a list of the software functions is needed to let the data base building program know what function is allocated to each hardware module.

The outputs for each system module are the load files. For those systems that are PROM based, the load file can be an input to a PROM burner. For a program that is intended to handle non-compatible system modules, a translator is needed for each type of module, otherwise the load file will not run on the target.

Occasionally the control and protection system will have to be changed to accomodate new requirements and the system must be capable of accepting these changes without the need for a re-verification of the entire system.

5.3.3.2 On-line Data base Design

The on-line data base update systems will consist of a number of programs to acquire real-time data and convert it to forms that are suitable for the different systems functions. For instance, raw data must be validated to satisfy security needs, instananeous current and voltage samples need to be converted to an rms form, time series data files need to be generated for non-real-time analysis, etc. Data base initialisation functions will have to be part of the system for start and test operations and for recovery faults. Hence, the on-line data handling software is more like a special data processing than a data base update maintenance function.

The data base for a substation control and protection system will contain data items used by many function modules. An example is the lock-out of a breaker or a protection zone, which will be needed in every function module that controls the affected breakers. This will be referred to as global data in contrast to the data used only by a single function module, which will be referred to as local data. (This is not a strict definition because within the function module there may be data items needed by many software modules, which is global within the specific module). Also, there are data items used only by a single software module, which can be labelled as local. An example is the trip setting of a specific distance relaying function, which can be stored in the local data base but the setting is used only by the distance protection function.

If it is necessary to meet the single failure criteria multiple copies of global data items will be required. Consider for instance that a single breaker can be tripped or closed from the SCADA system, the local operator, and a number of protection functions modules. Each of these functions must know if a breaker is tagged or locked out. Hence, if the functions are handled by different hardware modules, each must have these global data items stored in them.

In a strictly hierarchical system, a module at any level will contain the data bases for all lower units. Hence, in systems that are hierarchical and homogeneous, a central data base is a possible design approach. In such a system a lower level unit can always refresh its local data base as well as its part of the global data by inquiring a higher level unit provided the higher level unit is operable. This approach is however not viable for the substation environment; therefore, instead it will be assumed that the portions of the data base accessible on-line and therefore subject to change, will be maintained by each unit needing the data base for its operation and that copies of this data base segment are available in at least one other location for reconstruction of the data base after a system disturbance, such as a power failure. If there is a total system failure, failsafe recovery procedures in combination with default data base segments must be available.

Assuming a hierarchial hardware system, the top level in the station will have its own data base installed and initialised upon start-up of the system. Pieces of this data base, the global data segments, will be fed to the lower level units to enable them to operate correctly. This will include operating tags and other operational settings. If the top level fails, it can, upon recovery recall the global data base segments in the lower level units and restore parts or all of the key data. Similarly, a lower level unit can, upon recovery, get its global data base segments (settings, tags, lockout status, etc) from the higher level unit. It is possible to keep a second copy of the local data base segments in another unit in the hardware hierarchy but it may also be possible to operate from default segments in other segments stored in non-volatile memory. This is illustrated in Figure 5.4. Typical data items are listed in Tables 5.1, 5.2 and 5.3 for each level of three-level hierarchical system. The details will change depending on the functional software decomposition of the system.

Translation programs (gateways) will be needed where there are interfaces to non-compatible units. An interface to a SCADA system can be considered to be such a translation program because it maps the data of one system into the format for the other and vice-versa. Similary, if logical names are used for the data items at the highest level, they must be converted, somewhere in the system, to specific input-output point descriptions that identify the specific card and point on the card in a unit in order for the system to work. This mapping of one data space into another is an example of a translation routine.

5.3.3.3 Other Data Base Design Considerations

The data base must be secure in the sense that it is difficult for authorised people to make changes. Access codes if used should however not be used to prevent someone from viewing the operational data.

Detection of and recovery from errors is very important for the integrity of the data base. To satisfy the criteria that the system must perform critical functions even in the presence of any single failure, there must be redundancy in the data bases, although this makes it more difficult to guarantee the integrity of the data bases. Also, it makes the handling of concurrently changing data more difficult. For example, a change in breaker position may not be detected at exactly the same time by two different data acquisition units.

Consequently, one data item may show the breaker closed and the other shows it open. Preferably, this should result in a "don't know" condition unless one of the two data items can be shown through other means to be in error.

The testing of each function module must be considered in the design of the system. Under test, special data records will be used and generated that could lead to incorrect operations of other connected function modules unless the procedure is considered properly.

This means that test-generated data streams must be non-operational or invalid. Also, application programs must be properly designed so that they recognise invalid data.

A particular problem is data items updated only by exception; that is, when there is a significant change. Such designs will probably exist due to communication limitations. There are, however, some security problems in these designs because a lost data update message results in no new update until the data point changes again. Any system that uses data base update procedures of this type must have a periodic check of all the data items to ensure that a missed update is detected and corrected. This must be done in such a way that an update concurrent with a new data item change does not lead to a new error.

5.4 Some of the considerations for data structures and data bases in distributed processing systems of the type developed for substation control and protection applications have been discussed. The high speed execution required for protective relaying functions does not permit the use of conventional data base management systems for the on-line software. Economic and functional design requirements for the near term will probably limit the on-line system to data management. However, the concurrency, reliability, and systems integrity requirements make the design of the on-line data handling software for the generation of the on-line software, which must be capable of building the data bases in such a way that expansions of the system are feasible without requiring a retesting of the entire system. They must also be capable of handling systems with a variety of data base modules. To ensure software reliability, well-proven software development tools are needed.

RESIDENT DATA

Address of unit
Input point map
Output point map
Offset constants for analog inputs
Gain constant for for analog inputs
Default settings
Translation map for input/output for higher levels
Operating states (tests, service etc.)
Input contact bounce filter settings
Selftest check limits

UPWARD DATA FLOW

Data, analog and status
Error data (selftest results etc)
Operating state of unit
Output points in selected state
Output point in set or rest state

DOWNWARD DATA FLOW

Input poll initiate
Disable/enable output point
Disable/enable input point
Unit operating state select (test/service initilise)
Output point operate state (select for control and execute)
- monostable output (set/reset)
- bistable output (set/reset)
- data output (setpoint)
bounce filter settings

TABLE 5.1

DATA SET RELATED TO LEVEL 0

RESIDENT DATA

Address of umit
Input map
- level 1 to 0 (units 1 through M)
- level 1 to 2
Output map
- level 1 to 0 (units 1 through N)
- level 1 to 2
- level 1, 1 through level 1,1
Data scaling constants
Filter constants, data conversion functions
Default settings
Operating states (test, service, modes 1....J)
Selftest check limits

UPWARD DATA FLOW

Settings, function 1 through k
Data files
- analog, reprocessed (RMS, instantaneous etc)
- status
- time series data files (oscillography, events etc)
Output points selected for control
Operating state of unit

DOWNWARD DATA FLOW

Time and date
Settings, functions through k
Function disable/enable/test/initialise
Control point
- select for operation
- execute operation
- disable/enable, set/reset
Communication port, connect/disconnect

TABLE 5.2

DATA SET RELATED TO LEVEL 1

RESIDENT DATA

Address of unit
Input map
- level 2 to 1 (units 1 through X)
- level 2 to higher levels (units 1 through Y)

Output map
- level 2 to 1 (units 1 through X)
- level 2 to higher levels (units 1 through Z)

Data definition file
Default settings
Display definitions
Report format library
Selftest check limits
Operating states (test, service, modes 1....Q)
Station topology map
Settings function 1 through R
Date and time

UPWARD DATA FLOW

Data files (analog, status, time series)
Settings, functions 1 through R
Output points selected for control
Operating state of unit

DOWNWARD DATA FLOW

Time and date
Settings, functions 1 through K
Function disable/enable/test/initialise

Control point
- select for operation
- execute operation
- disable/enable, set/reset

Communication port, connect/disconnect

TABLE 5.3

DATA SET RELATED TO LEVEL 2

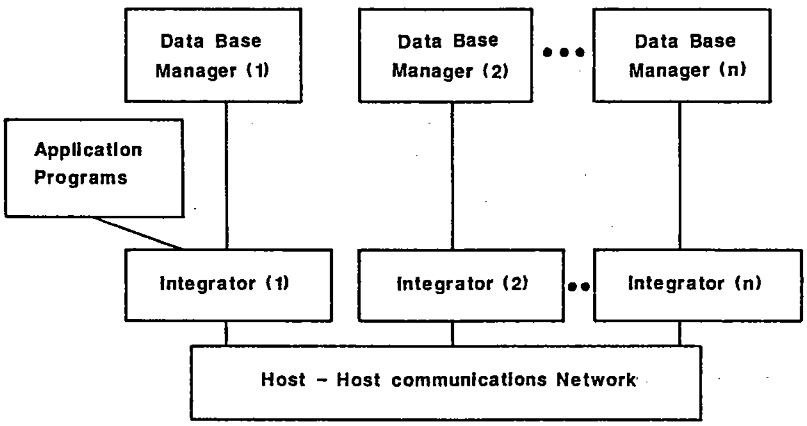

Figure 5.1 DATA BASE MANAGEMENT SYSTEM WITH SIMILAR DATA BASE MODULES

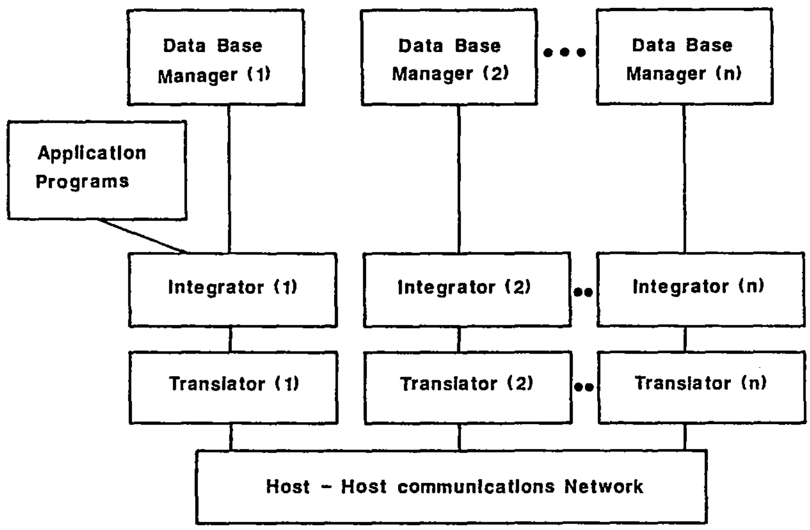

Figure 5.2 DATA BASE MANAGEMENT SYSTEM WITH DIFFERENT DATA BASE MODULES

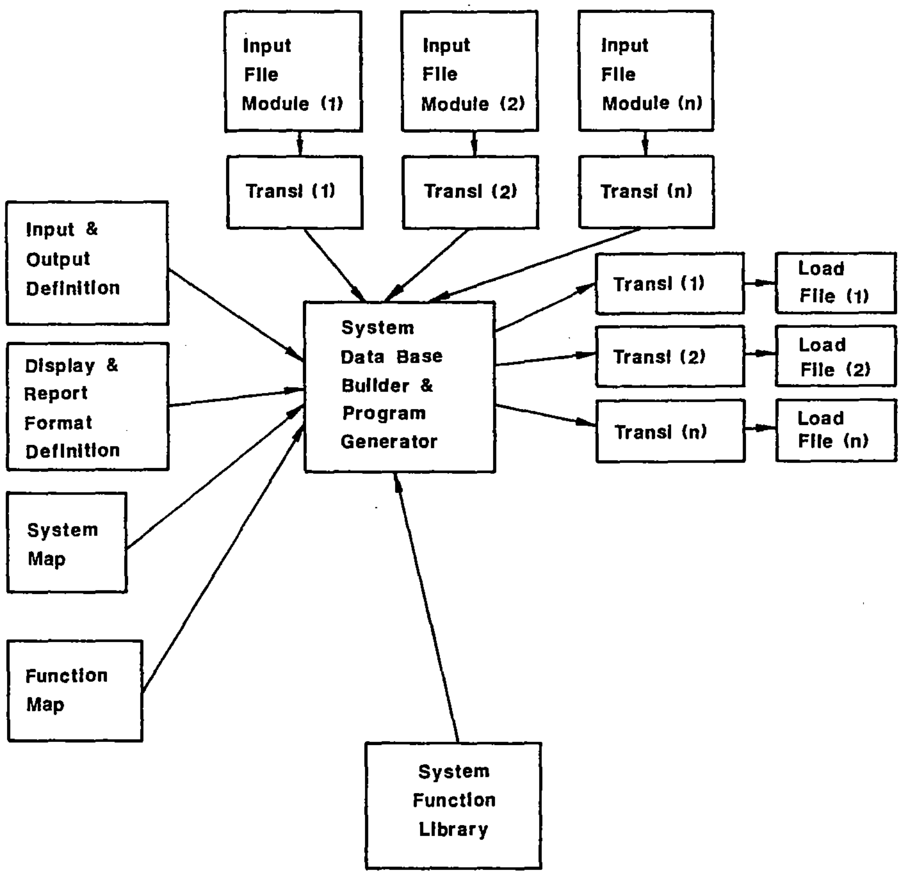

Figure 5.3 SYSTEM DATA BASE AND PROGRAM BUILDING FUNCTION WITH SYSTEM CONTAINING DIFFERENT DATA BASE MODULES

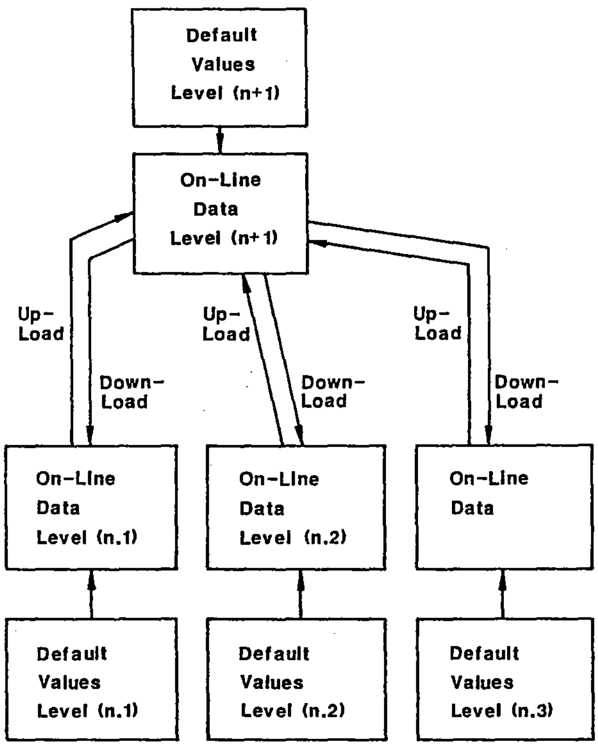

Figure 5.4 ON - LINE DATA BASE ORGANISATION

Note: Level (n+1) could be the substation computer and Level (n) could be the Protection Processors of the Substation Control and Protection System. Cold start (no operating data available) will utilize default values whereas hot start (one unit recovering from a temporary outage) will use the data base segments of operating units.

6 - Communication and Associated Protocols

6.1. Introduction

Digital Communication is the application of techniques in which information is encoded and transmitted in the form of binary sequences. Communication of digital signals between remote sites is well established in electrical utility operations, particularly in telecontrol systems. In general terms, wide area communication systems used by utilities, between substations and control centres or between substations, is strongly influenced by technology available from the telecommunications industry where digital PCM systems are rapidly being introduced.

Within substations and control centres it can be argued that it is the application of serial digital communication systems together with the microprocessor that makes possible the development of integrated schemes for control, telecontrol and protection. The driving force behind such communication systems are, not only by the telecontrol practices of the utilities, but also the needs of other industries such as computing, industrial process automation and office automation.

Substations tend to evolve over 30 years to 40 years. Thus, the instrumentation, control and protection equipments will go through many changes possibly involving two or three generations of different technologies. One must therefore assume that several generations of computer technologies will be a part of an integrated control and protection systems when a substation is fully developed. The communication systems within the integrated system may therefore be required to act as a buffer between the different technology generations. The data structures and procedures must, therefore, be compatible for the entire system, which gives a strong incentive for the adoption of standard communication protocols.

This chapter reviews the communication requirements both within and outside the substation and looks at the possible solutions available at present and in the forseeable future. Details of communication standards are given in Appendix A.

6.2. Functions and equipment

6.2.1. The functional analysis is of some importance

Contrary to point to point wiring used for central purposes in conventional substations, digital communication networks are multiplexed. Even if the communication is made up of several networks or point to point links, each medium has to transmit messages different type of satisfying the performance requirements length of the messages, or safety.

The choice of networks depends not only on the physical architecture, i.e. the set of functions and their relationships.

Functional analysis is needed to identify accurately which communications are needed by each function. Without it, we again run the risk of building a sold functional architecture with a new technology without taking full advantages of new techniques. Furthermore, incorrect restrictions can be identified or discovered during the analysis phase while significant characteristics cannot be seen during the definition stage.

6.2.2. Functional level and level of equipment

Complex control and protection systems such as those used in an electrical grid comprises a number of functions with widely varying characteristics (speed of reaction, degree of interaction with the environment or with human operators, etc.). Therefore, it seems that there are different classes of functions which involve communications. These can be put into four levels:

- Function Level 0: (FL0) — acquisition of high-voltage (HV) measurements and equipment status; tripping HV devices (sensors and acutators);
- Function Level 1 : (FL1) — automated mechanisms and systems (line protection, automatic restoration functions like reclosing, etc.);
- Function Level 2: (FL2) — real-time control and supervision

functions;

- Function Level 3: (FL3) control-dependant functions are not actually real-time time functions, e.g., maintenance, down-loading, off-line analysis etc.

Function levels are identified by the number of links that a particular function has with lower level functions, and by performance characteristics (response times, safety, etc.). For example, from a control screen (FL2) an operator is able to activate any circuit-breaker (FL0) in one second, whereas a line protection unit (FL1) activates a single circuit-breaker in twenty milliseconds after fault inception with a high degree of reliability.

These functions are shared among different categories of equipment according to the levels described in Chapter 4 (Architecture).

Communication needs vary according to the functions at are handled by the different sets of equipment. For example, the degree of preprocessing carried out by level 1 equipment determines the volume and nature of dataflows from level 1 to level 2 (e.g., degree of real-time transmission, periodic data transfers).

Items of equipment of level 1 are principally designed to perform functions of level FL1. Thus we therefore find that the levels of equipment described in Chapter 4 match the first three functional levels, but consequently, a particular functional architecture may correspond to several types of equipment architectures. Further-more, a particular level of equipment may not necessarily fit a given function level. For example:

- An operator tripping command (FL2) can be ordered from a remote centre, a substation CRT or form a feeder bay.

- An automatic switching sequence controller can be implemented at a centralized level (regional centre), at station level (level 2) or at unit level (level 1).

6.2.3. A communication system is an interface system

Data interchanges depend directly on the distribution of function within system. Sets of functions and equipment are defined and it is necessary to specify the boundaries between these sets. Communication systems emerge as a natural point or place which precisely define these interfaces.

Two types of data flows can be identified for each interface:

- Vertical communication (up and down) between different levels of equipment, e.g. circuit-breaker tripping by a protection (vertical interchange between level 1 and level 0);

- Horizontal communication (peer to peer) between the same level equipment, e.g. interchanges between a control computer and operator workstations in the control room (level 2 horizontal interchange) or between protection systems (level 1 horizontal interchange). Depending on the characteristics of data transmitted, it is important to identify whether the latter interchange should take place at the 0/1 interface.

This document will first examine the communication needs for control and protection functions before outlining possible communication infrastructures by examining the connections between the sub-systems and comparisons with international standards.

Characteristics of data transmitted

A list of interchanges possible at station level for a double bus substation is being drawn up by the CIGRE 34-03 Working Group. Hereafter, the interchanges will be primarily described from a qualitative point of view in order to identify the characteristics that must be required for transmission systems.

6.3.1. Intra-station interchanges

6.3.1.1. Interchanges Between Levels 0 and I

Two groups of data can be identified:

1-Periodic, high frequency analog data,
2-Switchgear status data and commands.

The first group comprises high-voltage measurements (current, voltage) for each feeder bay, sampled for protection needs, and for metering purposes. For voltage, two-byte samples delivered by a single voltage transducer are normally sufficient both for protection and measurement. By contrast, for currents, it may be necessary to distinguish between the channels reserved for protections high dynamics and moderate accuracy for nominal current). This arrangement corresponds to between 12 and 18 bytes depending on the data format. Current digital protection devices operate at sampling frequencies ranging from 0.24 to several kilohertz, which means that a 100kbits/s data rate per protection unit is required. Sometime, the throughput rate must be multiplied by a factor of two or more; e.g., transformer, line differential protecting systems, etc.

It should also be noted that sampling freqencies must be stable to meet the requirements of the protection devices, and that busbar protection requires a precise synchronization of samples between different level 0 modules. For example, a delay of 56 *fs* (46 *fs*) causes an extra phase shift of 1 electrical degree at 50 Hz (60 Hz).

Interchanges from level 1 to level 0 are generally commands for control of the Level 0 modules or commands for circuit-breakers, disconnectors, transformers, etc. When an insulation failure is detected, the circuit-breaker tripping command must be transmitted very quickly (2 millisecond or less).

The number of HV binary bits for state information is limited (twenty or thirty per bay). These bits contain information on the position of circuit-breakers, disconnectors and the state of inputs alarm. They must be transmitted rapidly to enable the centralized automatic and protection functions to indicate the status of substation topology in real-time and to make possible a precise time tagging of messages (unless messages are time tagged at the high voltage equipment level).

The remaining section of the 0/1 interface contains analogue data for use by monitoring euipment (e.g., oil temperature in transformers or pressure in circuit-breakers) or for maintenance purposes (e.g., total current interrupted by a circuit-breaker).

In conclusion, the communication system implemented between levels 0 and 1 must handle a high throughput volume and transmit commands at very high speed (around 1 millisecond). Furthermore, the system must be highly reliable, since it forms the link between protection systems and the high-voltage equipment.

6.3.1.2 <u>Level 1 Interchanges</u>

At this level, transmission involves binary data exchanged between automatic functions. The messages are brief and require very short transmission times (between one and a few milliseconds). From this standpoint the messages are similar to the binary data described in the preceeding section.

6.3.1.3 <u>Interchanges between level 1 and level 2</u>

The main characteristics of these interchanges are listed in tables 5.2 and 5.3 of Chapter 5. As far as communication is concerned, three types of message can be indentified at this interface:

- Type 1: Random, binary data (signals, commands), or few-byte data (parameter transmission, controls, etc.). Typical transmission time for such messages is one second or less.

- Type 2: Periodic, analogue data (telemetering information, etc.) for remote control centres. Transmission time for these messages should be 1 second (at station level).

- Type 3: Files for program downloading, database storage or fault-data records uploading. Since these messages are not composed of actual real-time data, a time-lag of several seconds or minutes is tolerable.

In most cases, transmission of these data extends beyond the station level to the remote control centres without the need for a specific processing procedure.

Average dataflows are low, but can increase drastically over a period of several milliseconds for certain kinds of faults. The system must be designed with a bandwidth high enough to absorb these bursts of data, or include prioritizing mechanisms that will accommodate a sufficiently high bandwidth for top-priority messages.

6.3.1.4 <u>Level 2 interchanges</u>

These interchanges only exist if control functions at the substation level are spread over several dedicated or duplicated computers. The definition of the architectures (physical and functional) of level 2 is necessary to define the interchange characteristics.

If the system can be considered as a distributed or duplicated data base, layer 5 (Session) or Application Service Element like FTAM may be of great use to keep data consistency.

(Note: FTAM - File Transfer and Access Management is an ISO Standard (IS 8571))

6.3.2 Communication outside the station

6.3.2.1 Interchanges Among Protection Systems

The type of interchanges depends on the nature of the protection system. Data transfers that result from protection logic are FL1 - FL1 interchanges (eg, distance relay acceleration signal), while transfers involving the exchange of high-voltage data are FL0 - FL1 interchanges (sampled currents, phase information, etc). In all cases, transmission must be rapid (a few milliseconds). The samples are sent to a limited number of destinations (typically one but sometimes two or three); the addresses are pre-identified and do not change for long periods of time.

6.3.2.2 Telecontrol and Telemetering Networks

This level primarily involves interchanges of significant volumes of Type 1 data and complete sets of Type 2 data, as described in section 6.3.1.3 of this chapter, between stations and remote control centres. These data are used in control and supervision applications (FL2) and for certain centralized protection or automatic control functions such as automatic voltage control (FL1).

The majority of the communication interchanges take place (or will take place) between level 1 and level 2 or remote equipment. The content of these messages therefore remain unaltered in transit between the originator and the end-user, even when they pass through one or more intermediate systems.

Acceptable transmission times can be several seconds, which makes it possible to adopt standard solutions. Furthermore, to ensure maximum consistency between databases that are either partially distributed or duplicated, it is preferable to adopt proven protocols that offer a very low rate of undetected errors. Because the on-line error rate is high on common carrier systems such as telephone links or PLCs, the use of well proven protocols will ensure maximum data security.

6.3.2.3 Other Types of Interchange

Broadly, this catagory of data transfers concerns functional level 3 applications, which, by definition, do not involve real-time interchanges but are typically used for remote equipment diagnostics, tests, downloading of programs or databases, uploading of fault recorder files, etc. However, such files have a large size and require very reliable transfers, as described in the preceding section. The data in these interchanges can be carried by the telecontrol network or another carrier (eg, the public switched nework). In the latter case, the system must be protected against human interference. Furthermore, the centres that process such data (maintenance centres, protection engineer office, etc) may differ from the processing centres in the telecontrol network and may therefore not have direct access to this network.

6.4. Communication system architecture

The choice of communication system architecture is closely related to the type of protection and control system architecture involved (see section 6.2 of this chapter).

Numerous parameters are to be considered, including:

Openness: the architecture selected should allow for the coexistence of different types and generations of equipment with different functions and levels of capacity.

Performance: the critical nature of dataflows and response times will vary according to the distribution of functions.

Expandability: the capacity of a system to accept new developments, which makes it possible to extend the life of a particular application.

Safety: the architecture must satisfy all safety requirements and must not endanger the operators.

Cost: the system must not be too expensive in order to warrant the investment. It will inevitably be dependent on the complexity.

Miscellaneous: integration of existing systems, protection of the environment, etc.

These criteria are interrelated, and the final solution will to some degree be a comprise. The benefits, too, are to some degree specific to each electrical utility. However, it does appear that these items do not vary a lot -- at least within developed countries -- since each utility must satisfy the same demands (performance, cost, safety, etc). The fact that a few major companies supply various electrical utilities, or that certain counries tend to pool part of their resources, serves to harmonize the views on those parameters.

However, it is generally accepted that three types of communication systems will suffice to satisfy the needs at the station level:

- level 0/level 1 communication system,
- intra-station level 1/level 2 communication system,
- communication system linking stations to remote centres.

Communication networks interface two levels of equipment in the station, and are thus of considerable strategic importance. Furthermore, the choice of a particular network for a given level is not independent of the choice of networks for the remaining levels. Close links exist between different functional levels, even when they are not adjacent. An example of this relationship is the transmission of a remote command which involves functions of level 0, 1 and 2.

These considerations have resulted in a communication system architecture composed of interconnected transmission systems (or subnetworks) that differ from each other according to the levels of performance or service required.

6.4.1 Physical architecture

Communication system architecture comprises a physical structure and protocols. Very often, network topology depends on the access method for the carrying medium, eg the CSMA/CD procedure requires a bus organization, and the token passing protocol is not the same on a bus as a ring. It must also be pointed out that full duplex transmission can only be used on point to point links. By contrast, the carrying medium is often independent of the access method (except, of course, insofar as it conforms to recent standards, which recommend using the most common forms of carriers).

Although a wide variety of media can be used for data transmission (wire pairs, coaxial cables, optical fibre, etc), it seems that fibre optics technology offers a number of advantages:

- natural isolation, between the different systems connected;
- resistance to electromagnetic interference, even at high throughputs;
- cables do not require grounding.

The use of optical fibre for point-to-point links is a proven and relatively problem-free technology. For multipoint systems such as bus LANs, there are two possibilities (Figure 6.1):

1. A passive star coupler configuration, where common mode failures are virtually impossible but in which optical components must be high efficient and the number of ports is limited (32 ports for links of less than 500 metres);

2. An active star coupler configuration, which allows for a high number of ports and increased cable lengths, but in which the coupler itself can be considered as the weak point of the communication system. However, it seems that nowadays in reality the penalty caused by such a system is insignificant.

6.4.2. Local communications

6.4.2.1. <u>Level 0/1</u>

1. <u>Point-to-point communication</u>

Point-to-point communications -- a tried and tested technology -- link two sets of equipment that communicate in a set and unchangeable manner, defined as a result of initial requirements analyses. Consequently, layers 1 and 2 of the Open Systems Interconnection (OSI) Reference Model suffice for this type of link, since the remaining categories of data interchanges are handled by specific devices. It should also be noted that openness is not of particular importance at this level. Point-to-point communication lines and circuits do not require sophisticated protocols, but effective use can be made of widely used protocols such as HDLC or SDLC, for which a large number of VLSI circuits currently exist.

At the station level, control or protection functions for a particular bay require only the data originating from its high-voltage switchgear, thereby limiting the number of physical links to a small number of channels. However, data from other sources is necessary for certain other functions, including reclosing and busbar protection. Dedicated links must therefore be created for that purpose.

2. Multipoint communications

Multipoint communciations are performed by LANs adapted for periodic transmission of analogue data or status information between transducers, switchgear and control gear, protection and automatic systems (see section 6.3.1.1 of this chapter). This type of network, known as field bus, is currently being standardized. The procedure is handled by the International Electrotechnical Commission (IEC) and particularly by the Instrument Society of America (ISA), which is currently examining a number of international proposals.

Standardization could make it possible to harmonize interchanges between Level 0 and Level 1 for certain architectures.

The field busses could replace links between measurement transformers, switchgear and control gear for only a single protective unit (unit level) or for all the equipment of the substation (substation network).

At unit level, a dedicated network handles communications for each feeder bay (or overlaps with a second feeder bay to ensure redundancy), linking the switchgear and control gear, and the measurement transformers of the associated unit. The throughput of the field bus is moderate (several hundred kbits/s), because there are few nodes. The period can be adjusted to match the acquisition cycles of the protection systems. This solution has the advantage of being simple, but it does not allow centralized sample-processing, (eg differential busbar relaying systems) which must be performed by conventional equipment or a more sophisticated system.

In the second instance (substation network), all level 0 data are distributed to the complete level 1 equipment network via a field bus, which can be designated as "measuring network" since its primary function is to distribute current and voltage samples. This "fully integrated" architecture maximizes the potential of digital technologies while at the same time simplfying station infrastructure. However, a number of questions arises as to the possibility of implementing measuring network architecture in the short term.

Advantages:

- All data, including measurements, are broadcasted to all nodes. It is therefore simple to modify or adjust a function by simply modifying the software.

- Inter-unit functions such as voltage control are easily provided for.

- Differential busbar protection can be a node and may not require specific cables and wires.

- Level 1 equipment can be non-dedicated (in which case, only software is different).

- Excellent function availability can be obtained easily and with minimal hardware requirements. Functions of level 1 equipment can be carried out by any available piece of hardware after downloading of streamlined database (if necessary).

- The network can synchronise the sampling units.

- Hardware can be regrouped in a single area, independent of station layout, while retaining a distributed operating structure. This capacity allows for better protection against environment (extreme temperatures, electromagnetic interference, etc), and simplifies power supply to the equipment and station infrastructure.

Disadvantages and Uncertainties:

- Required levels of performance are very high (tens of thousands of frames per second).

- Certain level 1 features (eg differential busbar protection) must be capable of handling high dataflows. The desire to simplify functions may thus lead to the use of increasingly sophisticated technologies for level 1 equipment. In other words, very high data rates increases the cost of the interface components to level 1.

- Given the levels of performance required, the nodes are numerous.

- The network must have a high reliability, and more especially must be fault tolerant. In order to achieve this level of security, the system must be duplexed or equipped with a backup system that is sufficiently powerful to ensure the continuity of the station's vital functions.

- The data refresh cycle must be compatible with the acquisition cycle of all levels of protection equipment, irrespective of origin and operating principles. Furthermore, standardization in this sector is highly desirable, especially when digital output measurement transducers are involved.

- This type of architecture is more particularly suitable to new stations.

6.4.2.2 Level 1/2

At this level of interface, the system is required to connect up to thirty or forty microcomputers, which interchange information of different types (section 6.3.1.3 of this chapter). This task can also be performed by a LAN. Even though other solutions are technically feasible, it would appear that they do not appeal to the majority of electrical utilities. Consequently, the remainder of this section will deal exclusively with LANs.

As seen in section 6.2 of this chapter, communication system architecture depends on how the functions are distributed among the different types of hardware modules and on the choice of network to handle interchange among level 1 functions. This latter factor has a direct influence on performance.
When making the final choice, users must consider a number of basic criteria that exert an overwhelming influence on the choice of protocol:

- specified transmission times ie if the network is required or not to transmit messages in few milliseconds;

- the expandability required, both for hardware and application software;

- interconnection with other networks, ie whether the network is to be considered as an isolated subnetwork or as a component of a wider communications infrastructure, which connects LANs with WANs (Wide Area Networks).

The above considerations narrow the field to a choice between collapsed architecture, which sacrifices numbers of services for enhanced performance, and a full architecture, as recommended by the ISO via its OSI Reference Model (see Appendix A).

Full architectures

Key features:

- full conformity to OSI profile, ie integration of layers 1 to 7 protocols;

- end-to-end communications, which make possible to use intermediate systems (routers or Level 4 gateways) specified by ISO;

- certified protocols;

- reliable transmission;

- open architecture that is both upgradable and interconnectable;

- full architecture is only of interest if the WANs connected to the station are also built to the ISO standard;

- performance is only just beginning to show signs of improvement. For example, some vendors are offering couplers for MAP LANs (Manufacturing Automation Protocol) with end to end response times of around 20 milliseconds and a throughout of 2 Mbits/s;

- present costs vary from between US$ 1000 and US$ 7000 per node depending on he capacity of the coupler (chip and memory capacity, type of modulation etc);

- organisation such as the Corporation for Open Systems (COS), the Standards Promotion and Application Group (SPAG), or developments such as the Technical and Office Protocol (TOP) recommend OSI-type configurations in sectors that are not specifically related to the power industry.

Other developments such as MAP (see appendix A) have accelerated the overall OSI standardization procedure and have led to the specification of industrial standards such as the Manufacturing Messaging Specification (MMS).

Collapsed architectures

Key features:

- Collapsed architectures are limited to layers 1, 2 and 7 of the OSI model. It should, however, be pointed out that layer 7 (Application) protocols differ slightly from full architecture protocols since they are obliged to partially reconstitute the mechanisms that are generally managed by layers 4 and 5 (Transport and Session).

- They are especially suited to rapid transmission of short messages.

- They offer limied upgradability (eg it is difficult to integrate ISO protocols other than MMS).

- They are isolated networks that can only communicate with other networks through a specific gateway; they are not OSI architectures.

- Connection costs are lower than with full architectures (starting at US$ 1000).

- Performance is halfway between the field bus and full-scale architecture levels (ie between 10 and 30 milliseconds for urgent messages).

- This type of architecture can be found in numerous industry-specific applications. The standardization of architectures of this kind has been attempted through Mini-MAP, a MAP spin-off that is less advanced that the Full-MAP specification. Two problems that remain to be solved are the adaptation of MMS to a collapsed profile and its connection to Full-MAP architecture.

- The services offered by collapsed architectures are similar to those of the field bus, but with lower levels of performance. With the arrival of high-efficiency full achitectures, reduced configurations such as Mini-MAP will probably make way for complete profiles or field buses.

6.5. Wide area communication

Extra-station communication is being investigated by the CIGRE WG 35-02 (Digital Telecommunication Network) and WG 35-03 (Digital Communications for Telecontrol) working groups. This section will summarize the activities of the principal standard bodies in that field and will examine the influence of the choice of WAN configurations on the internal communications infrastructure of the station.

Three standard bodies are active in the field of remote data interchange. These are the CCITT, the IEC and the ISO. When both ISO and CCITT standards exist in the field of distributed processing, they are broadly similar.

For the lower layers, the network can be modelled on existing public switched networks. Two types of profile exist according to whether layer 3 (Network) is configured in connection or connectionless modes (ie X.25 or INTERNET). ISO is alone in specifying standards for INTERNET, which demands a Transport layer that incorporates error-detection mechanisms.

For the upper layers of the model, specific developments should begin to appear for layer 7 (Application); however, it is not possible to rule out the fact that services will be provided to a large extent by Application services element such as MMS. A fully standardized configuration is suitable for FL3 applications. It should be pointed out that a public network can be used for this type of interchange on condition that certain precautions are taken to prevent unauthorized connection.

Until the last few years, the IEC has chosen to follow an independent path, with the objective of standardizing a communication protocol for telecontrol. Recently, alongside this project and due to the drawbacks of such an approach, a new working group has been set up to study the harmonizations of ISO and CCITT protocols for telecontrol.

6.6. LAN/WAN interconnection

The choice of a network relies in part on the way in which external communciations are handled. Communication between a piece of level 1 hardware and a machine on a remote site can be performed in two ways (figure 6.2):

1. via a functional level 2 control application

2. via a standardized LAN/WAN gateway

In the first instance, an application forms a screen between the station and the telecontrol system, making it possible to use specific features on either side of the gateway. Simplified protocols -- and therefore simplified transmission couplers -- can be used for the 1/2 interface at the station level. For example, the Network layer may not exist since the applications of the station that receives and processes messages is aware of their destination.

A collapsed architecture may be appropriate if it is considered that the error rate per bit is low compared to the error rate observed with WANs. This solution appears attractive at first sight, since it allows the users to upgrade technical solutions for local control and telecontrol independently. In many cases, point-to-point telephone links will remain the most common form of intersite communications. Collapsed profile LANs (which may be standardized) may be chosen as an interim solution for real time intra-station communications until the introduction of suitably efficient field busses which can then handle level 1 - horizontal communciations.

In the second instance, communications between a level 1 applications and a remote application is handled by a standardized LAN, a standardized WAN and by intermediate systems. Dataflows for these can be higher. For example, remote signals must be sent from each piece of level 1 hardware to all the machines involved in the control process.

The first alternative appears simple to implement, and may generate savings in the short term. However, such a solution relies on designing a gateway that allows for the communications needs defined at the moment of conception. Complications that appear in later phases of development can paralyse the upgradability of the entire system. A complete standardized profile for a LAN is clearly safer and more open, both for local- area and remote communications. The problem of communication becomes transparent to users at the application level (although perhaps not at the performance level), and is therefore more transparent to designers. Such a solution is particularly interesting, if external communication are handled by a standardized WAN.

6.7. Standardization and the industrial environment

The standardization of communications sytems has only become an issue in the industrial sector in recent years, as a result of efforts to impose standards in other sectors. For this reason, a number of specifically industrial needs have not yet received sufficient attention. For example:

- redundancy of media (although solutions are scheduled to appear in the near future under MAP);

- broadcasting at the Transport of Application layers

- protection against unauthorized connections

- accurate synchronization of equipment etc

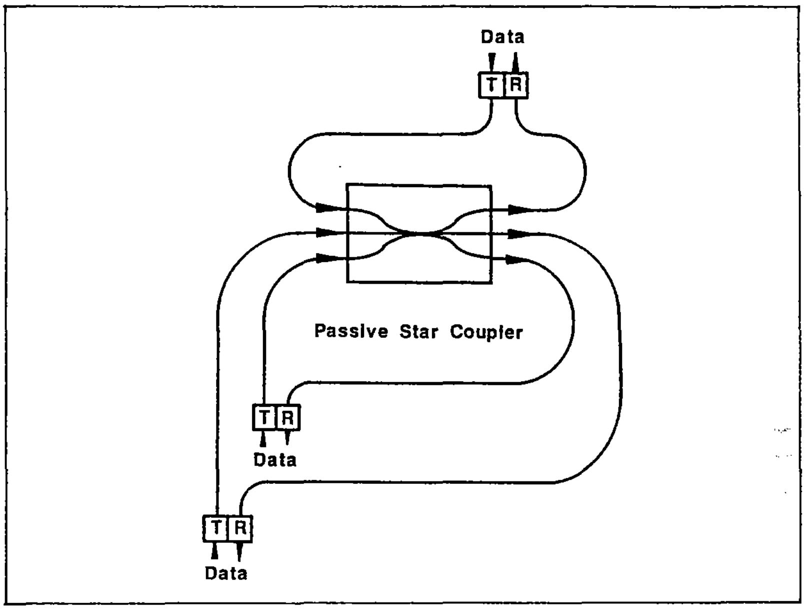

Figure 6.1a PASSIVE STAR NETWORK

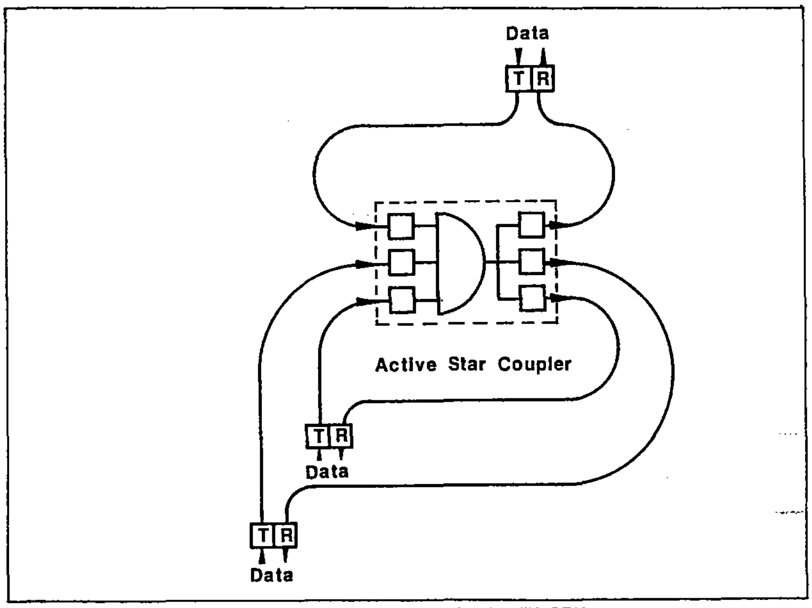

Figure 6.1b ACTIVE STAR NETWORK

Figure 6.1 OPTICAL FIBRE LAN TOPOLOGIES

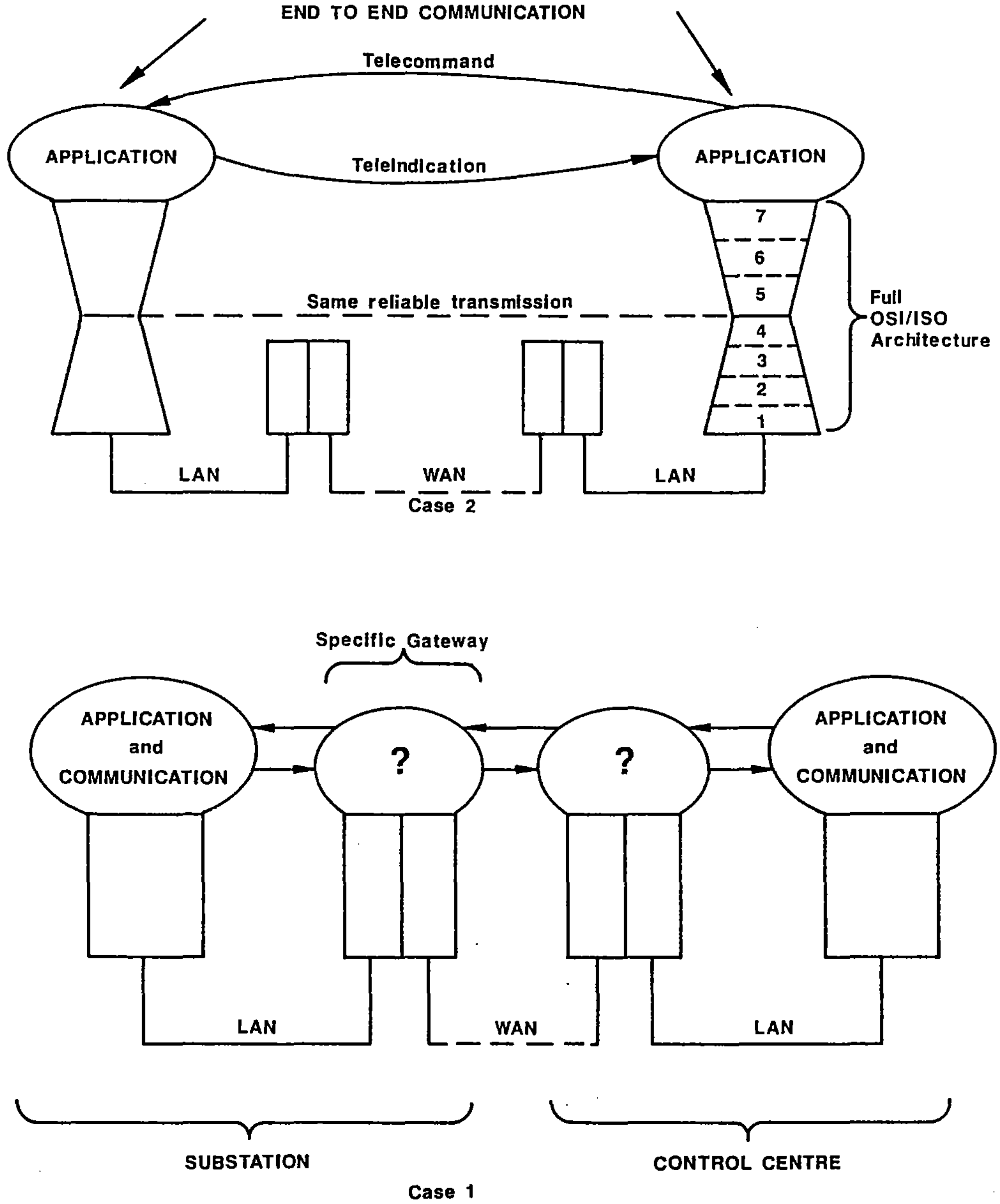

Figure 6.2 LAN/WAN INTERCONNECTION

7 - Conclusions

7.1 The hardware and analogue techniques used in sub-station control in the past are no longer readily available and are being replaced by suppliers witn digital techniques. It is therefore no longer possible for the user to continue with existing practices and changes must be made to digital techniques.

7.2 The integrated system solution is feasible technically with modern technology. The economic feasibility of introducing total integrated systems is still in question. Future trends indicate that it will become economic and therefore extensions and replacements should be compatible with the new technique to allow changeover at the appropriate time.

7.3 The transition to integrated control will have major organisational impact in the maintenance and construction aspects and also the operational methods of utilities. The full advantages of the new system are yet to be understood. New facilities will create new demands i.e. better diagnostics both in detail and speed, ability to work to closer limits and faster restoration times. Present trends indicate that the transmission system will be required to be much more flexible to allow operational demands such as combined heat and power systems, co-generation with industry suppling electricity back to the system. Integrated control will provide the flexibility to meet these new demands.

7.4 Introduction of integrated control will have a major impact on the primary/secondary plant interface. At present with the complications required in modern sub-stations this interface has a major impact on cost and design of primary plant. In future secondary requirements will be reduced and shared throughout the sub-station control/ protection system via the integrated control system.

7.5 Except in a very few cases, present applications of digital techniques do not include protection. Whilst this will be the case for a number of years until the technology has improved and obtained respectability, it is thought that eventually control and protection will be integrated fully.

7.6 The major factor which is slowing progress in the field and preventing implementation is the lack of a standard for communications within the integrated system. Various utilities have adopted different standards, some designing their own whilst others rely on industry standards which at present are less than satisfactory in every sense. Development of a suitable standard will allow part implementation with suitable interfaces to expand as this becomes economically justified. It will also allow equipment to be mixed from different manufacturers and generations.

7.7 The life cycle of hardware will almost certainly be less than the present 20 years which most utilities require. A figure of nearer 10 years is thought likely. The system must be sufficiently flexible to allow the introduction of new hardware as required with minimum cost and disturbance. This underlines the need for a suitable standard.

7.8 New products are required from manufacturersto meet the demands of integrated control. However, because of variation in a take-up both old and new systems will have to be maintained for some time. Design will be inbedded in the system rather than the components thus allowing off site testing and reducing installation/ commissioning time/costs.

7.9 The introduction of large scale integration is likely to reduce the number of suppliers to the power industry. Standardisation between suppliers must be maintained to allow competitive purchase of upgrades and expansions.

7.10 The major new factor which is introduced into the design by the integrated control approach is the total reliance on software. Whilst there have been major advances in this field it is thought that the development, design and implementation of software techniques is still in its infancy. Techniques are and will continue to evolve from the main users of software systems such as business, manufacturing industries and the military. Integrated sub-station control will rely heavily for its progress on developments in these major fields. It is most akin to the process control industry and may well be able to use many of the techniques adopted by it. In order to make most use of these developments every attempt should be made to follow industry standards and not invent peculiarities for sub-station use.

APPENDIX A

COMMUNICATION STANDARDS

1 - Introduction

Standardization in the field of communication systems offers many advantages such as:

- safety, through the utilization of tested protocol and the use of highly integrated circuits made possible by the wide spread availability of products

- open networks, which facilitate the connection of equipment of different manufacturers and therefore avoid the problem with users becoming captive to a particular development at a given time or to a very limited number of vendors

- network evolution, which allows for change or for modification of a part of the system without major expenditure

- low costs, made possible by the use of high volume production

The number and variety of fields covered by the standards applicable to the monitoring and protection of transmission grids (computer languages, electro-magnetic disturbances, operating systems, etc) are too great to be presented in this document. This section is intended to present succinctly the state of the art for the main standardization projects which could be used for our applications in the area of communications.

2 - Main Organization in Charge of Standardization

The discussion is limited to international organisations and certain other associations which have played an active role in the standardization of communication systems.

- CCIT

The "Comite Consultatif pour le Telegraphe et le Telephone" (International Consultative Committee for Telegraphy and Telephony) bring together both public and private telecommunication organisations. It has undertaken studies on the ISDN, messaging services (X 400) and packet switching (X 25).

CCITT and ISO have agreed to co-operate in the field of network interconnection and to conduct joint studies. The recommendations of the CCITT are international standards designated by a letter specifying the topic, followed by two or three figures:

. T series: office information systems (eg T100)

. V series: data transmission on telephone network (eg V24, V35)

. X series: data transmission networks (eg X21, X25, X32)

- ISO

The International Standards Organisation groups 87 national standardization organisations. The OSI (Open Systems Interconnection) covers all the studies conducted by the ISO for open computer systems interconnection.

- IEC

The International Electrotechnical Commission deals basically with electricity standards, but industrial applications such as process control have led it to cover communication networks.

Its technical committee 65, which is responsible for industrial process measurement and control, has promulgated the PROWAY-C standard and a "field-bus" project.

Its technical committee 57, which is responsible for telecontrol, teleprotection and associated telecommunications for electric power systems, is working on a set of standards relating to protocols in telecontrol field.

- IEEE

The Institute of Electrical and Electronics Engineers is a forum for writing standards with particular influence at ANSI (x), regarding local networks.

Note - ANSI: American National Standards Institute; ANSI is the US national body of ISO and IEC.

- EIA

The Electronic Industries Association is an American professional organisation which is mainly known for its definition of interfaces such as RS 232, RS 422, and its studies of a future standard relating to an application level of MAP (Manufacturing Message Specification) for industrial processes.

- ECMA

The European Computer Manufacturers Association groups roughly twenty European computer manufacturers. It participates in the work of the ISO and the CCITT and has performed major studies in the field of local networks.

- ISA

In the LANs field, the Instrument Society of America is in charge of pre-standardisation of field-busses (scope of SP 50) and of the use of MAP in the process industry (scope of SP 72).

3 - The OSI Reference Model

3.1 Why such a Model?

To enable various heterogeneous units of equipment to communicate is a complex job. Consequently, it is indispensable to divide the general problem of communication into different sub-problems which can be treated separately.

Before the emergence of standards in this field, computer manufacturers were marketing their own proprietary systems. As a result, these models are generally closed, although they are all layered models and generally provide the same services.

Basically at the request of users, ISO has examined the delicate problem of opening communication systems and has proposed a seven layer model: the OSI reference model (Open Systems Interconnection) '1§. Especially because of the diversity of needs, not all these levels are completely standardized, and when they are, the standards relate more to office automation function than industrial applications. It should nevertheless be observed that action in this direction has begun over the last few years, in the field of industrial control systems (MAP project).

3.2 Presentation of the Model

The main advantage of a layered model is the limited number of interfaces a given element of the model has to know. Indeed, layer N is only aware of (and must only be aware of) its interfaces with layers N + 1 and N - 1. It relies on he services of layer N - 1 provided via access points (SAP) to communicate with layer N of different equipment. The set of rules implemented in a layer to communicate via an interface is known as the protocol. The standardization of a layer requires a standard relating to services and a standard relating to the protocol.

The characteristics of the different layers are summarized below:

1. The physical layer performs the transmission of information on the medium. The unit of information processed is the bit. In particular, the communication medium or media and the characteristics of emission and reception elements are defined in this layer.

2. The data link layer provides the functional and procedural means to transfer data between networks entities and to detect (and sometimes correct) errors which may occur in the physical layer.

3. The network layer is responsible for conveying messaes between non-adjacent nodes. As a matter of fact in the case of meshed networks, the data packets can cross several intermediate nodes before reaching their destination.

4. The transport layer performs transmission of data which must be transparent and reliable between end systems, meaning that the layer must check that the messages have correctly reached their destination. If necessary, this level divides messages into blocks for emission and re-assembles the blocks for reception.

5. The session layer provides the mechanisms for organizing and structuring the interactions between application processes.

6. The presentation layer frees the applications processes from concern with differences in data representation.

7. The application layer provides all the services which can be directly understood by the application programmes.

This architecture provides a useful understanding of the various elements entering into a distributed system.

Most of the services offered by these layers can be connection orientated mode or connectionless orientated mode.

For the first mode, a connection between layers must be negotiated before sending the data. This mode creates a path over which will pass the packets of a same message (virtual circuit) and manages all the specific services of the layer (eg flow control, detection of errors, recovery of errors).

As regards the second mode, also referred to as datagram mode, the information tansmitted is fully contained in a packet. No prior negotiation is necessary between layers and the services rendered are very limited: no flow regulation, no aggregate error check for a set of packets, no segmentation of messages into packets, no real acknowledgement between layer, etc.

3.3 Implementation of the Model

Not all applications necessarily require the services of all levels, and not all layers are necessarily used: the extent depends on the degree of opening desired. For instance, the third layer is quite frequently non-existent for local networks which do not communicate with the outside. Moreover, some of the services required by applications may not be supplied, or are provided with inadequate service quality (eg the need for short transmission times, the need for synchronizing equipment, or the guarantee or enhanced operating reliability for many industrial applications).

The cost of a standardized system can also be too high by comparison with much simpler, but sufficient systems.

The communication system and the host computers must match in both economic and technical terms.

The services of all the layers of the model are not necessarily required for given applications.

In this context, a modification of the existing standards of the use of non-standardized systems may be necessary. However, one should be aware here of the risk incurred in adopting such architectures. Their advantages can be very small and temporary compared to a complexity and a reliability rarely satisfactory if the spreading of these products remains limited.

By contrast, the connection of different heterogeneous units of equipment while securing the upgrade path of both equipment and applications necessitates the definition of each layer.

The purpose of the OSI model is to connect reliably various units of equipment by formalizing with accuracy the tasks associated with exchanges of information. The distributed applications must then be liberated of tasks that are specific to data exchange. Partial implementation of layers shift certain communication problems to the applications level (eg checking errors, synchronisation), raising the question of the validation of the specific solutions found for these problems.

Making communication possible also means that all the equipment connected must respect the same specifications (and therefore the same standards and the same options) for all equipment, and moreover, must do so for all the layers used. Hence the idea of a communication functional profile which consists of selecting within the standards adopted the same options and parameters for all the couplers to be connected.

4 - Long Distance Networks

4.1 HDLC '2§

HDLC (Hight-Level Data Link Control) is a set of categories of data link procedure standardize by ISO, very much in use for point to point communication between distant nodes. There are many options, involving choices with a view to minimize the operating cost of the link. Consequently, categories of procedures have been defined to specify a set of basic functions by indicating a list of commands and responses. Three modes can be selected:

. unbalanced mode with a normal response in which the receiver can only transmit with the permission from the emitter;

. unbalanced mode with asynchronous response in which the receiver can transmit without permission from the emitter;

. balanced mode in which the receiver can transmit without permission.

The boundary of the frame (figure A1) is delimited by two flags represented by a special binary profile (0 111111 0) which also serve as a synchronisation profile. To avoid mistaking a binary series which looks like a flag with a flag, a 0 is inserted after each series of five 1. The inserted bits are deleted on reception.

The frame is made up of 4 fields:

. the address field which can only take two values (emitter or receiver)

. the control field which indicates he type and number of the frame

. the field of data transmitted to the upper level

. the frame check sequence field (FCS)

The HDLC procedure is widely used and is implemented in VLSI circuit for flows of between a few kilobits per sec up to 10 MBits per sec.

4.2 X 25

Protocol X25 covers the first three layers of the OSI model.

The physical level basically originates from the specification X21. Layer 2 is formed of a sub-set of the HDLC standard (balanced mode, LAP - B).

The latest standard for the layer 3 is referenced X25 -1984 '5§. This protocol uses the virtual circuit concept. It multiplexes on level 2 virtual circuits which are bi-directional associations of logical channels. The use of a network layer economises on the numbe of links over the communication network as a whole.

These protocols are used in some large national data transmission networks. Their use could be envisaged for remote control operation or other operations requiring long distance links in private or even public networks.

4.3 IEC Project

The studies conducted by IEC TC 57 relate to telecontrol, teleprotection and associated telecommunication for electric power systems. A set of documents presently being drawn up by this Committee deals with transmission protocols. The standard "TRANSMISSION FRAME FORMAT" is under printing and work is proceeding on other standards:

. transmission procedures

. data presentation

This standard specifies half duplex and full duplex link protocols that provide only window size one for error recovery procedures. The specified protocols are restricted to Telecontrol system with multiple point-to-point, multipoint-star, multipoint-partyline and multipoint-ring configurations.

Three frame formats are defined to meet the criteria of the three types of data integrity and transmission efficiency. Three types of frames are associated with each of these formats; their size varies depending on the nature of the information to be transmitted; long frames for transmission of data comprising four fields (length, control, address and data), short frames for the management of the protocol which only includes the control and address fields, and the "character" frames of one byte for acknowledgement.

New work is proceeding on the creation of standards relating to telecommunication for telecontrol in the context of transmission protocols compatible with the international standards of ISO and CCITT.

The new protocols will cover specification for data transmission in hierarchical or meshed network configurations utilizing store and forward techniques and packet switching techniques for messages with corresponding eror recovery procedures with window size greater than one.

4.4 ISDN

Integrated Services Digital Networks are multi-purpose: end to end digital connection, many services offered on 64 kbits per sec transmission channels (also referred to as B channels) with which are associated an independent channel referred to as semaphore channel (or the D channel), standard interfaces and conversion functions to render access transparent to the user.

ISDN provides two types of access to the user: primary and basic.

Primary access, whose standardizstion differs from continent to continent. It is made up of 23 (in the United States) or 30 (in Europe) B channels and one D channel at 64 kbits per sec, whereas basic access comprises only two B channels and a 16 kbits per sec - D channel.

The specifications of the ISDN are designed to inlcude services such as telephone, telecopy, videotex, etc, as well as packet switching transmission.

In the long term, the ISDN will offer three types of services:

. basic support services which provide transmission resources (stop at layer 3 of the OSI model)

. teleservices which, in contrast with the first group, cover the seven layers of the model by including all the resources needed for data exchange

. additional services (only some of them are standardized today)

This type of network will certainly influence how utilities deal with long distance communications over the next decade.

5 - Local Networks

5.1 IEEE Project 802

In February 1980, the IEEE (Institute of Electrical and Electronics Engineers) launched project 802 to define a standard for local communication networks. The aim was to concentrate efforts in this field to meet a rapidly growing market and obtain low connection costs. Differences in users' needs and pressure from large manufacturers have led the IEEE to draw up projects for several networks (reference numbers: 802.3, 802.4, 802.5, 802.6, etc). Most of these projects are currently being ratified by the ISO and bear the reference numbers 8802/1, 8802/2, etc.

Committee 802.1 was assigned the task of describing the relationships between the documents recommended by the different committees and the OSI system. It also defines the function of network management which allows the communicaion system to be monitored (failure detection, analysis of traffic).

Project 802.2 describes one of the two sub-layers of the data link layer (LCC sub-layer: Logical Link Control sub-layer).

The other documents cover the lower sub-layer of the data link layer which describes the access mode to the medium (Medium Access Control (MAC) sub-layer) and the physical level.

5.2 Logical link control layer (IEEE 802.2) ˙7§

This document groups the services of layer 2 which may be common to networks which use different access mode. The user can choose between three categories of services:

. class 1: it is a connectionless mode. The additional service offered by this sub-layer is therefore virtually non-existent.

. class 2: in addition to the services of category 1, this category offers a service with connection. It performs messages acknowledgement, flow regulation and recovery of errors from level 2

. class 3: in this category, point to point frames can be acknowledged immediately

5.3 Contention network (IEEE 802.3) ˙8§

This standard has been derived from ETHERNET. It operates at 10 Mbits per sec with Manchester-code, and the medium is formed of coaxial cable segments. The access mode is managed by a CSMA/CD procedure. According to this protocol, any station deciding to transmit can do so after having checked that the medium is free (carrier sense). However, sometimes, several stations may start emitting at the same time (to within the propagation time of signals), leading to a collision of messages which is detected locally by each station. Any station in conflict with the others re-transmits its message after a random delay.

The advantage of this protocol is that it is simple, and therefore very robust. Access to the carrier is very rapid at low load. However, since the emission algorithm is probabilistic, a maximum size of the frames is set by the topology of the network. Several manufacturers are proposing adaptations to fiber optics.

5.4 Token bus (IEEE 802.4) ˙9§

The co-called "token passing on bus" protocol is a relatively recent technique for access on a broadcast medium which is an adaptation of token ring mechanism on bus. This technique allows the bandwidth of the communication medium to be properly filled when the load is high and well distributed. In contrast to contention protocol, it guarantees a maximum transmission delay for sending urgent messages at the level of layer 2 (MAC sublayer). However, the need for a station to wait for the arrival of the token before transmitting can lead to a certain inefficiency when many stations are connected and the communicating applications are centralised.

The complexity of this protocol does not lie in the way in which the automatic system controlling normal operation is implemented, but rather in the recovery procedures following a temporary (ie loss of the token) or definitive (ie loss of a station) malfunction. In general the quality of this access mode is related to its ability to return to normal operation after an incident, without having systematically to start the re-initiation phases of all or part of the system afresh.

The stations on the bus form a logical ring, meaning that every station has a logical identifier (each identifier is different), and knows the identifiers of the preceding and the following station on this virtual ring (Figure A3).

A control frame, referred to as a token, controls the right of access to the medium. This frame contains a destination address which is nothing but the identifier of a station. The station which receives the token takes control of the bus for a given length of time during which the station can emit one or more frames, request a message from other stations or test whether a new unit or equipment is requesting connection to the network. It then passes the token on to the next station on the logical ring. Equipment can be connected to the bus without connection to the logical ring. In this case, it can only respond to requests formulated by the stations on the ring.

The network control and management frames managed by the MAC sub-layer 2 alternate on the communication medium with frames containing the data which are sent to the upper level (LLC sub-layer).

The standard includes several speeds and modulation modes:

. continuous FSK (Frequency Shift Keying) at 1 Mbit per sec

. coherent FSK at 1 or 5 Mbits per sec

. AM/PSK (Amplitude Modulated and Phase Shift Keying) at 5 or 10 Mbits per sec for broadband network

Coaxial cable is the recommended medium, but adaptations on fibre optics already exist.

5.5 Token ring (IEEE 802.5) °10§

The token ring technique is based on the use of a frame (token) that circulates around the ring when all stations are idle. A station wishing to transmit must wait until it detects a token passing by. It then changes the token from "free token" to "busy token". The station then transmits a frame immediately following the busy token.

There is now no free token on the ring, so other stations wishing to transmit must wait. The frame on the ring will make a round trip and be purged by the transmitting station. The transmitting station will insert a new free token on the ring when the station has completed transmission of its frame and the busy token has returned to the station.

For the present, this product is used more for office than for industrial applications.

5.6 Proway-C (IEC 655)

The purpose of the PROWAY study is to create a true digital local network for industrial applications which is rapid, safe and quite immune to electro-magnetic disturbances.

The general enthusiasm for the IEEE project 802.4 led the standardization committee to direct the studies towards a compatibility between PROWAY and IEEE 802.4, leading to the draft standard PROWAY-C. The link level of PROWAY-C is an over-set of the link level of 802.4 which was adopted for the MINI-MAP architecture.

The main characteristics of this network are as follows:

. access mode: token passing

. covers the physical level and MAC level of the data link layer

. maximum number of stations: 100

. maximum bus length: 2000 metres

. binary flow: 1 Mbit per sec

. data circuit bit error rate: less than 10^{-8}

. residual error rate: less than 3.10^{-15} at a bit error rate of 10^{-6}

. maximum length of the data field in the frame: 1000 bytes

. information transfer rate over 300 kbits/s

. access time to the medium: less than 10 ms

5.7 Field bus (IEC)

The term "field bus" refers to a set of local networks designed to acquire measurements or states transmitted by sensors and to send commands to actuators. Management is centralised, one master-station distributing cyclically a right of transmission to the other stations on a medium that can be doubled.

Today, cycle times are still too long (of the order of five milliseconds) to be suitable as an interface between levels 0 and 1 of stations, ie to be able to transmit information coming from the high voltage system to the protections and automatic system (states, currents and voltages), and to send commands to high voltage apparatus. However, a move towards faster frequencies is envisaged.

5.8 Digital Protective Relay System Interface Standard

(IEEE)

This is IEEE project PC 77.107, which has the aim to develop a standard for local man-machine interfaces, interfaces between protective relaying function modules in a digital protective relaying system and for interfaces to switchgear, switchboard devices, and communication equipment for protective relaying purposes.

6 - The Map Project

6.1 Origin of the project

GENERAL MOTORS developed the Manufacturing Automation Protocol in order to obtain a fully flexible production. The MAP project consists of defining communication profiles suitable for the industrial world, ie within the existing standards, to choose appropriate standards and options, and, if necessary to accelerate the process of standardization of certain projects.

6.2 General description

In MAP, communication is effected by a set of hierachized networks. At the top of the hierachy, there is one or more broadband networks which are the backbone of the whole system ("backbone" network, also called full architecture or Full MAP). Architectures whose orientation is much more towards rapid real time operation (Mini-MAP or even EPA: Enhanced Performance Architecture), or mixed MAP/EPA architectures, are linked to this network.

6.3 The full architecture

This is a true ISO communication profile. It is based on the specifications set out below (version 3.0, July 87) '11§:

1. Layer 1: broad band modulation and flow of 10 Mbits/sec. '9§

2. Layer 2:
. MAC sub-layer: token bus (IEEE 802.4

. LLC sub-layer: protocol without connection (LLC 1) '7§

3. Layer 3: ISO protocol without connection (Full Internet) '4§

4. Layer 4: ISO transmission layer, class 4 '6§

5. Layer 5: ISO Session '12§

6. Layer 6: ISO Presentation '13§

7. Layer 7: Not yet fully settled, but will contain ISO protocols such as CASE (Common Application Service Element) '14§, FTAM (File, Transfert, Access and Management) '15§ and/or MMS (Manufacturing Message Service) '16§, and Specific Application Service Elements to give services which are not covered by MMS and FTAM.

This architecture makes it possible to communicate with the outside world (public or other local network) via a standardized gateway at transport level. The services offered are very complete with, as a result, response times at application level which are not guaranteed and can be long for non optimized implementation.

6.4 MINI-MAP Network

It only covers the first two layers of the OSI model, and the seventh layer which is an adaptation of MMS on the data link layer.

1. Physical layer: coherent FSK modulation single channel at 5 Mbits per sec

2. ink layer:

. MAC sub-layer: token bus (IEEE 802.4) including the SDA and RDR options of PROWAY

. LLC sub-layer: IEEE 802.2, clause 3

By the use of priority, mechanisms transmission time can be guaranteed at the level of layer 2 for top-priority messages during normal or slightly disturbed operating conditions. this implies a limit on the size of all messages. For instance, 25 msec can be guaranteed when the limit is 256 bytes of data for 40 station-segment.

Thanks to PROWAY options, the station which has the token can delegate temporarily its right of access to the receiver station.

The SDA Option (Send Data, Acknowledge) allows the latter to acknowledge the message immediately, while the RDR option (Receive Data, Reply) allows it to return a short frame.

Mini-MAP is therefore a network, orientated towards real time operation.

Its efficiency is secured by sacrificing certain services offered by a full OSI architecture; for instance:

. the services offered do not guarantee end to end transmission of messages. They simply guarantee safe transmission at level 2, or inform the user of those services that the message could not be transmitted

. Messages to a node outside the segment are not directly acknowledged by the receiver station

. The frames should not exceed a given size, a few hundred bytes, if guaranteed transmission time is to be of the order of a few tens of milliseconds

. flow control is very limited

. there is no connected mode. It is not an OSI profile. For that reason, a Mini-MAP node cannot be directly seen by any real OSI node.

6.5. The MAP/EPA

In many cases, all the services offered by the seven layers of the OSI model are necessary. However, there may be a need to transmit very rapidly short messages corresponding, for example to danger warnings or other safety related information.

The purpose of the MAP/EPA architecture is to meet these two categories of needs by associating the FULL-MAP and Mini-MAP profiles side by side.

Moreover, a MPA/EPA profile can link a mini-MAP bus with a Full-MAP network.

6.6 Manufacturing message service

These applications services are adapted to the industrial message service currently being standardized by the ISO (DIS 9506). This draft standard originates from the studies conducted initially by the EIA. It has been adopted as one of the application level protocols for MAP architectures (Full-MAP and Mini-MAP).

These services are structured into roughly fifteen functional units which basically deal with:

. data exchanges by access to a remote memory
. definition of types and variables
. management of events and flags
. file transfer
. sending commands (starting or stopping a program remotely, etc)
. communication with operators

MMS includes an extension of the directives of operating systems to distributed systems.

In parallel to MMS, there are "Companion standards" whose purpose is to choose a subset of MMS services sufficient for some specific applications. At present, projects are under way regarding, eg digital control and programmable controllers. These standards could be envisaged for the control system of electrical substations.

References

'1§ ISO 7498 Information processing systems - Open system Interconnection. Basic Reference Model.

'2§ ISO 7776 Information processing systems. Data communications Description of the 1984 X 25 LAP B - compatible DTE link procedures.

'3§ ISO 8348 Information processing systems. Data communications - Network Service Definition.

'4§ ISO 8473 Information processing systems - Data communications - Protocol for providing the Connectionless - mode Network Service.

'5§ ISO 8208 Information processing systems. Data communications X 25 Packet Level Protocol for Data Terminal Equipment.

'6§ ISO 8072 Information processing systems - Open systems interconnection - Transport service definition.

'7§ ISO 8802/2 Information processing systems - Data communications - Local Area Networks - Logical link control.

'8§ ISO 8802/3 Information processing systems - Data communications - Local Area Networks - CSMA/CD Access. Method and Physical Layer Specifications.

'9§ ISO 8802/4 Information processing systems - Data communications - Local Area Networks - Token passing bus access method and physical layer specifications.

'10§ ISO 8802/5 Information processing systems - Data communications - Local Area Networks - Token ring access method and physical layer specifications.

11§ MAP 3-0 Manufacturing Automation Protocol Specification

•12§ ISO 8326 Information processing systems - Open Systems Interconnection - Basic Connection Oriented Session - Service Definition.

•13§ ISO/DIS 8822 Information Processing Systems - Open Systems Interconnection - Connection Oriented Presentation Service Definition.

•14§ ISO/DIS 8649 Information Processing Systems - Open Systems Interconnection - Service Definition for common application service elements.

•15§ ISO 8571 Information Processing Systems - Open System Interconnection - File Transfer Access and Management.

•16§ ISO/DIS 9506 Information Processing Systems. Open Systems Interconnection - Manufacturing Message Specification.

•17§ IEC - TC 57 Telecontrol Teleprotection and associated Telecommunications for Electric Power Systems.

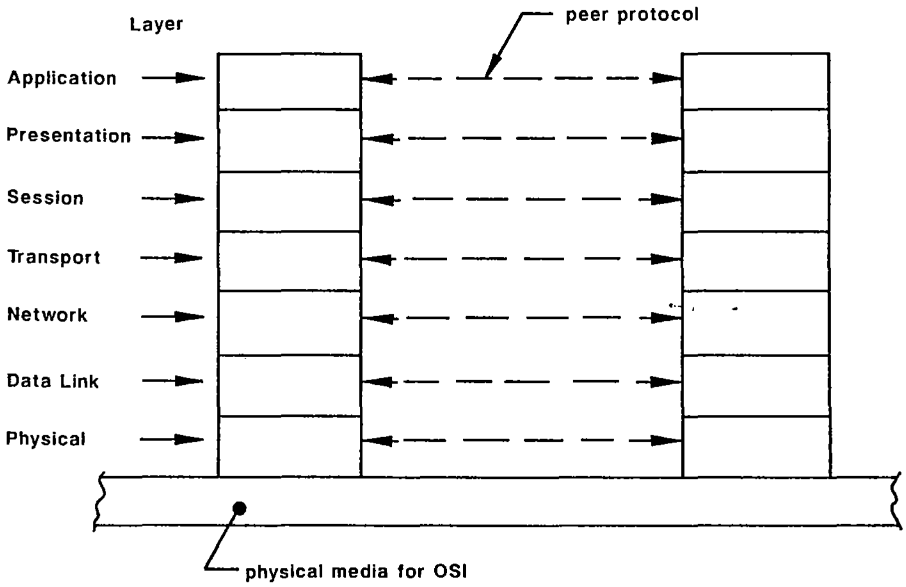

Figure A1 SEVEN LAYER REFERENCE MODEL AND PEER PROTOCOLS

0 111111 0	8 bits	8 bits	n x 8 bits	16 bits	0 111111 0
Flag	Address	Control	Data	FCS	FLAG

Figure A2 HDLC FRAME

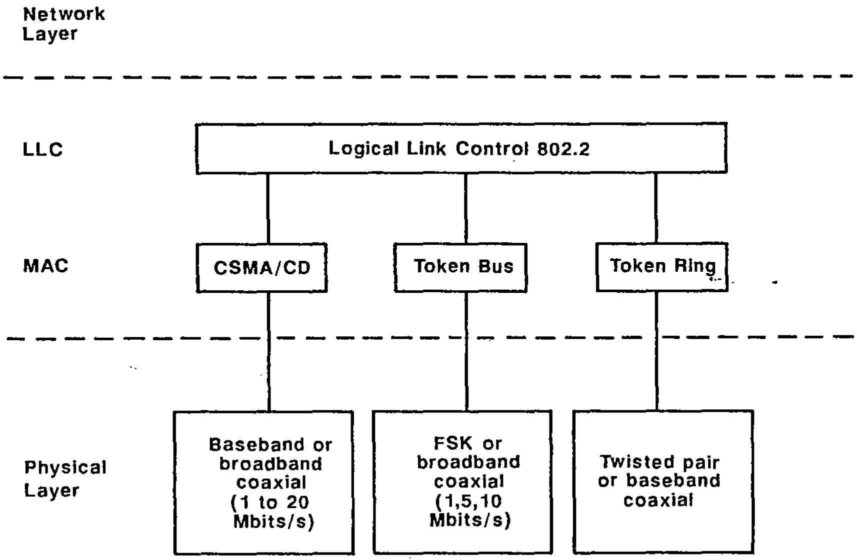

Figure A3 IEE LOCAL NETWORK STANDARDS

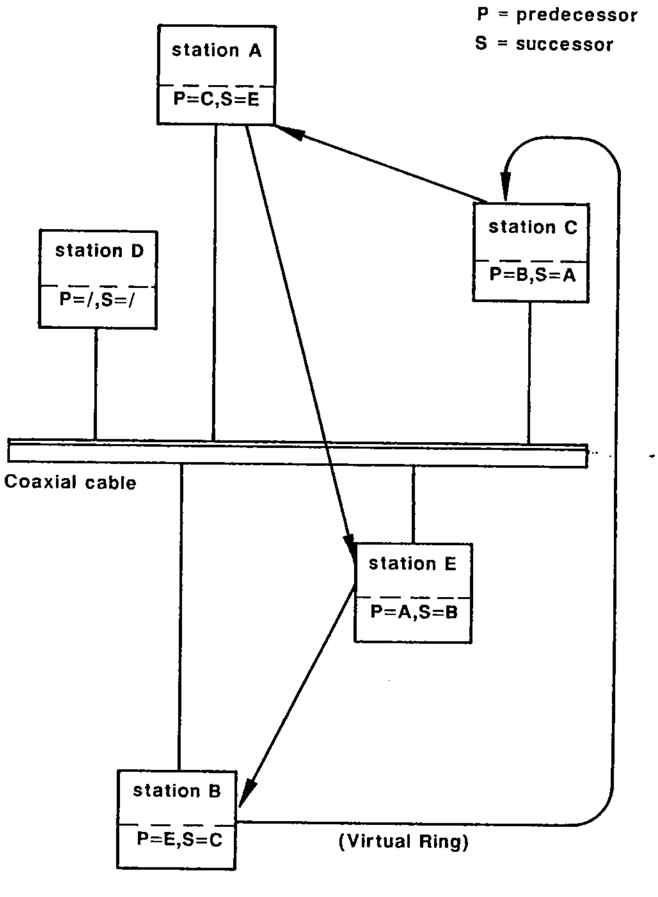

Figure A4 TOKEN BUS

3-5 rue de Metz - F-75010 PARIS