84

APPLICATION OF WIDEBAND COMMUNICATION CIRCUITS TO PROTECTION - PROSPECTS AND BENEFITS

Working Group 05 OF Study Committee 34
(Power System Protection and Local Control)

September 1991

C I G R E W G 34-05
Final Report

SEPTEMBER 1991 (rev. 1)

APPLICATION OF WIDE BAND COMMUNICATION CIRCUITS TO PROTECTION - PROSPECTS AND BENEFITS

This paper has been written by the
working group 34-05 members, whose names are :

J. HOEFFELMAN	BE	Convener
W. KWONG	GB	Convener (up to august 1990)
K. ALEM	FR	
L. CARMENA	ES	
C. STARACE	IT	
B. WIENHOLD	DE	

The authors are very grateful to :

MM. H. SPIESS	CH
T. YIP	GB
F. WELLENS	BE

for the useful comments they made about this work.

CONTENT

APPLICATION OF WIDEBAND COMMUNICATION CIRCUITS TO PROTECTION PROSPECTS AND BENEFITS

1. Scope and object

Protection using telecommunication links have been implemented for many years in meshed transmission systems.

In the past decade, better performances of protection systems have been necessary to cope with new constraints due to the increase of the size of generating units and the extension of transmission power networks. Such performances have been achieved using protection systems associated with telecommunication circuits.

More recently new constraints came from the development of complex transmission network configurations. More sophisticated protection functions will probably be necessary in the future.

Modern protections, particularly digital protections, matched with modern telecommunication systems, particularly digital circuits, will probably offer to the protection engineer new opportunities to cope with these challenges.

In this context, the scope of this document is to emphasize how to use communication technology for protection looking at new ways of applying modern telecommunication systems (prospects) and their impact on future implementations (benefits).

The report is also intended to be a mean for bridging the information gap between the protection field and the world of telecommunications covered in CIGRE by various general oriented telecommunication reports from SC 35. In this respect this document is arranged as a guide for protection engineers with little expertise and background on wideband digital telecommunication to explain to them what wideband tele-communication is and what implications it will have to their work in the future.

The look is also to technology that is not immediately available or not economically justifiable in order to give place not only to past experiences and present implementations but also to future possibilities.

Wideband digital telecommunication will provide more high speed channels and network capability though this does not always mean fast transmission time because of delay in multiplexing and demultiplexing telecommunication apparatuses.

These increased capabilities allow more information to be transferred from one part of a power system network to another. New applications, such as adaptive protection, system-wide protection, new back-up schemes, intelligent reclosing, etc., are all geared to exploit the extra information available. Most of the new applications however do not require high speed data channels, at least not at present.

Benefits coming from the use of digital wide band telecommunication can be summarized in the following:

- Improved selectivity by the use of more information transfer;
- possibility of fault location;
- improved security by lower transmission errors;
- possibility of remote setting;
- adaptivity to changing of field conditions;
- possibility of network supervision.

Having in mind these possibilities, an effort is made throughout all the document to pin-point the following main arguments:

- to identify the performances offered by telecommunication systems for modern protection systems, viewed from a protection engineer stand-point;
- to compare the ability of the various telecommunication systems to cope with the requirements of new protections;
- to investigate the advantages and drawbacks that would result from using new telecommunication circuits sharing facilities among various services;
- to study what level of standardization can be achieved for the interfaces between protection and telecommunication systems and for the structure of protocols and messages;
- to look if wideband telecommunication could bring simplification and new techniques to protection.

During the layout of the document special attention was dedicated to the work of related commissions and especially to the following:

- CIGRE WG 34-03 Classification and realization of protection and control function interfaces.
- CIGRE WG 34-04 Protection of complex transmission network configuration.
- CIGRE WG 34.06 Maintenance and management of protection systems.

2. WIDEBAND COMMUNICATIONS FOR PROTECTION

2.1. THE TREND TOWARDS DIGITAL COMMUNICATION

Until recently, telecommunications networks throughout the world have been dominated by the telephone service and were based on 19th century analog technology which amongst other drawbacks was slow in operation, liable to circuit noise and interference, fault prone and generally outdated in regard to the limited, disjointed services on offer. Digital communications, on the other hand, offer a way representing voice, and increasing data, text and image traffic in a standard format over existing physical media such as twisted pair wires or over new media of optic fibre, microwave or satellite links, all of which offer great improvements in speed, bandwidth and quality. Digital communication integrates with the digital technologies of data processing and automation, which together encompass the concept of "Information Technology". This standardisation and integration has resulted in new services and benefits being provided to businesses and industries. All these will have a dramatic impact on practices and working patterns to businesses and industries in the near future.

Around the world, a large portion of analog communication circuits is to be refurbished. In many cases, common carriers and end users are migrating to digital technology even their analog facilities have not reached the end of their useful life. Benefits achievable with digital technology are :

- better transmission quality
- improved performance through higher reliability and availability
- greater flexibility to meet changing requirements
- availability of tools to monitor and manage the network
- fast installation and restoration fo faulty links or equipment
- reduce modem costs
- ongoing development of enhancements and capabilities by manufacturers
- capability for interconnection with other digital networks.

Thus the manufacturers allocate most of their research and development efforts towards digital systems. It is likely that a declining market for analog communication equipment will preclude any significant new product development and will escalate future maintenance and equipment costs faster than the inflation rates.

Electric utilities are among the largest of communications of all industries, and according to some experts, the largest users of real-time data communications. It is natural therefore to follow a similar trend towards digital communications. It is important that power system protection engineers should consider seriously the future implications, applications and implementations of digital communication technology within their organisation.

2.2. THE NEED FOR WIDEBAND COMMUNICATION

Telecontrol and data transmission for the operation and management of the power network represent the bulk of power system operational communication traffic. For example, a recent survey by hydro Quebec on the number of communication circuits provided on long haul routes showed that :

- protection	350 circuits
- telecontrol	1000 circuits
- data transmission	1200 circuits

The data capacity requirements of some data transmission can no longer be satisfied by the conventional "4 khz" voice band circuits. Some new differential protection also require wideband circuit for signalling.

A steady growth in business oriented data communication traffic is forecasted. A recent survey carried out by Ontario Hydro in 1988 predicted the following traffic growth :

- long distance telephone growth 1 % per year
- computer communications 10 %
- telex 0%
- facsimile 8%.

There were a number of high information capacity applications where wideband communication facilities could improve business efficiency, but where the high costs of leased wideband facilities could not be justified. The geographic distribution of the locations means unavailability of digital wideband service offering at many locations. Many utilities are not happy with this reliance of business communication on common carrier service offering and to the affordability of tariffs. This encourages electric utilities to consider providing their own wideband facilities through private digital communication networks. Such developments mean that more communication channels, with higher data carrying capability, will be available in the future. These wideband channels will be used not just to improve business data communication, but will also be available for protection and system control applications.

2.3. COMPARISON OF TRANSMISSION MEDIA FOR WIDEBAND COMMUNICATION

Private underground/aerial cables, power line carriers (PLC) radio links, fibre optics and rented circuits from PTT may be used as communication media. The characteristics of these various types of transmission media had been discussed and compared in the CIGRE WG35-04 (1985) Publication "Guide For Planning of Power System Telecommunication Networks" and in the CIGRE WG34/35-02 (1987) Publication "Protection Systems using Telecommunications". In implementing a wideband communication network, cables and PLC are generally not suitable and there are basically four alternatives :

1. Analog Microwave - Replacing the aging portion of existing analog microwave network and expanding the network using analog technology.

2. Rented facilities - Utilize facilities rented from PTT for operational communications as well as continued renting for business information needs.

3. Digital microwave - Replacing the aging analog microwave facilities and expanding the network using digital microwave technology.

4. Fibre optics - Replacing the existing analog microwave facilities and expanding the network using digital fibre optic technology.
   Digital microwave radio could be used on routes where it is more economical and where the capacity of fibre optic facilites will not be required.

A summary of the technical comparisons of the four alternatives is given below :

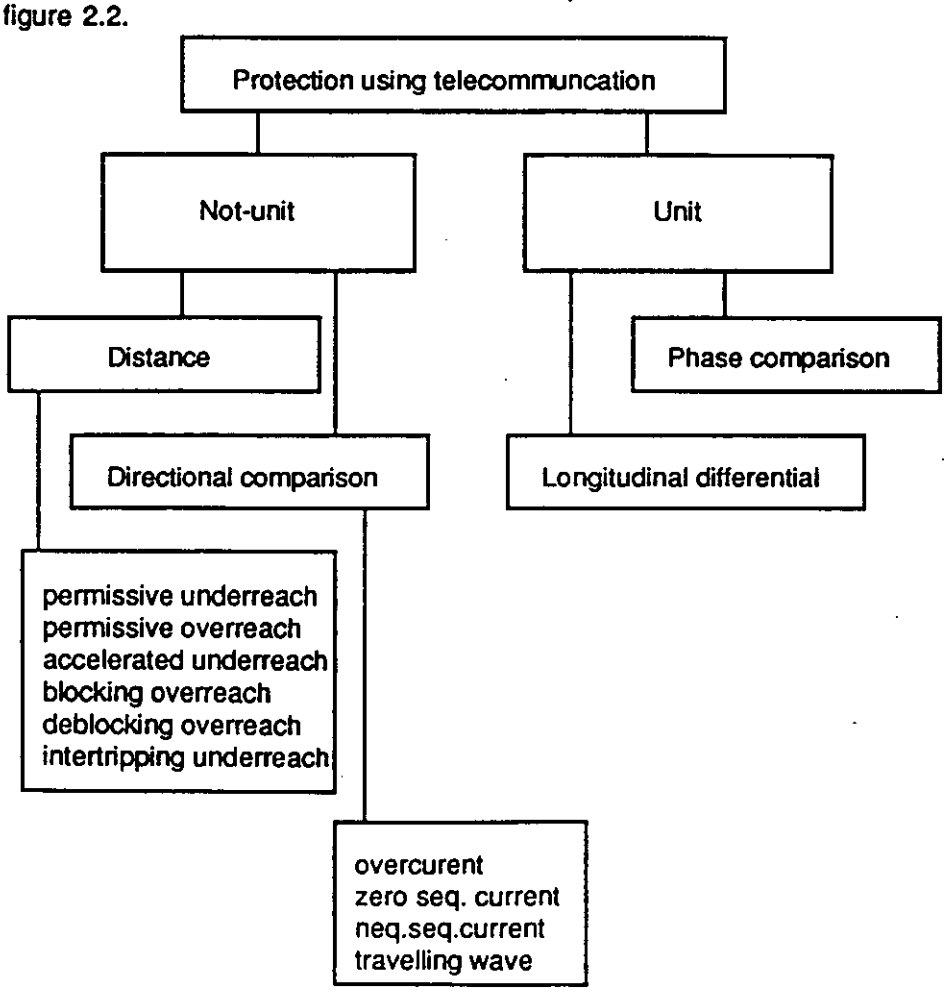
Parameter	Analog Microwave	Rented Facilities	Digital Microwave	Digital Fibre optics
Meets reliability and security needs	yes	no	yes	yes
Low risk of technological obsolescence	no	yes	yes	yes
Substantial expansion capability	no	yes	no	yes
Design & operating flexibility	no	yes	yes	yes

In many cases, rented facilities are technically unacceptable because they may be switched during maintenance and change their parameters, and the reliability and noise characteristics of circuits associated with the public telephone network do not meet the requirements of high speed power system protection and control.Many electric utilities also insist that telecommunication facilities utilised for critical applications of protection and control of power systemsmust be self owned and controlled. It ends up that the choice is just between microwave and fibre optics.

Many electric utilities had also carried out financial evaluation on these alternatives to help deciding on which transmission medium was to be used. However, different conclusions were drawn. This was because utilities had differing practices in apportioning capital cost, that the types and capacity of services required were varied, and due to differences in monopoly regulations which permitted or prevented collaboration with PTT and other services utilities.

2.4. PROTECTION SYSTEMS USING TELECOMMUNICATION

Telecommunication is a widely used means to improve performance of protection systems.The different types of protection systems using telecommunication are described in detail in the relevant CIGRE WG34/35-05 (1987) Publication "Protection Systems using Telecommunications". The most common protection schemes used are summarised in figure 2.1. the communication channel bandwidth requirements of these schemes are summarised in figure 2.2.



Note :
Sometimes permissive overreach distance protection is called directional comparison
Zero sequence current protection is also called residual current protection

Figure 2.1. : Common Protection Systems Using Telecommunication

Protection system	Protection information	Characteristics of signal delivred to telecomm.system	Telecommunication system	Number of circuits and bandwidth
Command	ON-OFF	-	- Specific design PLC	1 Unmodulated
		FM	- PLC Radio link (FDM or TDM) Fibre optic link (TDM or dedicated)	1 Narrowband
		A&D	- Radio link - fibre optic link (TDM or dedicated)	1 wideband
Non segregated differential	Power frequency sine wave	-	- Pilot wires Specific design digital link	1 Unmodulated
		FM	- Coaxial cable Radio link (FDM or TDM) Fibre optic link (TDM or dedicated)	1 Narrowband
		A&D	Radio link (TDM) - Fibre optic link (TDM or dedicated)	1 wideband
Segregated	Power frequency sine wave per phase	-	Specific design digital link	3 Unmodulated
		FM	Coaxial cable - Radio link (FDM or TDM) - Fibre optic link (TDM or dedicated)	3 Narrowband
		A&D	Radio link (TDM) - Fibre optic link (TDM or dedicated)	1 wideband
Non segregated phase comparison	Power frequency square wave	-	- Specific design PLC	1 Unmodulated
		FM	- PLC Radio link (FDM or TDM) Fibre optic link (TDM or dedicated)	1 Narrowband
		A&D	Radio link (TDM lor dedicated)	
Segregated phase comparison	Power frequency square wave per phase	FM	- PLC Radio link (FDM or TDM Fibre optic link (TDM or dedicated)	1 to 3 Narrowband
		A&D	Radio link (TDM) Fibre optic link (TDM or dedicated)	1 Wideband

Figure 2.2 : FM : frequency modulation - A&D :analog or digital- PLC : power line carrier - TDM : time division multiplex - FDM : frequency division multiplex

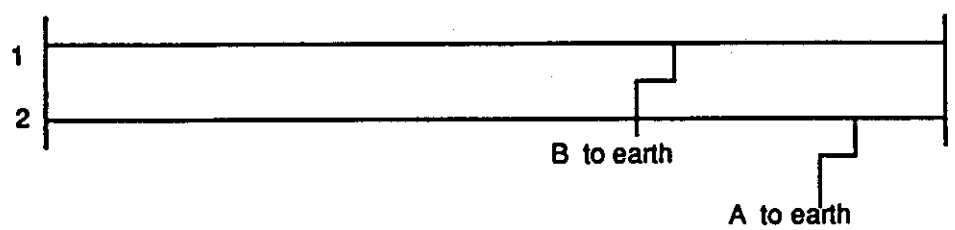
2.5. SOLUTIONS TO EXISTING PROTECTION PROBLEMS

In order to achieve the necessary transmission capacity at a minimum cost and with a minimum demand on new transmission lines and rights of ways, power system planners have to propose more complex solutions such as multi-circuit lines, multi-terminal and tapped lines, series compensation lines, and special shunt compensation and static VAR compensation schemes. Protection of these complex transmission line configurations will raise difficulties. A solution to these appplication difficulties is to adopt a protection scheme which utilises an extended exchange of information between the line terminals. This in turn generates a demand for new types of unit protection systems and a demand for teleprotection systems with more information carrying capacity higher availability and better security.

The CIGRE WG34-04 (1990) Application guide on "Protection of Complex Transmission Network Configurations" gives an excellent review of the protection problems of complex transmission network. In many cases, sophisticated protection schemes in combination with telecommunication must be used to solve these problems.

Often the best solution to the protection problems would be to use phase segregated longitudinal differential protection or to provide more command protection signalling channels such as in a phase segregated command protection schemes. These solutions are, however, seldom applied as a wideband channel or more signalling channels have to be provided. This is on one hand expensive to provide a wideband channel or several signalling channels at present and on the other hand the bandwidth needed by these equipments is normally not available with the existing communication systems. With the growth in application of radio links and fibre optics, these schemes could become more popular in the future.

Example 1 : Double transmission lines and teed lines



Actual classical distance protections have phase selectivity problems to protect doubles lines terminal and teed lines.

For the relay in 1, it is quiet difficult in some configuration to select a B to earth fault instead of a A-B to earth fault. By the use of a channel for example of 64 Kb/s transmitting currents, voltages and phases between relay 1 and relay 2 the situation gets better.
For more than 2 ends lines problems on distances protection get worse even with the use of teleactions.

Example 2 : Of existing problems

A major problem with the distance relaying schemes using command signalling is the relative lack of sensitivity. This is particularly critical in the Australian application where the ionised gas rising from bush fires burning underneath the line causes long unstable arcs. This type of fault is more like an overload than a conventionnal fault and is difficult to detect. Directionnal earth fault comparison schemes offer improved sensitivity but are generally time delayed and phase selectivity for single pole reclosing schemes is a problem.

A problem with analogue pilot wire schemes is the probability of indiscriminate tripping during faults if the pilots have been open or short circuited. To overcome this problem current check relay set above load current are used which reduces overall sensitivity. Current differential schemes will overcome these problems.

2.6 PRESENT PRACTICES AND FUTURE TRENDS

2-6-1 Introduction

In order to carry out a survey on the uses of wideband telecommunication in electric power networks a questionaire has been sent to all members of SC 34 .

The objectives of this survey are :

1 - To find out how widely used are wideband channels at present in the telecommunication networks of electric power utilities and the trend within the next few years .

2 - To investigate the different telecommunication media used for wideband telecommunication and related bandwidth .

3 - To survey the use of wideband channels for protection and the type of protection schemes used .

4 - To examine the benefits and drawbacks of using wideband channels for protection .

2.6.2 Result and analyse of the questionaire

The replies to the questionaire came from 16 countries on behalf of 52 electricity board Considering the extension of their telecommunication networks , we can say that :

17 electricity boards have large networks
21 electricity boards have medium networks
13 electricity boards have small networks

Some of them have or plan to install analog wideband networks but the tendency is decreasing as illustrated by the following figures :

19 companies have analog wideband channels in service of which :

16 have radio links
9 have cables
6 have fibre optic links
12 have PLC systems
10 have PTT rented links
3 have other rented links

15 companies plan to install analog wideband channels in the following fields:

10 plan radio links
2 plan cables
8 plan fibre optic links
3 plan PLC systems
3 plan PTT rented links
1 plan other rented links

On the contrary much more companies have or plan to implement digital wideband networks and the tendency is toward an increase in number as can be seen from the following figures :

32 companies have digital wideband channels in service of which :

22 have radio links
15 have cables
30 have fibre optic links
4 have PLC systems
12 have PTT rented links
5 have other rented links

40 companies plan to install digital wideband channels in the following fields:

25 plan radio links
17 plan cables
35 plan fibre optic links
3 plan PLC systems
14 plan PTT rented links
5 plan other rented links

If we consider the use of wideband channels for protection we can see that this use is not very common also for the near future but again we observe the tendency towards increased use of digital wideband channels at the expense of analog ones .

The figures derived from the questionaire are as follows :

15 companies use or plan to use analog wideband channels for protection :

15 use wideband analog channels
12 plan to use wideband analog channels
4 will dismiss , in the future , used wideband analog channels

25 companies use or plan to use digital wideband channels for protection :

20 use wideband digital channels
24 plan to use wideband digital channels

Examining the answers relating to the use of wideband digital channels one discovers that,on 25 replies , 20 indicate the bit rate of 64 kbit/s as appropriate for protection , the other replies , with different bandwidths , come essentially from Japan .

The choice to share the link supporting the protection channel with other services is predominant . The replies on the matter were 22 and :

10 companies prefer sharing while 9 admit to have channel sharing on some circuit in a proportion variable from 33 to 90 % .
2 companies only has completely dedicated channels for protection .

2.6.3 Predictions and trends to be considered

1. Current differential protection systems will be used more frequently in particular as solution to complex network configurations .

2. Faster and more secure command signalling,reducing problems in sequential tripping. This will prompt a review on the command system used,i.e. whether it should be underreach or overreach;intertripping,permissive or block .

3. Phase comparison becomes less popular due to availability of wideband channels. Current differential protection systems gradually take over .

4. Wideband communication network built up from point to point wideband links . Allow data to be transferred more freely between different points of the network .

5. Abundant channels and availability of alternate routes makes back-up channels attractive . This affects the overall 1st main / 2nd main / backup philosophy and can also affect the philosophy in command protection systems used .

6. Current differential protection, being an unit protection, will not provide remote back-up protection as distance protection . A review on the philosophy of remote back-up protection is needed. In some case it can restrict the use of current differential protection .

7. New distance relays usually provide fault locator facility .
   A current differential relay , specially provided with voltage signals (primarily for starter purpose), will be able to do fault location . Moreover , it can potentially provide more accurate fault location because by default the relay has access to currents signals at all terminal (particularly it has got access directly to the fault current) .

8. Segregated comparison becomes more popular than mixed phase comparison due to availability of data channels and abundant VF channels and because it is easier to set without the need to consider what proportions of positive , negative and zero sequence current are to be used . Segregated comparison also provides phase selection and so obviates the need for a local phase selector ; it also detects intercircuit faults much better.

9. A command protection system can carry several ON/OFF signals instead of one , e.g which of the three phases of the distance relays have operated or even information on which zone . This improves discrimination of the protection systems in particularly with single pole tripping .

2.7. OPPORTUNITIES FOR NEW APPLICATIONS

Gradually, a utility will build up a digital communication network from point to point communication links. It will allow data to be transferred more freely between different points of the network. Most of the future opportunities for applications of wideband communication for protection are centred on the idea of sharing data between devices at different parts and levels of a power system through a communication network. This allows protection systems to adopt their characteristics to the prevailing system conditions and to react in a more co-ordinated manner under system wide disturbances. Data speed is less of an issue at least for the present. In many cases, some of these new applications may well be regarded as control or energy management system (EMS) functions other than just protection functions.

2.7.1. Integrated Substation Protection and Control

The integration of substation protection and control functions have been studied by a number of working bodies, and more recently by CIGRE WG34-02 (1989) and WG34-03 (1989). It is apparent that high speed data transfer between devices within a substation is a key issue in the integration of protection and control functions - a job best handled by wideband communication.

2.7.2. Adaptative Protection

If more information about the power system configurations and conditions such as loading, status, and notification ofswitching to be done are available through the communication network, then a protection system can be made to adapt to the operating conditions and yields improved performance.

This adaptive protection concept has become an attractive possibility due to the simultaneous emergence of three technologies.

- availability of fast, relatively inexpensive computers for on-line analysis and state estimation
- ongoing development of wideband communication systems to link all nodes of a utility network
- digital relays whose performance can be influenced by decisions made locally or by remote commands through their communications lines.

Adaptive protection is being studied by CIGRE W34-01 and other working bodies. Some examples of adaptative protection are :

- line overload protection setting adjusted according to the weather forecast
- adaptative system impedance model which permits the calculation of fault distribution and to adjust relay settings accordingly
- adaptative multi-terminal relay coverage to account for changes in infeed ratios and breaker openings.

2.7.3. Back-up schemes

Data sharing, diagnostic and communication capabilities presents attractive possibilities for local and remote back-up protection.

2.7.4. System-wide Protection

The reliable operation of a power network can be threatened by rare but serious events followed by unfavourable primary and secondary consequences, as have been illustrated by blackouts or partial blackouts in the past. The initiating event can be followed by voltage collapses, overvoltage conditions, out-of-step operation of generators or generation areas, unbalanced between production and load, overload on transmission lines and transformers. To limit the consequences of such failures, it is necessary to implement high speed automatic emergency control functions (e.g. load and generation shedding, power system splitting etc...). This implies communication and coordination between remote relays and a need for a high integration of real-time control.

Use of digital technology improves the possibility to design new protection for the whole power sytem. Such protections might get their measurements from substations and send commands back to them . They could for example provide optimum automatic network islanding and load shedding during a major disturbance, by using a global view of phenomena. One solution may be to have centralised decision in control centres and high speed, high capacity communication links. Another solution would be to have decentralised power system protection devices, which are kept updated with power system information via communication links from control centres during normal state. Creation of this kind of power system wide protection would be rendered possible by co-operation between the disciplines of power system control (EMS), communication, and local digital protection and control.

2.7.5. Automatic Switching for Service Restoration

Information from different parts of the power system through the communication network will help the conditional logic and automatic switching of circuit breackers in substations and power stations to restore the service after a total or partial blackout.

3. ADVANTAGES AND DRAWBACKS OF WIDE-BAND COMMUNICATION CIRCUITS SHARING FACILITIES BETWEEN PROTECTION AND OTHER PURPOSES AND PROBLEMS TO PROTECTION

In the past and partly up to now the problem of sharing communication facilities between protection and other services was not considered as an essential point of discussion because protection conceptions were based on complete autonomy.
Inspite of a failure in communication circuits protection was mostly able to operate, but a prolonged tripping time had to be accepted.

Nowadays and in the future the demand for fast and efficient telecommunication links will increase in order to realize more sophisticated protection schemes able to manage the growing difficulties (e.g. network stability, large generator units, difficult network constellations etc.)

So at the one hand protection engineers have to keep up the well-founded and proved principle of protection autonomy and on the other hand they have to obey to the requirement of cost reduction.

Especially in those cases when a large (wideband) telecommunication network of sufficiently free capacity is still existing, the demand for a separate protection - communication network in parallel cannot be regarded as a realistic answer to the problem in general .

The solution for protection, on the contrary, has to be found on a middle course.
It is, therefore, necessary to know the advantages and restrictions that will result well before shared telecommunication facilities become an integrated part of protection schemes. Furthermore it should be outlined how the existing or supposed drawbacks can be overcome.

Protection engineers will not be able to solve all these problems alone. Users, telecommunication engineers, and manufacturers will have to work together in order to satisfy all demands.

In the following discussion on the advantages and restrictions for protection using shared telecommunication systems, the most serious arguments for shared systems and some grave negative aspects one has to look at are lined out.

3.1 Strong arguments for the use of a shared telecommunication system

Wide-band communication networks of large extension mostly already exist, offering free capacity for protection purposes (e.g. primary and secondary protection, demand for path diversity, more sophisticated protection schemes). This means low investment costs for teleprotection systems as far as links and equipment are concerned and a short time for realization.

With regard to older power lines, shared telecommunication links will often be the only answer to the contradictory problems of tower strain and the demand for additional telecommunication links.

Nowadays the high demand of such links for protection on multi-circuit lines can only be met economically by sharing them.
The participation in shared links will be a chance for protection to substitute less performant telecommunication links like plc.

Radio links in most countries suffer from frequency restrictions. This makes it difficult for protection to obtain new frequencies, exclusively used for teleprotection purposes.
The participation in a multiuser system may often be the only way out to cover the requirements of protection for additional dedicated telecommunication links .

Shared equipment normally conform to international standards (e.g. CCITT). These standards will lead protection to more economical solutions such as:

- reduced number of standardized active modules and spare parts
- lower price
- redundancy of equipment by system pooling

Nowadays, non-protection services such as data communication require faster and more secure data links and equipment. This will lead to a permanent and rapid improvement of all elements concerned. Protection can benefit from this improvement.

3.2 Negative effects on protection when shared telecommunication systems are used and how they can be overcome

3.2.1 General comments

In view of all the positive aspects mentioned above the negative effects on protection have to be outlined as well. This has to be done because protection is a function of utmost sensibility. Malfunctions resulting from the telecommunication system used may cause serious problems to the network itself.

So a gain in new possibilities for protection using shared telecommunication systems must not reduce the high standard of security and availability attained up to now even under heavy working conditions in case of a fault (e.g. arc of lightning, fast transients, disturbance of power supply).

The necessarily short time for starting, measuring, and tripping makes high demands on shared telecommunication systems when they are integrated in protection schemes.

New techniques, however, as for example the wave length division multiplexing on optical fibres, will enable protection in the future to share optical fibres with other services but without the need of sharing the same terminal equipment.
Thus the proven structure of a dedicated protection system can be kept up using the benefits of an existing telecommunication network.

3.2.2 Testing conditions and system. structure of shared equipment

Communication equipment usually does not have to withstand the specific disturbance tests used for protection facilities (e.g. IEC 255, IEC 801-2,3,4). Normally it belongs to a lower testing class.
Malfunctions may result from this fact and have to be avoided principally. (cf. 5.4)

All elements of a teleprotection device have to be regarded as an integrated part of the protection system.

When shared facilities are used, they have to be immune to high frequency disturbances, as protection is expected to be.
This means the same testing class in general.
According to the different mounting locations within a substation, a lower testing class may be sufficient as far as a lower disturbance level can be expected.

Individual local measures to limit the disturbance level will in many cases be an adequate means to apply a lower testing class to shared facilities.

In shared equipment defects or disturbances in one channel or module may cause problems to adjacent protection channels

or modules. In order to minimise these negative effects on protection, teleprotection should be kept separate within dedicated modules.
Just a minimum of common functions (e.g. DC-supply, multiplexer) should be designed.

Regard must be paid to these remaining common functions and central parts so that availability and security of this system do not fall behind protection.

As an example, DC-supply of the telecommunication equipment should be able to operate even in case of a DC-voltage drop caused by a faulty line or DC circuit. DC energy should be buffered for a sufficient period of time to allow protection to operate.

Availability of a teleprotection system using shared facilities depends on the error rate and outage time which is necessary for maintenance and testing purposes concerning the protection channel itself. Additional to this it can be influenced by the effects arising from all the other non-protection channels belonging to the same shared equipment.

As an example, the total system can be blocked because of a peripheral (non-protection) fault or the central DC-supply has to be switched off to allow the changing, adding, or testing of modules and channels for other services.

To overcome these restrictions to protection the system structure of shared facilities should allow to keep protection under function while other channels or modules are under maintenance (e.g. changing modules under tension). Otherwise a redundant teleprotection system should be available.

The outage time of the teleprotection system due to a system fault within shared equipment can be reduced to a minimum when alarming, blocking, or signalling information given by the shared equipment is as detailed as possible. So the time for maintenance and repair can be reduced.

According to the individual requirements of the different services using shared facilities, an individual setting of alarm levels would be very helpful to optimise working conditions. (cf. 4.5.2)

To achieve a reduced outage time especially for the protection system, alarming and warning signals should be transmitted and centralised. So diagnosis as well as parametering, surveillance, and repair (limited) can be done by remote teleactions.

The documentation of all signals concerning the teleprotection system is of utmost importance and has to be done in detail.

3.2.3 Local problems

When shared communication facilities are used, protection signals mostly have to be transmitted from the bay house to the central telecommunication room (distance of some hundred metres).

This connection has to be designed very carefully to avoid any disturbances of the teleprotection signals caused by external high-frequency interferences. Fibre optics can be very helpful.

Mostly protection staff and telecommunication staff belong to different branches of the utility. The teleprotection system is the common link in between. To avoid any problems to protection resulting from this, responsibility for the teleprotection system within the substation as well as for the link has to be assigned clearly to the different groups. Consequently, the testing and the maintenance have to be done in good coordination.

3.2.4 Redundant protection systems and common mode failures

Special attention has to be paid to the conception of redundant protection systems using shared facilities for teleprotection.

For reasons of security the redundant teleprotection systems should not be installed within the same telecommunication equipment or link.
Path diversity for the links and different equipment are requirements for a real redundant protection system.
Both telecommunication systems may be shared by other services and, if necessary, by the teleprotection systems of other power line circuits.

Attention has to be paid to common mode failures which can hit the telecommunication links and energy circuits or different telecommunication links or equipment at the same time mostly caused by the same event. An unselective tripping of two or more power circuits with all the negative effects on load, stability, frequency etc. may be caused by this. Therefore, path diversity as well as splitting of equipment is very useful.

Path diversity, however, is often limited by frequency restrictions, static problems of the towers for additional cables etc.
In this case, one should set up two different cables on the same tower, two different radio beams or a combination of both, which would be the best.

If path diversity cannot be realized, the demand for redundancy on multi-circuit lines might in practice be met by combining all primary protection systems as well as all secondary ones in two separate shared telecommunication links.

3.2.5 Rented telecommunication links

Rented links (e.g. PTT, private companies) may be a solution to overcome the restrictions on path diversity for the teleprotection systems.

National regulations and practice, however, have to be regarded and sometimes they confine the application for protection.

The long-term experience in some countries e.g. shows that security and reliability of rented systems do not satisfy protection requirements.

Important reasons for this are:

- rented systems are sometimes shifted automatically for operating reasons. The characteristics of the telecommunication circuit can be changed by this and may cause problems to protection functions.

- Maintenance and testing conditions of the teleprotection systems are more difficult in a rented system.

- The protection staff cannot keep up its exclusive responsibility for the total protection system.

In some countries, however, PTT start to offer special dedicated telecommunication links with guaranteed characteristics which seem to be applicable to protection.

4. COMMUNICATION PERFORMANCE PARAMETERS AND THEIR EFFECTS ON LINE PROTECTION

4.1. About channel capacity

In section 2.3. different kinds of wideband channels have been mentioned. Depending on which is chosen, performance parameters will vary significantly. In order to understand more easily the importance of these parameters, which are represented on figure 4.1., it is worth highlighting some basic concepts such as the difference between analog and digital channels and between narrowband and wideband channels.

What is a wideband channel ?

In the context of this work a wideband channel is any communication channel of which the information transmission capacity is larger than that of a classical analog 4 kHz telephone channel.
This needs some clarification about what is the information transmission capacity (C) of a channel.
The capacity C of a channel is the steady state amount of information that can be transmitted per unit of time without any error regardless of the transmission delay.

The information quantity I contained in a symbol which can take n statistically independent and equally likely states is given by the relation $I = \log_2 n$.
For a binary signal (bit) with two possible states $I = \log_2 2 = 1$; so the unit of information is the bit and the capacity C is measured in bit/s.
This is not to be confused with the baud rate of a digital channel : the baud rate V is the total number of elementary signals which flow across the channel per unit of time.
Only when one elementary signal is used for coding one bit the baud rate will be equal to the bit rate.
The maximum baud rate of an analog channel is given by the Nyquist sampling theorem. This specifies that a minimum of 2 B samples are necessary to reconstitute a signal of which the bandwidth is B (Hz).
Translated in other words this means also that a maximum of 2 B independant signals can be sent accross a channel of bandwidth B(Hz) during one second, i.e. $V = 2\ B$.
So the maximum baud rate of a 4 kHz channel is 8 kbaud.

As the maximum rate of elementary signals which can be sent in an analog channel is $V = 2\ B$ and as each signal contained $I = \log_2 n$ bit of information, the capacity of the channel will be :

$$C = 2\ B \log_2 n.$$

Shannon has demonstrated that the maximum number of discernible states is

limited to $n = (1 + S/N)^{1/2}$ for a noisy channel (with S the mean power of the signal at the receiver and N the mean power of the noise (*) at the receiver). So the maximum capacity of an analog channel, i.e. its maximum error free bit rate is always limited to

(*) supposed to be white and gaussian, which is the worst case

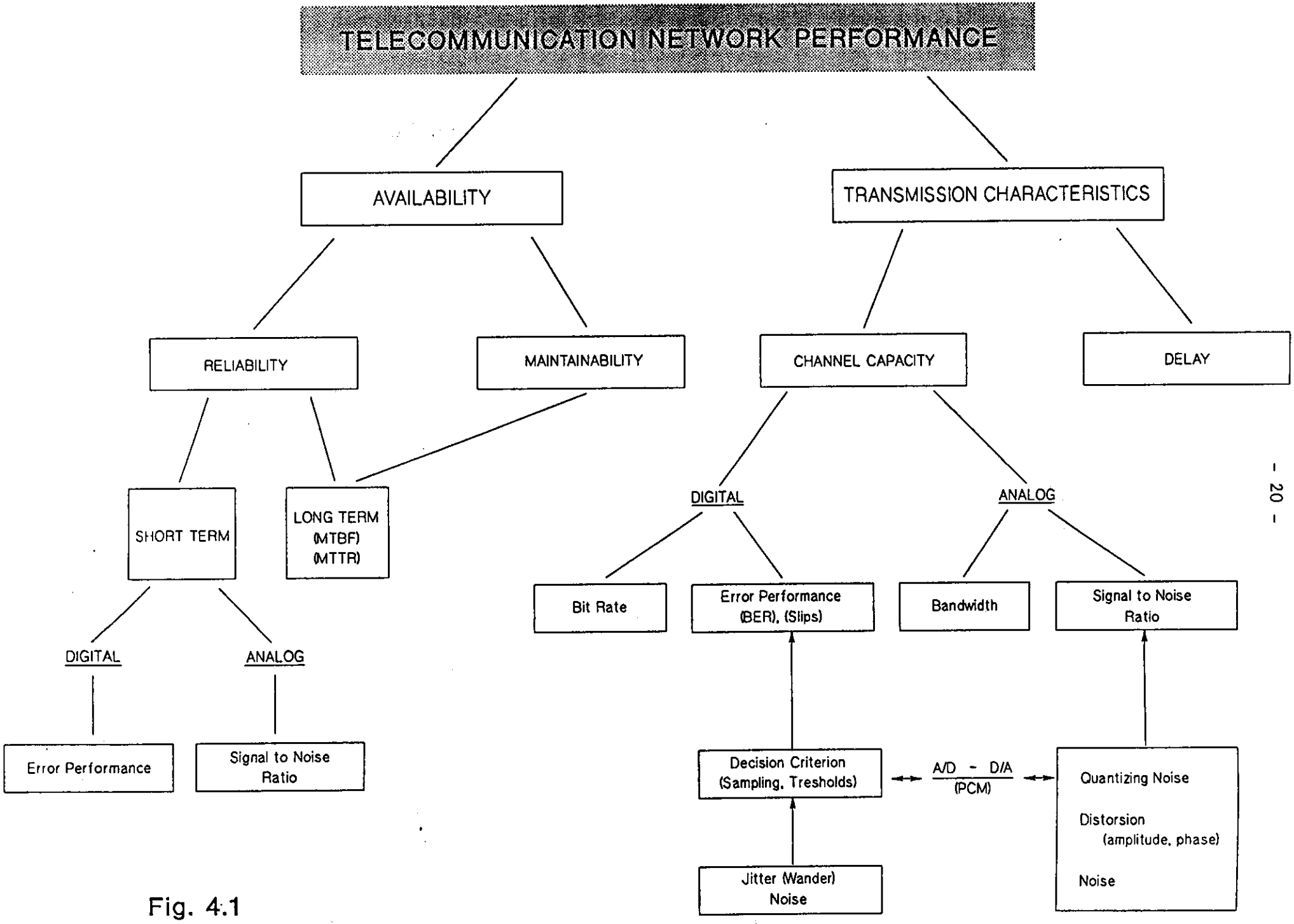

TELECOMMUNICATION NETWORK PERFORMANCE
AVAILABILITY
TRANSMISSION CHARACTERISTICS
RELIABILITY
MAINTAINABILITY
CHANNEL CAPACITY
DELAY
SHORT TERM
LONG TERM (MTBF) (MTTR)
DIGITAL
ANALOG
Bit Rate
Error Performance (BER), (Slips)
Bandwidth
Signal to Noise Ratio
DIGITAL
ANALOG
Error Performance
Signal to Noise Ratio
Decision Criterion (Sampling, Tresholds)
A/D - D/A (PCM)
Quantizing Noise
Distorsion (amplitude, phase)
Noise
Jitter (Wander) Noise

Fig. 4.1

$$C = B \log_2 \left(1 + \frac{S}{N}\right)$$

This equation can also be used to calculate roughly the information capacity of a digitalised analog signal. As an example when a 4kHz analog signal is to be transmitted through a digital channel it will be converted into a digital form by PCM coding :

Each sample will be compared in amplitude to a 256 steps scale and transformed into a 8 bit pattern.

The existence of 256 levels for quantizing a sample means that a quantization error of (plus or minus) half a level can be made or that the amplitude signal to noise ratio of the quantized signal is at best of 256/1. The maximum signal to noise ratio in terms of power is $(256)^2$(*) and the information flow is equal to $C = 4000 \log_2 (1 + 256^2) = 64$ kbit/s (**). This result could of course be directly derived from the Nyquist theorem knowing that 8000 samples are necessary to restore the signal and that each sample is coded by a 8 bit pattern, giving C = 8 x 8000 = 64 kbit/s (***)

As seen from this example, the equivalence in information content between a 300 - 3400 Hz voice frequency signal and a 64 kbit/s digital signal exists as far as no other noise sources than the quantification noise are considered. When dealing with an analog channel (instead of an analog signal) other unavoidable impairements such as phase distortion (group distortion), amplitude distortion and different kinds of noise appear. For this reason the maximum baud rate of an analog voice grade channel is limited to about 2400 baud instead of 8 kbaud whereas the maximum bit rate doesn't exceed 19200 bit/s.

A wideband analog channel is thus a channel of which the bandwidth is higher than 4 kHz whereas a wideband digital channel is a channel of which the bit rate is higher than 19 kbit/s, ie : 32, 48, 56, 64 kbit/s etc.

On the other hand, contrary to narrowband analog channels, wideband digital channels (with the exception of radio modulation) are usually not limited by their actual bandwidth. So the Nyquist criterion is no more a limit and there is no need to encode more than one bit per baud. Some other information like the bit and byte clocks can even be included in the bit stream giving rise to a baud rate higher than the binary bit rate.
As a example a 64 kbit/s G.703 co-directional channel has a transmission speed of 256 kbaud/s and occupies a bandwidth of several hundred kHz, which is not without consequence in the field of electromagnetic compatibility (see § 5.4 and fig. 5.4).

(*) A rigourous calculation leads to $(256)^2 - 1$

(**) Practically, as the signal is not always at its maximum, quantizing levels following a quasi logaritmic law are used. This has as consequence that the signal to noise ratio becomes independent of the signal level but is reduced to 38 dB instead of 10 log $(1+256^2)$=48 dB giving an actual capacity of $(3400-300)\log_2 (1+79^2) = 39$ kbit/s.

(***) There also exists a 7 bit pattern PCM standard leading to C = 56 kbit/s

Finally we must point out the difference that exists between channel capacity expressed in bit/s and transmission speed i.e. binary rate, also expressed in bit/s : the channel capacity is in fact the net bit rate regardless of the time used for the error detection/correction scheme assuming that the best one has been chosen. When the channel doesn't suffer from any impairment, channel capacity and transmission speed are equal. When, as it is usually the case, the bit error rate is not equal to zero, the channel capacity becomes slightly smaller than the actual bit rate and can be compared to the net bit rate of the transmission protocol from which the redundancy bits have been removed. However the channel capacity remains always higher than the net bit rate because the ideal error correction scheme doesn't exist (it would furthermore increase the transmission delay to infinite !).
Actually, as the channel impairment level is usually not known or can vary in time, a rather large amount of redundancy bits will be added to the information flow depending of the security level to be achieved.
It is usually the duty of the user to look for a good communication protocol (cf. § 4.5.1.). When a sufficiently high channel capacity cannot be guaranteed at any time, other improvement methods have to be found like alternative routing (cf. § 4.7.2.).

To resume this long - but important - introduction, we can say that :

1°) the capacity of an analogue 4 kHz channel can theoretically be higher or lower than the capacity of a 64 kbit/s digital channel depending of the noise level.
2°) When the noise level of an analogue 4 kHz channel is equal to the quantizing noise level of a PCM channel, the maximum signal to noise ratio is 20 log 256 = 48 dB (actually limited to some 40 dB due to the non linear repartition of the quantization levels) and the channel capacity is equal to 64 kbit/s.
3°) Most time however the channel capacity of an analogue 4 kHz channel is lower than 64 kbit/s due to other impairments like group distorsion, crosstalk, interferences etc..
4°) The real difference - as far as capacity is concerned - between a good analogue 4 kHz channel (e.g. a PCM channel) and a true 64 kbit/s digital channel lies in the fact that the full capacity of a disturbance free analogue channel can only be approached by choosing a good modulation scheme whereas it is directly usable with the digital channel. In other words it is by far more easy to exploit the full capacity of a digital 64 kbit/s channel than its analogue equivalent with a 4 kHz bandwidth; that is what makes the actual superiority of the digital channel. (*)

4.2. Availability

Availability (defined by CIGRE SC34 as the probability that a device, an equipment or a system is able to perform correctly its required functions, under stated conditions, at a given instant, when required) depends on the reliability of the equipments expressed by the concept of mean time between failure (MTBF) and on their maintainability which implies both mean time to repair (MTTR) and out-of-servicing due to programmed (preventive) maintenance.
When speaking about reliability a further distinction must be made between "long term" and "short term" reliability. Long term reliability is caused by failure of equipment. When outages due to maintenance are taken into account the term "long term availability" is used.

(*) see also appendix 1

Recommendations and figures about short term reliability are given in the next paragraph dealing with error performance; both concepts are indeed closely related.
A general discussion about the effects of unavailability on protection is given in § 4.7.

4.3. Error performance

Error performance has been traditionally quantified by the long term mean error ratio. An individual error occurs when a received bit status differs from the bit status that was sent. A bit error rate (BER) of 1E-3 implies that the long term mean individual error is one every 1000 bits transmitted.

The concept does not contain any information regarding the distribution of errors with time. It has been based on the assumption that errors are randomly distributed. In practice errors occur in bursts. In radio systems they are normally caused by disturbances or fading. In optical links it usually means there is something wrong with the cable. Errors can also be introduced by failure in terminal equipment, slips (loss of alignment), etc.
In the following paragraph subdivisions we will try to describe the mechanism of error occurence and its influence on the dependability (i.e. the probability to operate when required) and on the security of the protection (i.e. the probability not to operate unnecessarily) at the communication level.

Both dependability and security will depend, at the highest level, on the protection scheme and within this scheme of the existence or not of some redundancy. At the lowest level it will depend on the protocol and message structure and on the way these messages are affected by errors.

4.3.1. Protocols and message structure

A protocol is a set of conventions between communicating processes of which the aim is to make possible the exchange of informations on a given physical link with a given reliability and a given efficiency.
To make implementation and usage more convenient in sophisticated networks, higher level protocols may use lower level protocols in a layered structure (cf OSI model of ISO).
For efficiency reasons protocols for teleprotection are usually low level protocols which are based upon the choice of a specific frame format for the messages to be exchanged, i.e. a specific arrangement of the bits or bytes.

A frame or block contains different fields with well defined functions (fig. 4.2.)

1°) the Delimiters or Flags at the beginning and the end of the frame allow the frame synchronisation (e.g. start and stop bit in an asynchronous protocol)

2°) the Control field, when existing, is used for service and handshaking purposes (message type, frame length, frame number etc ...)

3°) the Address field is only necessary when there are more than one station in the network or in order to avoid the consequences of an accidental loopback.

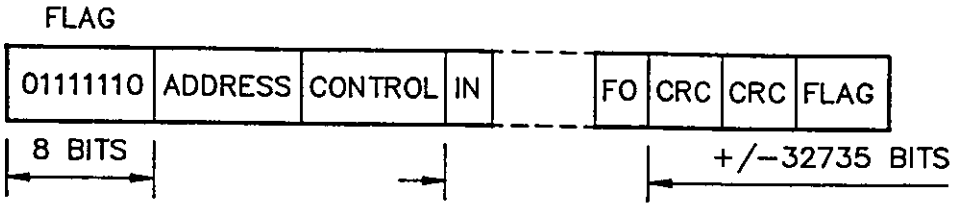
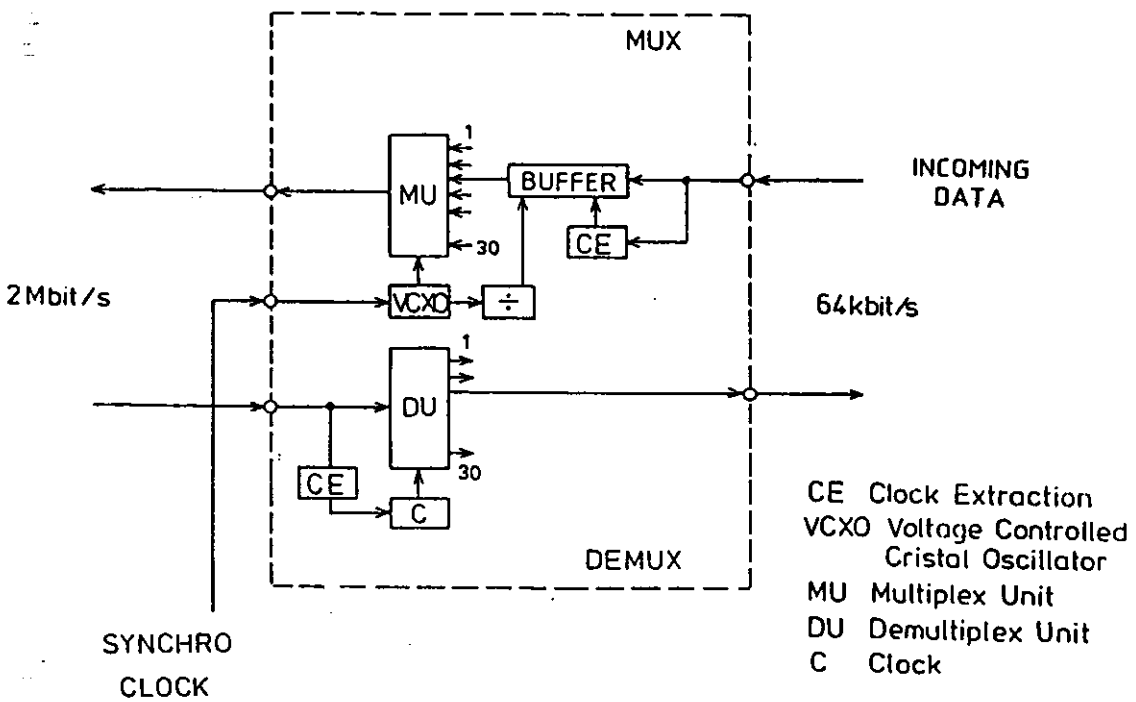
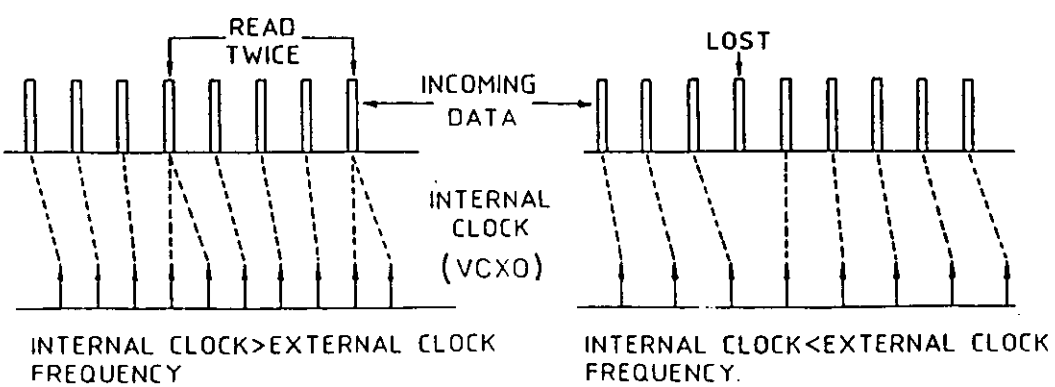


FIG. 4.2 EXAMPLE OF FRAME FORMAT (HDLC) FOR A COMMUNICATION PROTOCOL.





SLIP MECHANISMS

Fig 4.3

4°) the Data field contains the actual information

5°) the Frame Check Sequence (FCS) is a pattern of redundancy bits used for the detection of transmission errors (see also § 4.5.1.). The most encountered FCS are the Cyclic Redundancy Codes (CRC) and the parity bit (which is in fact a very simple CRC).

Due to the real-time nature of the communication of a protection system, error detection will produce rejection of the information. Retransmission of data is not to be considered.
Error correction is not impossible but can be very dangerous if there doesn't exist a mechanism for the detection of high bit error rate. Indeed error correction is a sophisticated way to ensure data integrity (mostly used for communications with very long transmission delays). As such it doesn't make exception to the principle described in appendix 1 : Error correction operates very well on a reasonably good channel but when the BER exceeds some threshold, the correcting mechanism, instead of reducing the BER, adds other bit errors in the transmitted pattern and the system fails.

The unit of information in a protection system is a block (or message). For a differential protection system, there will be a message for every set of current value that is sent for comparison to the remote terminal, in general, every time this magnitude is sampled.

For sampling rates of 200 to 2000 Hz (4 to 40 samples per cycle on a 50 Hz basis) message length must be shorter than 5 to 0.5 ms to keep in time with analogue signal sampling. These considerations are similar for a phase comparison protection system.

4.3.2. Relation between errors occurence and disturbed messages.

Let T be the duration of one message (e.g. T≈ 1.5 ms for a 100 bit message at 64 kbit/s) Let P be the probability that a transmitted message is corrupted i.e. that at least one bit error occurs during its transmission time T.

Assume also that the interference process is stochastic and that the errors are randomly distributed (this assumption is seldom true but will be discussed hereafter).
In this case the distribution of the errored bit will follow a Poisson law and $P = 1 - \exp(-\lambda T)$ where λ is the mean bit error rate per second.

$$\text{or } \lambda = C \times BER = \frac{1}{T} \ln \left(\frac{1}{1 - P} \right)$$

with C the bit rate and BER the bit error rate. Knowing that P is equal to the block error rate (BLER) and that C x T is equal to the message length (n) in bits we finally get

$$BER = \frac{1}{n} \cdot \ln \frac{1}{1 - BLER}$$

This important formula gives the possibility to calculate the required Bit Error Rate knowing the acceptable Block (or Message) Error Rate and the Message Length.

As an example suppose that a protection will work correctly, i.e. with an acceptable operating time (tac), if, on an average, no more than one message in every four messages is corrupted i.e. :

$$BLER = 25\ \%$$

Assume also that the message length is equal to 100 bits (T = 1.5 ms), we get then a maximum acceptable bit error rate of 2.9 E - 3.
It is important to see here that the shorter the messages are the lower the requirement for the bit error rate is and the higher the dependability will be. (*)

Moreover each message should be independent of the previous ones.
Under such conditions if a message is corrupted and discarded by the teleprotection receiver, the only consequence is a supplementary delay in the tripping decision equal to the duration of the last message.

As an example the protection should be able to operate correctly even if the communication is altered by lightning. The total duration of a lightning phenomenon can last between 0.1 and 2 s and involves several strokes (typically four) whose duration is normally shorter than 1 ms. So if the message length is no longer than say 2 ms only a very few percentages of the transmitted messages will be lost during the total duration of the lightning and the protection will operate correctly.

So far we have made the assumption that the transmission errors were randomly distributed. If instead we had assumed that they were uniformly distributed (flat distribution) we would have found the very simple result :

$$BER = \frac{BLER}{n}$$

(*) Note that if the messages are too short the security can be affected as the probability that noise simulates a valid message can be no negligible.

This is of course never the case but the calculations issued from this formula give usually quite good results for message error rates lower or equal to 25 %.
Actually errors are neither uniformely distributed nor randomly distributed but they occur mostly in burst (*)

However even with a burst distribution we can make the following assumptions :

1°) errors are randomly distributed within a burst
2°) bursts are randomly distributed within a disturbed period
3°) disturbed period are randomly distributed in the time

The first assumption leads in its turn to two possibilities according as the bursts are longer or shorter than the message length.

Most time they will be shorter than the message length and no matter the error distribution within the burst as the occurence of one burst means the corruption of only one message. So only the burst distribution and the rate of disturbed periods are relevant.

Sometimes the burst periods will be longer than the message length or it will be impossible to define an average burst length but the total time can always be divided into at least two periods with two different BER and the same assumption of randomly distributed errors within each period.

Anyway it is clear that the bit error rate is always higher than the burst rate. So, speaking about long term BER is irrelevant or at least very conservative. In other words an actual transmission channel with a long term BER of say 10^{-4} will be better (as far as data transmission is concerned) than an hypothetical channel with randomly distributed errors and the same BER. Conversely errors occuring in bursts are more disruptive to analog transmission (e.g. voice services) than the equivalent number of randomly distributed single bit errors.

For all those reasons it appears necessary to give some information about the distribution of errors and the way of measuring them.

4.3.3. Error distribution and measurement

In order to answer this question CCITT has proposed a set of rules through which measurement results could be presented to the user in such a way that they related the error distribution to the effect the impairment has on services.

(*) The usual definition of a burst is a bit group starting and ending with an error which is followed by at least k nonerroneous bits and whose distance between errors is less than k.
Practically it is spoken about burst whenever the bit error distribution clearly shows more than one peak (usually two).

This set of rules defined in the recommendation G821, basically applies to the 64 kbit/s communication channels that form part of an ISDN. Three parameters have been developed by CCITT to describe error performance regarding its distribution in time : degraded minute, severely errored second and errored second.

A degraded minute is a one-minute period where the short term error ratio, evaluated over one minute, exceeds 1E-6. In telephony, this error ratio is a boundary between virtually unimpaired transmission and impairment as likely to be perceived subjectively.

A severely errored second is a one-second period where the short term error ratio, evaluated over one second, exceeds 1E-3. This parameter is intended to be the means for controlling the occurrences of loss of frame alignment in multiplexer and other equipment within the network.

An errored second is a one-second that contains one or more errors. This parameter is mostly intended for data services, where the information is transmitted in blocks containing error detection mechanisms which ask for retransmission on errored blocks. Maximization of throughput therefore requires minimization of the number of errored blocks, a one-second period is adapted as a compromise value for data block size.

As has been said, if error performance is severe enough communication can be considered unavailable. CCITT has divided total transmitting time into different categories. More than ten consecutive severely errored seconds (BER>1E-3) mean that the connection is unavailable. Unavailable time ends when the bit error ratio falls down below 1E-3 every second during ten consecutive seconds. These latter seconds are counted into the available time. Degraded performance is obtained when there occur degraded minutes, errored seconds or less than ten severely errored seconds. The counting of degraded minutes is carried out only in that time when the connection is available and the severely errored seconds are excluded. Unavailable time due to transmission errors is counted into the total unavailable time already defined.

Are the CCITT recommandation G.821 suitable for teleprotection circuits ?

1°) Degraded minutes

A BER threshold of 10^{-6} is irrelevant for digital teleprotection circuits and is too low to seriously affect analog circuits. At the very most exceeding this threshold is an indication that something is getting wrong with the telecommunication link whether temporarily (e.g. fading on a radio link) or permanently (e.g. aging or damage in an optical link component).

2°) Errored seconds

As the length of the transmitted blocks for digital wideband protections is usually far shorter than one second this parameter hasn't a great significance and should be kept only for comparison purposes. A value of 100 or 10 ms would certainly have been more suitable in the context of protection.

These three grades are defined as

- local grade
- medium grade
- high grade

Depending of the grade considered apportionments are block allowances regardless of the length or on the contrary are proportional to the length.
Details about these apportionments can be found in [1].
This document proposes a logical way for making the correlation between CCITT HRX model and the CIGRE model.
This correlation leads to the following requirement for a 64 kbit/s circuit of power utilities :

% of minutes with BER < 10^{-6} : 98.5 %
% of seconds with BER < 10^{-3} : 99.97 %
% of error free seconds : 98.8 %

As regard the availability objectives, CIGRE WG 35-02 proposes a percentage of 99.99 % available time for the highest level of telecontrol circuit.
According to CCIR Recommendation 557, digital radio links should have an availability better than 99.7 % referred to a theoretical 2500 km circuit.
Applying a proportional rule for a shorter length L (km) this gives

$$A\ (\%) = 100 - (100 - 99.7)\frac{L}{2500}$$

e.g. for L = 200 km, A = 99.98 %.

All these availability and error performance objectives seem to be quite acceptable and even conservative when compared to the observation results of a six hops 200 km microwave link given in table 4.1.
Other figures coming from different countries confirm these results.

3°) Severely errored seconds

Although originally proposed for voice traffic, this paremeter can be considered as the most important for teleprotection. Discussion exists about the choice of 10^{-3} for the threshold which seems quite high. But as teleprotections are relatively insensitive to high B.E.R. (*) it could be a very suitable parameter.

4°) Availability

The choice of 10 consecutive severely errored seconds as limit for (short term) unavailability has no particular meaning for protection. It can however be a way to determine the origin of a disturbance, e.g. for a radio link long periods of severely errored seconds could be attributed to fading or radio interferences whereas short periods would be due to transient interferences.
Nevertheless the most important parameter from a protection point of view seems to be the sum of the unavailability periods and of the severely errored seconds. It must however be pointed out that this result is only an indication about the quality of the channel but is not necessarily equal to the unavailability of the protection itself which can be much lower (cf. § 4.7.). Moreover the correlation factor between unavailability periods and faults occurence is of the utmost importance.

Aside from these considerations we may stress on the fact that the essential merit of this CCITT recommendation is to exist and is to be a widely accepted standard for measurement and comparison purpose.

Measurements can be made either by using dedicated pseudorandom patterns or by monitoring "coding rules violations" in real traffic. However it has been shown [3] that the latter method could sometimes lead to erroneous results when dealing with burst errors.

4.3.4. Performance objectives

CCITT G.821 recommendation specifies the performance objectives for an Hypothetical Reference Connection (HRX) of 27500 km. Each of the objectives is expressed as a "percentage of time" during which the criteria set by the relevant performance parameter are being met. They can be resumed as follows :

% of minutes with BER < 10^{-6} : 90
% of seconds with BER < 10^{-3} : 99.8
% of error free seconds : 92

Since the model uses a connection length of 27500 km and most systems operate over lesser distances it was found necessary to provide a strategy which allocated proportions of the overall performance objective to different circuit classifications within the HRX. The apportionment is based on three grades of circuit quality each of which is representative of a practical digital transmission section.

(*) This due to the short length of the messages and to the large amount of redundancy enclosed in the protocol (message repetition) or sometimes in the protection scheme (path diversity).

Performance over one year of a belgian 200 km radio circuit (6 hops - 2.6 GHz)

(according to CCITT G.821 definitions)

		Monthly results		Comparison basis			
		Average	Std. dev.	CCITT HRX	CIGRE objective	CEGB objective for protection	British Telecom. objective
a	% availability	99.993	0.007		99.99	99.99	99.85
b	% of seconds with BER < 10-3	99.997	0.003	99.8	99.97	99.999	99.95
c	Total % of second with BER < 10-3 (*)	99.99	/		99.96	99.99	99.8
d	% of minuted with BER < 10-6	99.97	0.03	90	98.5	99.9	99.5
e	% error free sec	99.992	0.007	92	98.8	99.9	99.5

Table 4.1.

(*) (1 - c) = (1 - a) + (1 - b)

4.4. Dependability

4.4.1. Relationship between error performance and dependability (*)

A relation between the maximum allowable - short term - bit error rate and the acceptable message error rate has been established in the previous paragraph.

This relation has shown that the threshold of 10^{-3} fixed by CCITT for defining the severely errored second (S.E.S.) was not far from the maximum allowable BER for a protection.
In the absence of information about error distribution inside the S.E.S. we will assume that each time a S.E.S. happens the protection is not able to operate correctly. This is a rather conservative assumption knowing that a BER of 10^{-3} means only 64 errors during 1 s (at 64 kbit/s) which can all be concentrated in one or two messages as they occur mainly in burst.
Conversely we assume, by simplification, that there is no more than one fault per line per second. In other words a protection equipment is not required to operate more than once per second.
We further assume that there is no correlation between fault occurence and S.E.S. (both events are independant) and that the S.E.S. are randomly distributed in the time so that their probability of occurence (or repetition rate) is equal to their percentage :

- Let P_{ses} be this probability
- Let R be the fault rate per line, per year (i.e. the number of times a protection equipment is required to operate each year)
- Let P_{ft} be the acceptable failure to trip probability per equipment year (due to the telecommunication system).

Then we get :

$$\boxed{R \times Pses \leq Pft}$$

Example (very conservative) :

$R = 10$ (10 faults per year, per line)

$Pft = 10^{-2}$ (one failure to trip in 100 equipment-years)

giving :

$$P_{ses} \leq 10^{-3}$$

This is to compare to the CIGRE objective for P_{ses} :

$$P_{ses} = \frac{100 - 99.96}{100} = 4.10^{-4}$$

which appears to be a very realistic dependability objective.

(*) We assume here, by simplification, that the dependability of the protection relates directly and solely to the availability of the telecommunication channel.

It is an evidence, on the other hand, that a protection scheme in which the telecommunication system shows some correlation between its failure probability and the fault probability will require far better figures for P_{ses}.
Such systems should be avoided or the correlation factor has to be reduced sufficiently by proper design (screening, earthing,...).

4.4.2. Other parameters affecting dependability

Slips

A slip is the loss or insertion of a bit or a series of bits in the data stream. Slips occur each time the clock used to sample the data stream is not exactly at the same frequency as the data speed.
When the significant instants of the digital signal deviate on an erratic way from their ideal position in time, one speaks about jitter (or wander for very low frequency jitter). Jitter is mainly due to repeaters used on cable communication links. When the deviation increases continuously it means that there is no synchronization between data and clock i.e. that the clocks at each end of the communication link are not exactly at the same frequency (they are said to work **plesiochronously**).
In this case, a bit will be periodically lost or inserted in the data stream (fig. 4.3.). This is called a **controlled slip**.
However at the 64 kbit/s level and sometimes also at higher levels memory buffers are used with independent write and read clocks. The write clock is derived from the data stream whereas the read clock is synchronous to the local clock.
These buffers act as filters for the jitter, reducing highly the risk of slip due to jitter.
In case of lost of synchronization they will only reduce the occurence of slips but increase their length i.e. the number of repeated or lost bits.

To understand this assume a buffer size of n bits, an incoming data speed (equal to the write frequency) of f1 (bit/s) and an outgoing data speed (equal to the read frequency) of f2.

If $f2 = 0$ the buffer will be full after $T = \frac{n}{f1}$

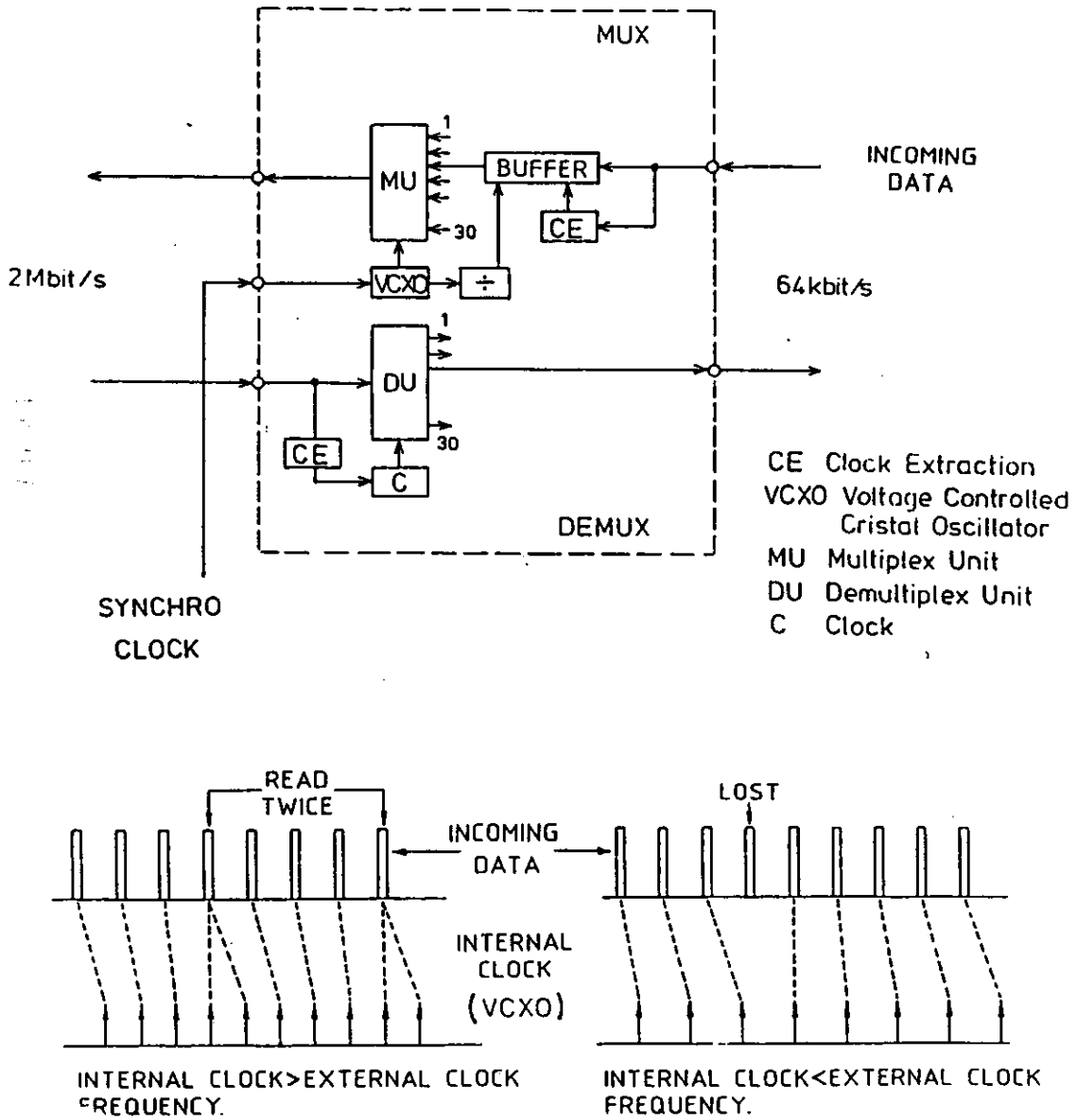
with $f2 \neq 0$ the buffer is full after $T = \frac{n}{|f2 - f1|}$

Specifying the buffer size in seconds instead of number of bits we have :
buffer size (b) = n/f (with $f \simeq f1 \simeq f2$)

and $$T = \frac{b.f}{|f2 - f1|} = \frac{b.f}{\Delta f}$$

knowing that $\Delta f/f$ max is the clock tolerance or deviation and that the time between slips is equal to the buffer filling time we get :

$$\text{Minimum time between slips} = \frac{\text{buffer size (in s)}}{\text{clock tolerance}}$$



SLIP MECHANISMS

FIG. 4.3

As an example most multiplexer oscillators, when not synchronised, have a clock tolerance of ± 50 ppm as specified by the CCITT
The buffer size at 64 kbit(s) is normally at least equal to one byte (8 bit) that is : 125 µs. So the minimum time between slips will be of

$$\frac{125.E-6}{1.E-4} = 1.25 \text{ s}$$

The duration of the impairment will be of one to a few bytes and will thus not affect more than one or two consecutive messages.

Network synchronization

In order to avoid slips in a data network all the oscillators of the network must operate at the same frequency (*). This is usually achieved by synchronizing all these oscillators whether following a master-slave hierarchy or a mutual procedure. The synchronizing information can be included in the data stream or follow a special sub-network.
When data have to cross from one network to another there will be unavoidable slips. For that reason the master clock of each network is usually chosen with great stability and accuracy (Cesium, Rubdium or oven stabilized quartz oscillators) so as to insure a minimum rate of slips. Such a system, working with independent clocks, is called plesiochronous. With very high grade clocks (Cesium) slips will occur no more than one time every 70 or 80 days.

(*) This is only true for the low level of the multiplexed hierarchy (see § 5.2.2.-2°) i.e. at 64 kbit/s and 2 Mbit/s. For the higher levels plesiochronous working is possible thanks to the existence of a bit stuffing mechanism (insertion/deletion of supplementary bits in the data stream).
Thanks to this justification mechanism the multiplexed hierarchy is called Plesiochronous Digital Hierarchy (PDH) by opposition to the recently developped Synchronous Digital Hierarchy (SDH).
Failure of that mechanism leads usually to a slip of one bit at the 2Mbit level called a non-controlled slip.
One should also point out that digital networks that carry only analog data can operate without any synchronization.

This is to compare with the plesiochronous working of a network which has lost its synchronization : each oscillator will fall back on its own frequency with an accuracy of ± 50 ppm and in the worst case slips will occur every 1.25 s as explained hereabove.

Another kind of desynchronization happens when, in a TDM system, the frame or multiframe alignment is lost. This means that the message structure at the first multiplex level, i.e. 1.5 or 2 Mbit/s, can no more be recognised, with a consequence that the receiver enters a frame delimiter search procedure in order to recover synchronization. The total duration of the synchronization loss ranges about 1 or 2 ms ; its occurrence depends on the existence of elastic buffers at the 2 Mbit/s level and on the cause of impairment. Most impairments are jitter or wander (i.e. very slow jitter) mainly encountered with repeater structures on cable transmission. Fading on radio transmission can also be at the origin of frame disalignments.
At the user level, impairment is seen as a burst error of the same duration (≃ 1 ms) sometimes partially replaced by an AIS filling sequence or by a modification of the co-directional 64 kbit/s pattern (suppression of the 8 kHz synchronization).

Anyway as far as protections are concerned controlled slips at 64 kbit/s level (due to lost of synchronization) or even loss of frame alignment at higher bit level seem to have little influence on the dependability because no more than one transmitted message is normally affected.

4.5. Security (*)

If the dependability of the protection depends directly on the error performance characteristics of the telecommunication channel, its security mainly rests on the methods and more particularly on the protocols, used for detecting errors and insuring data integrity.

4.5.1 Protocols

In an imperfect environment high data integrity and fast data transmission are conflicting properties : increasing demands for data integrity will be fulfilled at the expense of decreasing net speed of information flow with the result that the supplier could be tempted to minimize the response time of his protection at the expense of security.
Data integrity is usually achieved by redundant block coding methods (CRC etc...) whose main characteristic is the Hamming distance.
This Hamming distance (i.e. the minimum number of bits which have to be corrupted in a message to give rise to an undetected residual error) is only an indication of the capability of the code to detect errors at small bit error rates (BER). At higher BER the Hamming distance becomes totally insufficient to insure a low residual error rate (RER) (**)
This is illustrated on figure 4.4. by two different protocols.
Protocol 1 has only a Hamming distance of 1 while protocol 2 has a Hamming distance of 4. Both protocols used the same number r of redundancy bits (which is given by the RER at a BER of 0.5) but protocol 1 gives better protection for high BER whereas protocol 2 is more suitable for low BER.

(*) seen at the telecommunication level

(**) residual error rate = $\frac{\text{Nr of undetected wrong messages}}{\text{Total Nr. of messages sent}}$

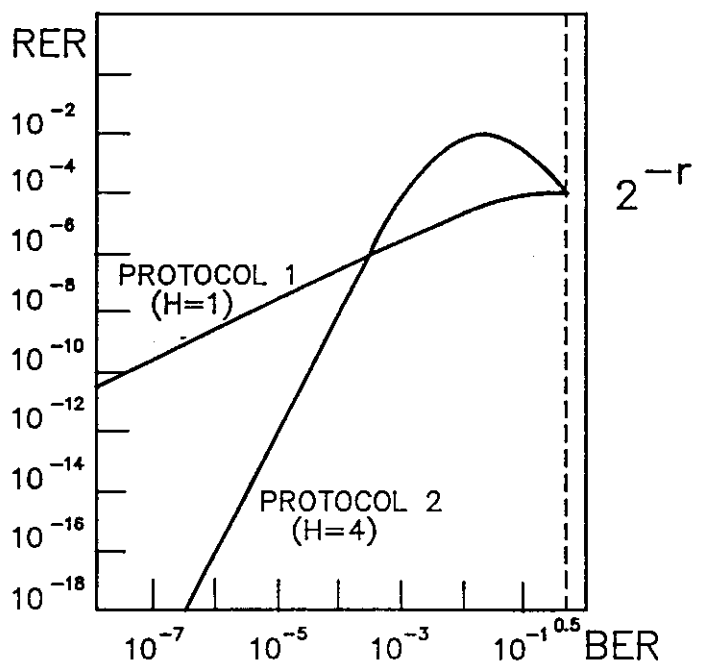


FIG. 4.4 EXAMPLE OF RESIDUAL ERROR PROBABILITY IN FUNCTION OF THE BIT ERROR PROBABILITY.

This example clearly shows that the chosen protocol has to meet specific requirements.
In the absence of existing specification for protection it seems advisable to refer to the works of IEC TC 57 on "Telecontrol equipment and systems - part 5 : Transmission protocols" published under IEC 870-5 standard.
Three integrity classes have been defined in this standard and are presented on table 4.2.

To illustrate their significance, let us imagine a system which transmits message blocks of n = 100 bit, at a rate V of 64 kbit/s, over a channel with noise producing a bit error rate of p=1E-4. The relation between expected mean time between undetected erroneous messages, Θ, and residual error probability, R, is given by :

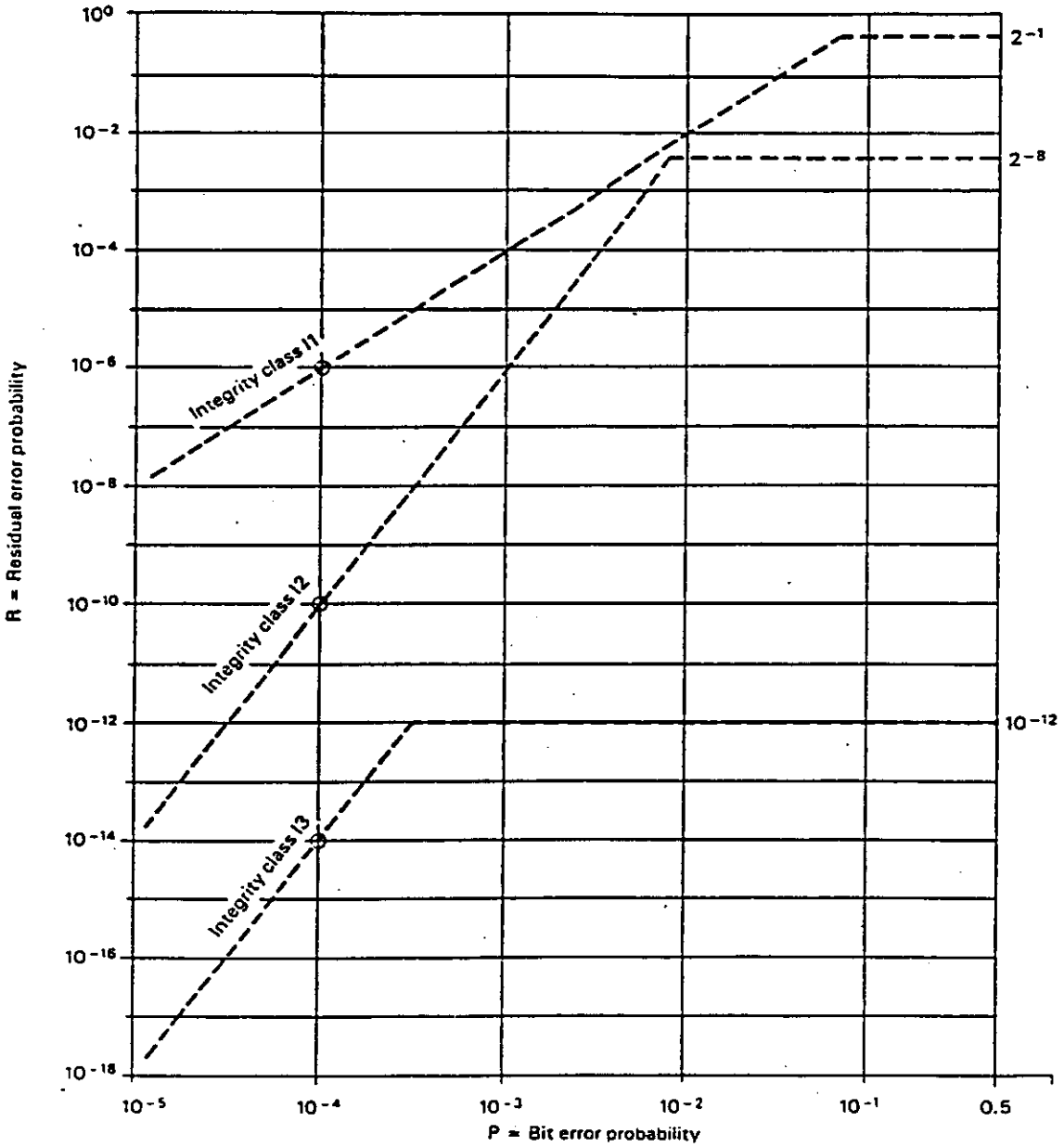
$$\Theta = \frac{n[bit]}{V\ [bit/s] * R}$$

So, for each data integrity class, we have

I1	R(p=1E-4)	$= 10^{-6}$	Θ = 26 minutes
	R(p=0.5)	$= 2^{-1}$	Θ = 3 ms
I2	R(p=1E-4)	$= 10^{-10}$	Θ = 181 days
	R(p=0.5)	$= 2^{-8}$	Θ = 0.4 s
I3	R(p=1E-4)	$= 10^{-14}$	Θ = 5,000 years
	R(p=0.5)	$= 10^{-12}$	Θ = 50 years

With the integrity class I3, the expected mean time between unwanted tripping T will be kept beneath 50 years under continuous disturbed conditions. Knowing that such conditions are normally encountered during less than 1 % of the time we come back to an actual T of 5000 years which is quite acceptable.

Requirements of class I3 protocols are a minimum Hamming distance of 4 and a maximum RER of 1.E-12 regardless of the BER. This class is intended for "critical information transmissions" such as telecommands; it can certainly be retained as a standard requirement for protection as the effect of undetected errors on protection is uncontrolled and could result in both undesired tripping or no tripping. Although, as most protection designs require more than one message to make a trip or command decision, the residual error probability of an undesired trip is significantly lower than the residual error probability of an undetected wrong message.
We must also consider that the protection, especially an analogue protection system, may further detect errors as incongruous information. But the inverse can sometimes also be true : if the communication channel used by an analogue protection is accidently looped back and if the protocol doesn't involve a special check on the address field the received messages will pass all the error controls and the risk of faulty trip will be very high.



Data integrity classes.

TABLE 4.2

So the integrity requirements should in fact apply to the protection in its whole and not only to the telecommunication protocol. In other words the correct definition of the residual error rate should be here :

$$RER = \frac{\text{Nr of maloperations}}{\text{Total number of messages sent}}$$

4.5.2 Signal quality supervision

As had been shown hereabove, protocols achieving class I3 security requirements must use redundancy codes of very high quality giving rise to a difficult tradeoff between efficiency (speed) and security. Moreover high level codes, with a minimum Hamming distance of 4, are sometimes of poor efficiency at high bit error rates (*).
Knowing that most telecommunication channels present generally a "bistable" behaviour, i.e. a very low BER in the absence of disturbances and a very high BER in the presence of disturbances (*), one could be tempted to use other methods to achieve data integrity objectives.
Among them signal quality supervision is a powerful means for detecting elevated disturbance levels. It gives the possibility to raise an alarm signal whenever the transmission quality decreases under a given level. Such a system exists in most radio TDM systems where an alarm inhibit signal (AIS), i.e. an only "one" filling sequence, is generated by the telecommunication system each time a sufficient transmission quality is not achieved for a given time. Such an alarm prevents the BER to rise above 1.E-4 or 1.E-3 but leads to an increase of the unavailability periods. Moreover, due to the error detection mechanism, there usually exists some hysteresis in the alarm occurence extending again the unavailability time. This can be a severe drawback for protections using shared telecommunication circuits, and more specifically radio links where fading can severely affect the transmission quality during periods of several seconds or even minutes without actually preventing the communication possibilities.
The consequence of this is that signal quality supervision which is very useful for data transfer seems to be less suitable for circuits involving protections or should be adapted for each kind of application.

4.6. Transmission delay

An important feature of the telecommunication medium, when dealing with teleprotections, is the transmission delay. This delay depends not only on the distance between protections but also for a great deal on the type of carrier and multiplexing equipment used. Moreover this delay, even for a given path, is not always constant with the time because of the existence of elastic buffers in the multiplex equipments.

(*) This is in accordance with the general behaviour of high quality systems mentioned in appendix 1.

The introduction of intelligence in the late telecommunication equipments (automatic rerouting, channel insertion or deletion etc...) has also as a consequence an increase of the overall delays.

For all those reasons telecommunication protocols for protections should be able to cope with a wide range of time delays and should preferably include an automatic adaptation to it.

A digital differential protection will usually calculate the transmission delay for each current sample. The usual method is to measure the time it takes for a message to reach the protection at the other line end and return, and presume half of the delay corresponds to each way. This is usually a valid supposition, though care must be taken in those cases where channel routing is different in each direction of communication. This method places no theoretical restrictions on transmission delay or its variations.
Independently of individual solutions to take transmission delay into account, the fact remains that this parameter is one of the significant components of protection operating time. Power systems have become more heavily meshed and with greater short-circuit power. This has made fault clearing time critical for the stability of the power system. We can say that protection systems in service today narrowly meet this requirement and that care must be taken for the choice of a suitable communication medium with an acceptable transmission delay.

Following table shows the typical range of the one way delays.

Equipment	Delay (µs)
symmetrical or coax cable	5/ km
optical cable	5/ km
radio propagation	3.3/km
2 to 8 Mbit/s multiplexing	5-15 (*)
2 Mbit/s terminal/repeater	0.5-1
Optical terminal	0.4-1
radio emitter/receiver	5-15 (*)
64 kbit/s to 2 Mbit/s multiplexing	300-600 (**)
" " with insertion possibilities	600-1000 (**)
300-3400 Hz FDM filter (for comparison)	600

The table shows that the delay over the medium itself (cable, optical fibre, microwave) is equivalent in all cases, the greater difference coming from the level of multiplexing of the communication link. A dedicated optical link, two hundred kilometres long, has a one way delay in the order of :

(*) delay variation between two different equipments
(**) delay variations for the same equipment

t= (0,4 to 1) x 2 + 5 x 200 ≃ 1 ms

while a multiplexed circuit of the same length with three links at 64 kbit/s has

t = (600 to 1000) x2 x 3 + 5 x 200 ≃ 4.6 to 7 ms

This last figure is in the order of the transmission delay of telecommunication systems being used today for protection purposes. If the evolution of protections and circuit breakers can achieve shorter clearing times (under half a cycle), communications for protection purposes would necessarily need a dedicated link.

4.7. Effect of telecommunication channel unavailability on protection

4.7.1 Radio link versus optical fibre

When comparing microwave to optical fibre, long term unavailability figures may be worse for the latter because its MTTR is normally higher; but more important than the absolute figures is the correlation between the unavailability periods and the faults occurence.

As the optical fibres will usually share the same path as the power line, part of the unavailable time may be due to a failure involving the power line itself (fallen towers, broken earth cables, etc...) and may therefore not affect the protection user (this is also the case with PLC links)
However, wether the teleprotection circuit takes the same path as the protected line (e.g. in a multiended scheme), or not, the risk is high, for instance by stormy weather, that a positive correlation exists and that the dependability of the protection is affected.

Short term reliability or availability refers to non permanent outages or non acceptable transmission conditions due mainly to disturbances (fading, radio interferences, lightnings, transient disturbances etc...)
As optical fibres are not affected by electromagnetic disturbances they will normally show better short term reliability figures but special care must be taken for the terminating equipment which can be very sensitive to disturbances.

Most outages occuring on radio links are due to fading or radio interferences (radar, mobile radio) and are seldom correlated to faults on power lines.
On the other hand, experiments made at the Lightning Discharge Study Station of Saint-Privat-d'Allier in France during the summer of 1990 and 1991 have shown that radio links were very insensitive to indirect lightning strokes but that a direct impact on a telecommunication tower could lead to several Severly Errored Seconds when the cabling was not very well shielded.
It has also been established that the important storms of the winter of 1990 haven't had any effect on the 2,5 GHz radio network in Belgium whereas a lot of power line towers fell down.

4.7.2 Alternative routing

Equipment redundancy is of course the only way to approach the 100 % availability of both the communication channel and the protection scheme. However it is always difficult to know how far to go in redundancy; in most cases preference will be given to a scheme using a primary and a secondary protection system which are not 100 % reliable, but with a minimum of correlation between respective unavailability periods, rather than to a highly redundant system in which common mode failures remain unavoidable.
Nevertheless the existence of two equivalent systems, the one of which, though normally switched on, is not operating ("hot standby"), can be very helpful and also better availability by reducing maintenance time. Both systems (main and back-up) can also operate in parallel avoiding the use of an actual switch that can be itself at the origin of a failure. This is the case, for example, with radio antennas working in space diversity in order to cope with different propagation paths and to minimize the effect of fading.
When alternative routing is used the level at which the switch over decision is taken is important. Preference should be given to a protection system able to manage on its own the alternative routing than to a system where the switching is operated at the telecommunication network level. This can easily be achieved in a multiended protection scheme where each node can be used as a "rerouter" in case of loss of one link between two nodes but it should also remain possible in a two ended scheme as far as a secondary telecommunication path can be offered.

4.7.3 Protection behaviour

Long term unavailability of the telecommunication system (outages) usually renders the protection system unavailable too.

As a partial exception, a distance protection can remain in service without communication, although its performancce is degraded : simultaneous fault clearing is not assured, selectivity is time delay based and failure design criteria may not be complied with.

For an unit protection, i.e. an absolutely selective protection system (differential, phase comparison or directional comparison), unavailability of the telecommunication channel would have following consequences :

a) Loss of security in a blocking phase comparison or blocking directional comparison system, which would trip for faults anywhere inside their area of sensitivity.

b) Loss of dependability in a tripping (or unblocking) phase comparison, directional comparison or differential protection system, which would be unable to trip for faults in the protected line.

It is therefore desirable for these protections to have mechanisms for the detection of unavailability of communication. Digital links provide permanently active telecommunication circuits to the protection user, allowing for easier permanent supervision of channel integrity. The action following the detection of unavailability should be user-selectable. In most cases blocking of the protection will be preferred, and therefore security over dependability.

Short term or sudden unavailability is produced by fading, disturbances, errors, slips, etc. As has been said in 4.3.3. the definition of ten consecutive severely errored seconds as the limit for short term unavailability has no special meaning for protection. It is the non reception or the rejection of errored messages which will affect protection behaviour.

In a differential or phase comparison protection, it is necessary for each protection to have information about the sampling instant of the protection at the other line end (or of the time delay of the telecommunication channel, which is practically equivalent). This will probably imply a time tag included in each message. Due to this need, a lost message may affect one or several consequent words until synchronism between terminals is regained, rendering the protection unavailable for a longer time than unavailability of the telecommunication channel lasts. As an example, let us imagine a protection which only accepts a message as valid if its time tag is in sequence with the one in the previous message. The protection function will be lost if, in the average, one out of every two messages is corrupted. This corresponds to a BER of 7E-3 using the formule of p 6 and messages of 100 bits.

As noise actually occur in burst, given the above BER, less messages will be affected and the protection will probably still function.

Another effect of non-received or rejected messages is a delay in protection decision. In a digital protection, any final decision (tripping, blocking, unblocking, etc.) needs a certain subsequent number of coincident decisions. The loss of a message may imply a break in such a sequence, restarting the internal counter or just delaying decision for a duration equal to one message length.
Delay in tripping, if the maximum acceptable tripping time is exceeded, is equivalent to no tripping (loss of dependability). We can establish an acceptable instantaneous operating time tac, under disturbed channel conditions (e.g. 40 ms). An operating time longer than tac shall be regarded as a loss in dependability. Moreover if back up protection has time to operate (e.g. t = 250 ms), there will be a loss of selectivity. If the increase in operating time stays below tac, there will be only a loss in speed.

In a blocking scheme, the delay in the decision of "reception of blocking signal" in case of external faults may be the cause of an undesired trip and therefore a loss of security.

The effects of unavailability or poor performance of telecommunication system on protection have now been discussed, but we must underline that the impairments described concern the dependability and occur when there is coincidence between degraded telecommunication performances and fault (short circuit) in the power system. Comments about the probability of such coincidence has already been made. When the power system isn't faulty, the security of the protection system becomes the main parameter; it depends on the protection design and barely on the quality of the transmission.

4.8. Command teleprotections

So far in this section we have dealt essentially and implicitly with equipments exchanging a great amount of information, i.e. differential protections.
The question which arises now is : what can a wideband channel bring to a classical command teleprotection system ?

It has been pointed out in § 4.1. that there was no real difference, as far as channel capacity is concerned, between a good analogue voice band channel and its digital equivalent a 64 kbit/s.

However a command teleprotection is a system designed to transmit ON/OFF signalling i.e. information in its pure digital form. Whenever the only available telecommunication medium is analogue, as it is in most cases, it is necessary to convert this digital information into a suitable analogue form by means of a dedicated modulation procedure. The best known and also the simplest to implement is the FSK modulation which is almost universally implemented. However a modulation technique is nothing else than a tool used to adapt the caracteristics of a signal in this case a digital signal - to the transmission characteristics of the channel in order to approach as near as possible the information capacity of this channel. This tool, of course, is never perfect. Even coherent phase modulation which is one of the best modulation technics (some 4 dB less exacting in S/N than FSK) is far from the ideal Shannon limit (cf. appendix 1.). When, on the contrary, the channel is already digital it is of course preferable to exploit it in its digital form and to make use directly of the available capacity.

In this respect it is a technical nonsense and an important waste of capacity to first convert the digital signal into an FSK analogue signal and to digitalise this latter by PCM coding into a 64 kbit/s stream.

The consequence of this is that a well designed command teleprotection with a digital wideband output should be better than any well designed command teleprotection with analogue voiceband output. (*)
Better means here that the digital equipment (i.e. with digital output) will have
either a better security
or a faster response
or a greater capacity (more commands simultaneously transmitted in the same channel)

4.8.1 Security

By the choise of a good protocol it becomes easy to achieve a very high security comparable to Integrity class I3 of IEC 870-5 standard. In other words it is possible, whatever the noise level or the BER, to keep the probability of an unwanted tripping beneath 10^{-12}, what seems not possible with a classical analogue command teleprotection.
Direct trip schemes can thus be done without extra criterions.

(*) Provided they are associated with the same wideband communication system. It is an evidence that a classical analogue teleprotection remains necessary whenever a classical (not PCM) voiceband channel has to be used.

4.8.2 Faster response

The use of very short messages (typically 5 or 6 bytes, i.e. shorter than 1 ms) and the absence of selective filters indispensable in any analogue command protection makes it possible to achieve tripping times in the range of 2 ms with the security level of class I2, or 5 ms with that of class I3.

4.8.3 Dependability

As has been explained in § 4.3. and in appendix 1, modern digital communication systems (whatever their user interface is : analogue or digital) present generally a go-no go behaviour : in the absence of disturbances exceeding a certain threshold, they are very good whereas in the presence of such disturbances they can be considered as unavailable.

In consequence, the dependability of the command protection lies more in the availability of the channel than in the design of the teleprotection equipment itself.
For this reason the expected gain in dependability will not be as evident as the expected gain in security.

4.8.4 Greater capacity

Up to a recent past analogue command teleprotection were based on analogue technology; so it was difficult to include in one single equipment more than one or two commands.
Nowadays digital technology allows a greater integration of the teleprotection functions and nothing more prevent the manufacturers from multiplying the number of commands per equipment.
However it remains by far more easy to add some bits or bytes in a message than to time multiplex digital filters. Therefore, it should be logical that the cost of a multi command digital teleprotection remains close to that of a single command teleprotection and certainly lower than that of a multi command analogue teleprotection.
Moreover going from a single command to a six commands digital system will have practically no incidence on the security, the dependability and the response time, because it only adds a few bits to the messages whereas the same evolution in an analogue command teleprotection reduces in proportion the available bandwidth and affects directly the performance parameters.

4.8.5 Conclusion

It seems to be evident that the coming out of command teleprotections with wideband digital output is a significant progress and can lead to the implementation of fast and reliable phase selective command protections.
An example of a possible teleprotection organisation needing up to 9 commands in a segregated scheme is given on fig. 4.5.

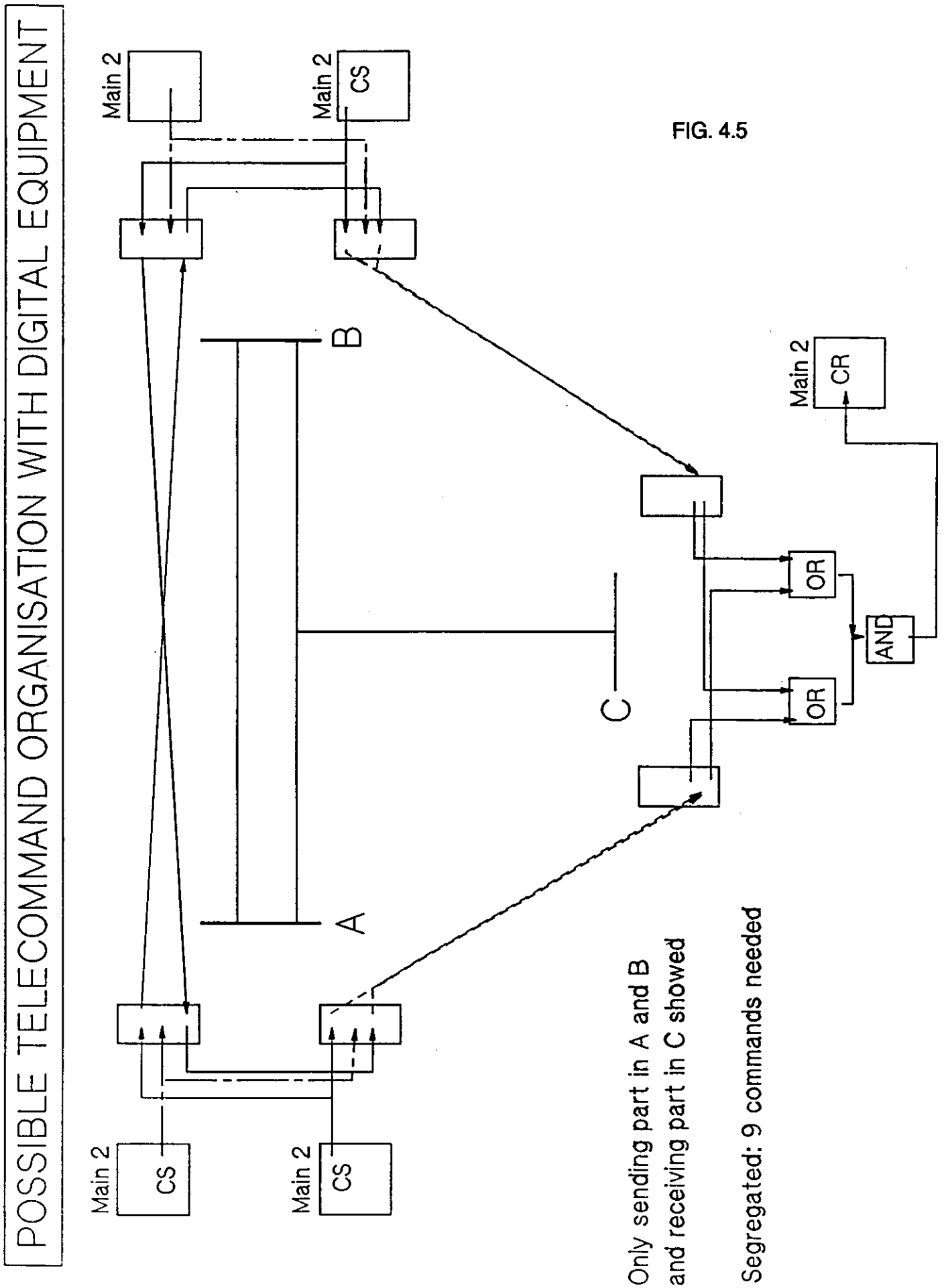

POSSIBLE TELECOMMAND ORGANISATION WITH DIGITAL EQUIPMENT
Main 2
CS
Main 2
CS
Main 2
CS
Main 2
CS
Main 2
CR
A
B
C
OR
OR
AND
Only sending part in A and B
and receiving part in C showed
Segregated: 9 commands needed

FIG. 4.5

5. STANDARDIZATION FOR PROTECTION/COMMUNICATION INTERFACES.

5.1. Scope and definitions

Extending the definitions of CEI-TC57 publication 834-2 and CIGRE WG 34/35-05 on "Protection systems using telecommunication" it is necessary to distinguish different levels of interface (cf. fig. 1).

a) Interface between protection equipment and current or voltage transformer.

This interface is out of the scope of this document.

b) Interface between protection equipment and teleprotection equipment (*)

Most time, for broad band equipment, protection and teleprotection are in the same equipment or are provided by the same supplier. However it could happen, mainly for command protections, that command signals coming from different protection equipments were sharing together the same teleprotection equipment in order to reduce costs or to make use of an optimal coding process and to be sent on a wideband telecomminication channel.
Nevertheless in the context of this document and as far as analogue protection are concerned, protection and teleprotection will be considered as part of the same equipment.

c) Communication medium within the substation.

Protection equipment and telecommunication equipment can be separated from each other by several hundred meters. Communications between both equipment have to be done by a special medium which has to cope with severe EMC conditions.

Though this communication medium could theoretically be shared with other users (L.A.N) it will normally be dedicated to the protection and based on a direct metallic or optical link for which an interface has to be defined.

d) Interface to the telecommunication system

Two cases have to be taken into consideration whether the telecommunication medium is shared with other users or not.
In the first case the interface should normally be imposed by the telecommunication system.
In the second case the telecommunication medium will be a simple metallic or optical link. The transmitter/receiver system whether analog or digital is usually proprietary of the protection supplier and will be included in the teleprotection equipment. The supplier is then free of the kind of interface and/or protocol he wants to use.
In any case when the distance between protection equipment and telecommunication equipment is short, interface d) and c) ar not discernible from each other.

(*) The term "teleprotection" should be understood here in its wide sense, i.e. as well for analogue protections as for command protections.

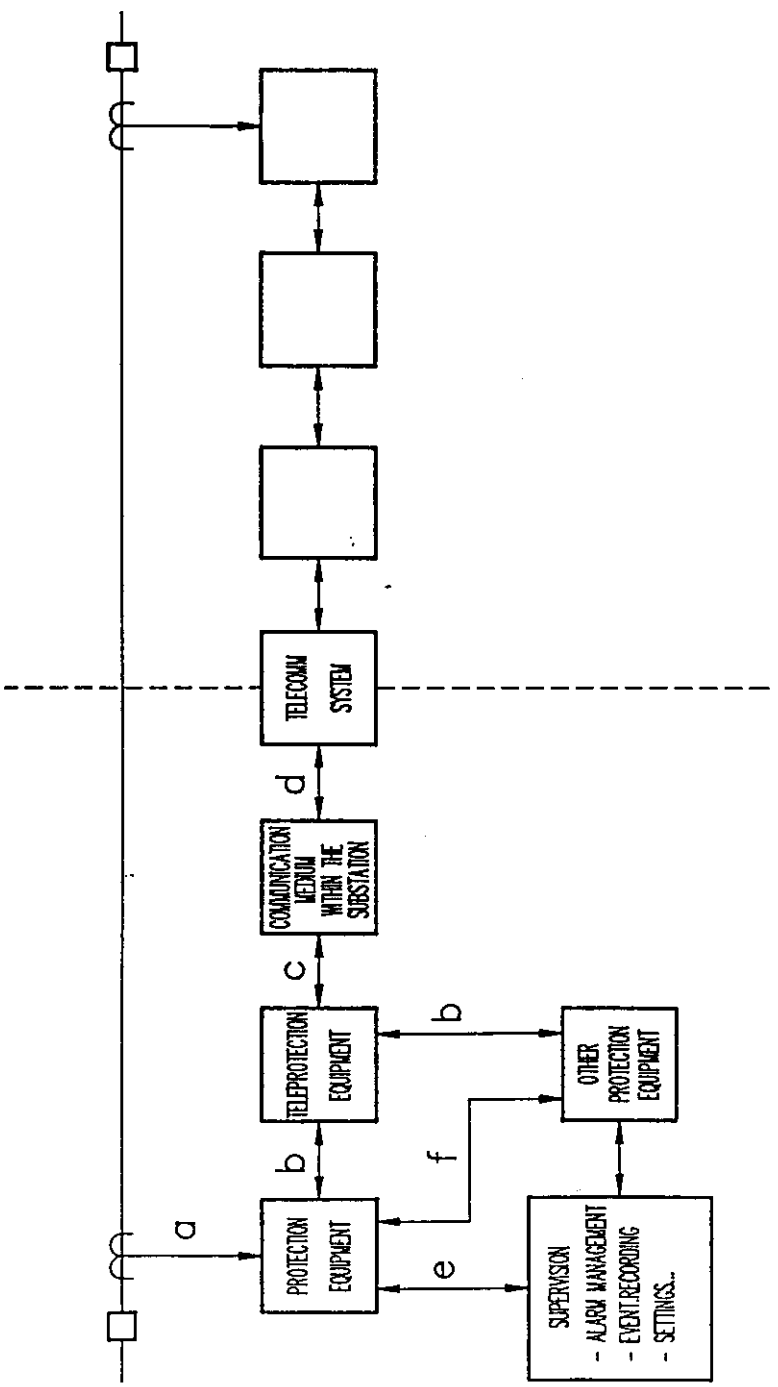

a
PROTECTION EQUIPMENT
b
TELEPROTECTION EQUIPMENT
c
COMMUNICATION MEDIUM WITHIN THE SUBSTATION
d
TELECOMM SYSTEM
b
OTHER PROTECTION EQUIPMENT
e
f
SUPERVISION
- ALARM MANAGEMENT
- EVENT RECORDING
- SETTINGS...

FIG. 5.1

e) Interface between protection equipment and outside world

This interface relates to the connexion with other equipments like event recorders, local or telecontrol equipments etc... or concerns the exchanges with the operator (man machine interface) for settings, controls or alarms.
It should be normally an open low speed interface and can be realized by a serial port or an access to a local area network. This latter is outside the scope of this work; moreover low speed access to a LAN can generally be done by a classical serial port.

It is only possible here to mention the most important existing or to be normalised standards.

CSMA/CD (IEEE 802.3) : Ethernet...
Token bus (IEEE 802.4) : MAP, Proway C ...
Token Ring (IEEE 802.5) : IBM,...
Optical Token Ring (ANSI X3T9.5) : FDDI...
Fieldbus (ANSI RS-485) : FIP, Profibus...

f) Interface between different protection equipments

This dedicated interface deals with data exchanges between distinct devices of the same supplier.

Examples are the link between the parts of differential protection of a double line or of busbars. In those cases the flow of information is of the same nature as for a teleprotection equipment and can be wide band. The interface will also be the same as in b) or c).

5.2. Interfaces to the telecommunication system

Whether dealing with teleprotection (cf 5.1.d) or with telecontrol (cf 5.1.e) it is necessary to make some classification in function of the signals to be transmitted and of the telecommunication medium at disposal.
Transmitted signals are always digital for telecontrol purpose but can be analogue or digital for teleprotection use.

Analogue transmissions

Narrow band (i.e. voice band) transmissions are outside the scope of this work and have already been dealt with in CIGRE WG 34/35-05 publication on "Protection systems using telecommunication".
Wideband analog transmissions (FM, PM etc...) are only possible on a dedicated telecommunication medium or on a primary group of a FDM (frequency division multiplex) system.
As the modulation procedure is normally defined by the teleprotection supplier and as it is unlikely to be used for new developments, it shall not be emphasized here.

Digital transmissions

Following and extending CCITT classification, digital transmissions can be subdivised into 6 groups :

1 Transmission on analogue circuits
  1 a PSTN (Public switched telephone network) : CCITT-V recommendation
  1 b private or leased circuits " "

2 Transmission on digital circuits
  2 a CSDN (Circuit switched data network) : CCITT-X recomm.
  2 b PSDN (Packet switched data network) : CCITT-X "
  2 c TDM (Time division multiplexed network) : CCITT-G "
  2 d ISDN (Integrated services digital network) : CCITT-I "

5.2.1 Interface for Supervision/Management

As stated in 5.1.e the interface between protection equipment and telecommunication equipment is normally a serial port.
The most popular one is standardized by CCITT V.24 recommendation for the interchange circuits definition and by CCITT V.28 recommendation for the electrical characteristics (or their EIA equivalent RS.232 c or d).
Other CCITT standards like V.24/V.10 (EIA RS-449/RS-423 A), V.24/V.11 (EIA RS-449/RS-422 A) or V.35 can also be used but are less recommended except for special applications.
A comparison of those standards is given in table 5.2.
More details about the electrical characteristics of this interface can be found in IEC standard 870-3 on "Telecontrol equipment and systems - Part 3 : Interfaces".

Other characteristics of this interface will depend of the chosen telecommunication medium as described in appendix 2.

5.2.2 Interface for teleprotection

Contrary to telecontrol, teleprotection should not interface switched telecommunication networks. Transmission will normally be done on permanent dedicated circuits which can be analog or digital. However digital networks are sometimes able to make end to end connexions following non permanent physical paths but with overall transmission delays and switching time staying within specific limits. Teleprotection protocols should be able to work in conjunction with such "virtual permanent circuits" and some ISDN networks are likely to offer them.

1°) Private or leased analogue circuits

High speed transmissions from 32 kbit/s up to 144 kbit/s require broadband modems to interface either a primary FDM group (60 - 108 kHz) or pilot wires meeting requirements H.14 of the CCITT.
Other proprietary base band or carrier modulated modems can be used on limited range pilot wires (10 - 20 km).

Main interface standards

The main interfaces for those modems are the CCITT V.35 and V.36 interfaces.
This latter is very near the EIA equivalent specification RS-449.
The electrical caracteristics of V.36 (RS-449) are specified by the recommendations V.11 (RS-422).
The list of definition for the junction circuit used in those interfaces is given by the V.24 recommendation. However for a teleprotection application the telecommunication link is permanent and no handshaking signals are to be exchanged with the modem, with the consequence that very few of the junction circuits defined in V.24 are actually used.

The connector required for the V.35 interface is the ISO 2593 (34 pins) connector.
The connector required for the V.36 (RS-449) interface is the ISO 4902 (37 pins) connector. However as the multiple handshaking signals of this interface are not used, ISO 4903 (15 pins) connector can also be used.

Other interfaces

The already mentioned CCITT V.24/V.28 (EIA RS-232) interface is normally designed for data speed up to 19 200 bit/s but many manufacturers propose it for higher speeds up to 64 kbit/s. Its main disadvantage is to be an unbalanced interface only usable for very short distances between equipments (< 15 m).

The CCITT V.10 also known as X.26 (EIA RS-423) interface is an intermediate standard between the V.28 and the V.11 in this sense that the transmitter uses a dissymmetrical driver whereas the receiver is a symetrical circuit.
For all those reasons V.11 interface should always be prefered to V.28 or V.10 mainly when the equipments are not located in the same cabinet or when a risk of disturbances exists (cf. table 5.2).

2°) Digital circuits

Digital circuits are usually built up by connecting individual links together in a digital network ; this network is almost always based on a TDM (time division multiplexed) structure leading to standard fixed bit rates from basic 64 kbit/s channels. Owing to the pulse coded modulated (PCM) system, voice, data and signalling signals can be multiplexed together. The CCITT standards adopted by most European systems recommend multiplexing 64 kbit/s channels into 2, 8, 34 140 Mbit/s and higher rate bit streams. The standards adopted by North America and Japan are slightly different. The primary multiplexer operates at 1.5 Mbit/s. A basic channel, though also of 64 kbit/s normally only supports 56 kbit/s data transmission.

Interface standards

Interface to the TDM network can be the already mentioned V.11 or V.35 standards but, as the transmission is done on a permanent, non switched circuit, preference goes to a direct access to the multiplexer equipment by means of a CCITT G.703 interface which allows the following bit rates :

64, 2048, 8448, 34368 kbit/s (Europa, other countries)
64, 1544, 6312, 44736 kbit/s (USA, Canada)
64, 1544, 6312, 32064 kbit/s (Japan)

At the basic bit rate of 64 kbit/s three variants co-exist. They result from different historical approaches taken towards data synchronisation. For high speed communication (> 19200 bit/s), data are generally transmitted synchronously, i.e. a timing signal is generated (normally by the telecommunication medium) to regulate when data can be transmitted and when received data should be read. The G.703 recommendation specifies three types of timing arrangements (fig 5.3).

Centralised "clock interface", i.e. all timing signals are supplied from a centralised clock.
Contra-directional interface, i.e. timing signals associated with both directions of transmission are originated from the multiplexer.
Co-directional interface, i.e. timing and data signals are transmitted in the same direction.
The centralised clock interface is only to be used in a network were the synchronisation is made by an external clock channel. It should not be taken into consideration for new developments.
The contra-directional interface makes use of four symmetrical pairs : one for data signals and one for clock signals in each direction.
An AMI (Alternate Mark Inversion) code at 64 kbaud is used for the data signals. This is a three levels code in which zeroes are transmitted without change and ones are transmitted alternately as positive or negative marks as shown on fig 4. The advantages of this coding scheme are that no DC component is transmitted and no polarity is to be respected; it therefore allows isolating transformers or AC amplifiers to be used in the communication path. Moreover some error monitoring can be achieved on the data stream by checking for code violations.

The clock signals involve a 64 kHz and a 8 kHz information and are also AMI coded though at twice the data baudrate i.e. at 128 kbaud. The co-directional interface is the latest and more popular one as it makes use of only one symmetrical pair by direction. Indeed clock and data signals are incorporated in the same ternary bit pattern which is for this reason more complex than in the contra-directional function and has a line speed of 256 kbaud instead of 128 kbaud.

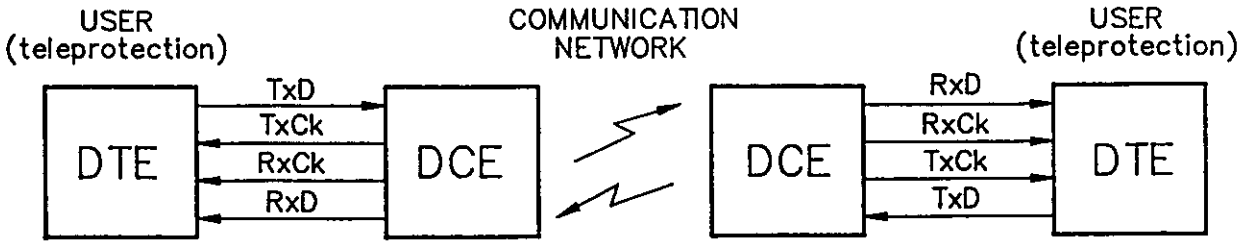

USER
(teleprotection)
COMMUNICATION
NETWORK
USER
(teleprotection)
DTE
TxD
TxCk
RxCk
RxD
DCE
DCE
RxD
RxCk
TxCk
TxD
DTE

FIG. 5.2

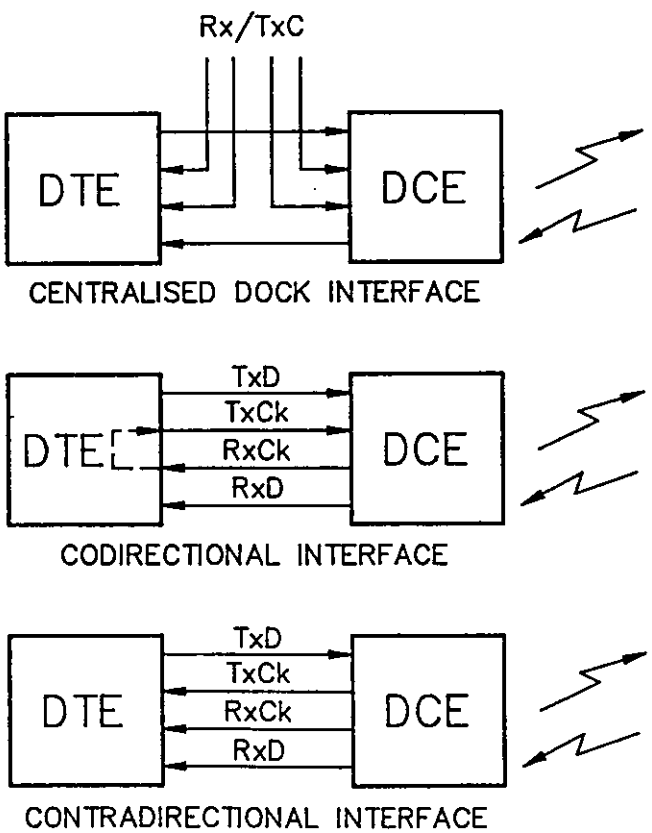
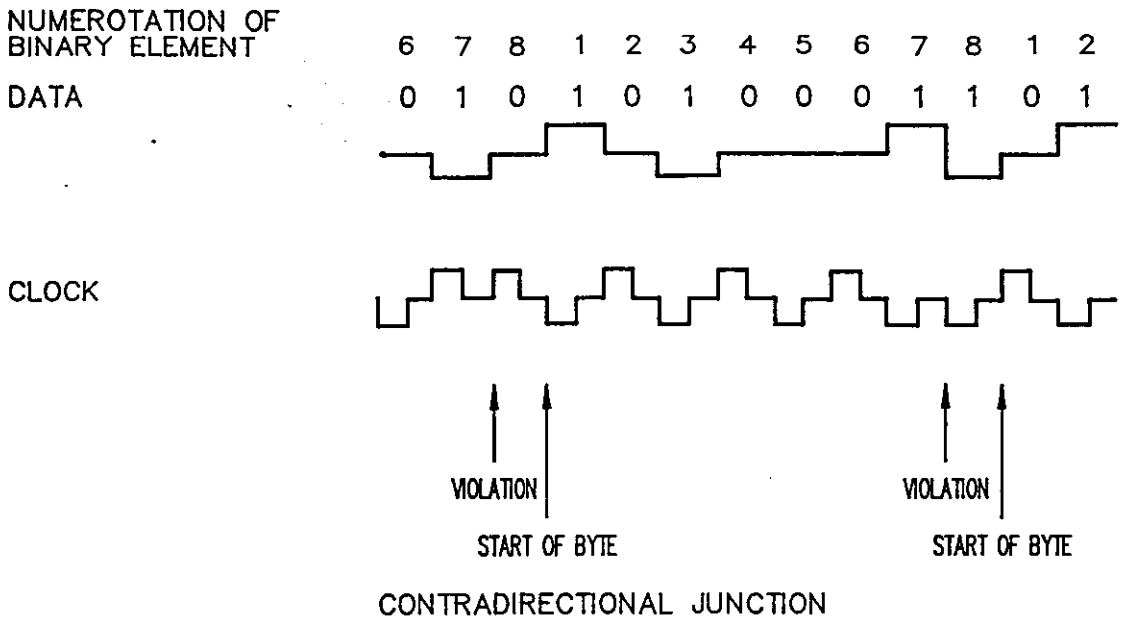
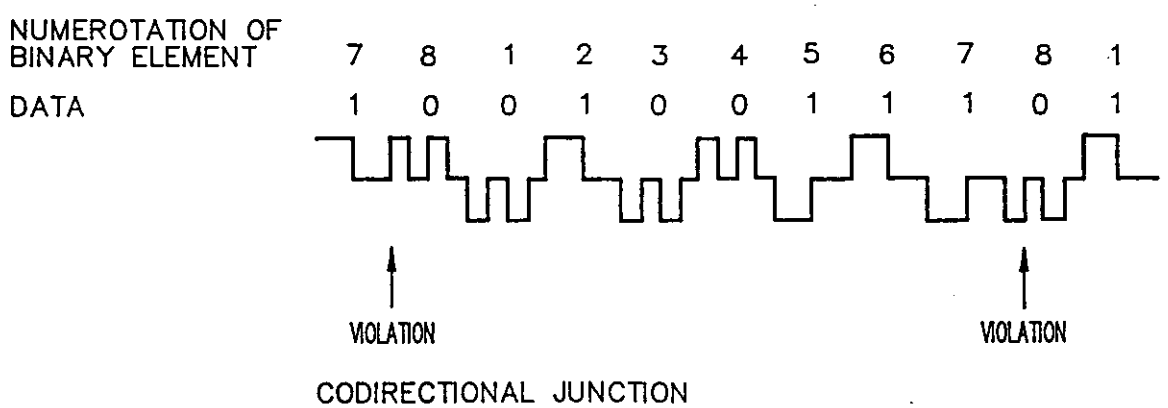

Rx/TxC
DTE
DCE
CENTRALISED DOCK INTERFACE
TxD
TxCk
RxCk
RxD
DTE
DCE
CODIRECTIONAL INTERFACE
TxD
TxCk
RxCk
RxD
DTE
DCE
CONTRADIRECTIONAL INTERFACE

FIG. 5.3



CONTRADIRECTIONAL JUNCTION



CODIRECTIONAL JUNCTION

FIG. 5.4

Choise between co and contra-directional interface

As stated hereabove the co-directional interface is the latest and most logical one : data and clock are transmitted together on the same twisted pair in what is called a "clock transparent pattern".

The only drawback of this interface is that the bandwidth of the signal is broader than for the contra-directional one and so the maximum distance between equipments can be somewhat smaller. Sensitivity to electromagnetic interference is therefore also slightly higher. At the other side there is no need for phase adjustment between data and clock as in the contra-directional scheme where an elastic buffer can sometimes be necessary for long distances between equipments.
A summary of the main difference between co and contra-directional is given in table 5.1.

	Co-directional	Contra-directional
number of symmetrical pairs	2	4
bit rate	64 kbit/s	64 kbit/s
baud rate	256 kbaud	128 kbaud
max. allowed attenuation (*)		
at 32 kHz	/	3 dB
at 128 kHz	3 dB	/
max. recommended distance (*)	/	450 m
typical usable distance (**)		
with 0,4 mm wire	500 m	400-700 m
with 1 mm wire	1400 m	2000-4000 m (***)

Table 5.1
CCITT G.703 64 kbit/s interfaces

(*) according to CCITT
(**) following measurements made on different equipments
(***) with elastic buffer
(/) No CCITT recommandation

5.3. Communication subsystem between teleprotection and telecommunication equipment

As follows from § 5.1. c) and d) when the communication subsystem is dedicated to the protection function it can be a metallic link (pair cable or coax-cable) or an optical link.

5.3.1 Metallic link

Transmission on metallic wires have to cope with disturbance problems (cf. § 5.4) diaphony, attenuation and characteristic impedance.

a) Coax cables

Coax cables have a good immunity to high frequency disturbances but a very low immunity to low frequency disturbances. Moreover their low characteristic impedance doesn't match the majority of the digital interfaces mentioned in 5.2. They can for those reasons only be taken into consideration as extension of a dedicated telecommunication coax cable for which no interface specification has to be defined.

b) Symmetrical pair cables

Cable with symmetrical pairs, when they are correctly screened (cf. § 5.4.) can provide an economic solution to the interconnexion between telecommunication and teleprotection equipment.
Two possibilities exist to make this interconnexion

1° direct junction of the interfaces
2° use of a network terminating unit (NTU) for matching the cable.

Direct junction

This means that the teleprotection interface is the same as the telecommunication interface and that the two parts of this interface are only remote from each other.
Considering the three main interfaces mentionned in § 5.2. it can be stated that the V.35 is not recommended for such an application because the signals, though symmetrical, have a too low amplitude (0,55 V) which limits the noise immunity.
The V.11 interface (also V.36, X.21, X.27, RS-422, RS-449) has also symmetrical differential interchange circuits with a maximum open circuit signal level of 6 V and is well suitable for this application if it is provided with a sufficient galvanic isolation (cf. § 5.4.)
It is recommended to use an additional load resistance (≈ 120 Ω) at the receiver side in order to match the characteristic impedance of the interconnexion cable.
The G.703 interface works also with differential signals but with smaller levels, i.e. : 1 V. Most time the interfaces are provided with 1 kV pulse transformer. For higher immunity levels additional transformers have to be used.
Table 5.2 resumes the main characteristics of those interfaces.

Network terminating unit

When the interconnexion cable is to long for the chosen interface a NTU has to be used. It can be an interface converter (see § 5.3.3) a remote multiplexer or a short range base band modem.

Baseband modems à 64 kbit/s allows bidirectional transmissions on 4 wires telephone links of 1 mm diameter, up to about 15 km.

5.3.2 Optical link

The main advantage of the optical fibre is of course to be immune to electromagnetic interferences. However it needs optical modems and remains more expensive than classical wiring. At the protection side the modem can be incorporated within the teleprotection equipment or physically separated from it.

Characteristics	CCITT Recommendation V.28	V.10	V.35	V.11	G.703
other equiv CCITT Rec EIA Rec	X20bis, X21bis RS232	X26, X20 RS423/449		X 27,X21,V36 RS422/449	
typical signal level (V) (with load)	12	5	0,55	3	1
circuit	unbalanced	unbalanced	balanced	balanced	balanced
polarity to be respected	/	/	yes	yes	no
connector	ISO 2110 25 pin	ISO 4902(4903) 37 pin (or 15)	ISO 2593 34 pin	ISO 4902(4903) 37 pin (or 15)	
galvanic isolation provided	no	no	no	no	yes
max recommended distance in function of the speed for 0.5 mm wire diameter	15 m (20 kbit/s) (NIU)	100 m (10 kbit/s) 10 m (1 kbit/s)	/ (NIU)	1000 m (100 kbit/s) 10 m(10Mbit/s)	450 m (64 kbit/s)
minimum number of wires for a permanent circuit (no handshaking)	4	6	6	6	4 (co) 8 (contra)
recommended for teleprotec- tion use	up to 20 kbit/s (*)	(*)	(*)	yes	yes
recommended for telecontrol use	yes (*)	special application (*)	special application (*)	special application	no
(*)	only for very short distance between equipments				

Table 5.2 : Main CCITT data interfaces

In this latter case it has exactly the same function as the NTU and can make use of all the interfaces mentioned hereabove. This interface can then be different for the protection side than for the telecommunication side; for instance a V.11 or a V.35 interfaces at one side and a G.703 interface at the other side.
One problem with optical fibres is the lack of standards in these areas. A lot of fibre diameters and connector types coexist. It must be remembered that optical fibres can be of two types : the multimode type (step index or now more often encountered graded index) and the monomode type. Both are characterised by their core and cladding diameters given in µm. The smaller the core diameter the more difficult it is to inject sufficient light into the fibre but the smaller also the attenuation is. So it remain always a compromise between cost of terminals and cost of fibre depending of the range to be covered. When an optical cable is used only inside the substation or for short distances between substations, attenuation problems are not of great importance and multimode optical fibre requiring low cost terminal equipments and connectors can be used as the 50/125 (cf. CCITT G.651 and CEI 793-2) graded index fibre and the well known SMA and ST connectors.
Other standards are also wide spread : like the 62.5/125, 85/125 and 100/140 fibres.

Monomode fibres though cheaper than graded index fibres have a core diameter of only 8 to 10 µm (ex : 8/125). So, they are less recommended for short distances because they require more expensive terminal equipments.

Covered distances can be derived from the simplified formula :

$$l\ (km) = \frac{A}{a_l + a_s/2}$$

where - A is the allowable attenuation between transmitter and receiver (A ranges typically from 10 to 40 dB) (*)

- a_l is the attenuation by km

- a_s is the splicing attenuation assuming one splice every 2 km (usually less than 0.1 dB).

Typical figures concerning the most encountered fibre standards are given in the following table :

(*) a margin of 5 to 6 dB should be added to A in order to take account of the aging of the material.

Fibre type (µm)	attenuation (dB/km at :) (*) 850 mm	1300 mm	1550 mm	l (km at) (*) 850	1300	1550	bandwidth (MHz.km)
step index							>10
200/...	.../10			.../2			
graded index				5/...	.../80		100-1500
50/125	2.5/4	0.5/1.5					
62.5/125	3/6	0.7/2					
monomode							>10.000
8-10/125		0.4/0.5	0.25/0.4		100/...	.../200	

As can be deduced from those figures, bandwidth is not very relevant in the choice of an optical fibre for low or medium speed applications like teleprotections.
Plastic fibres are much cheaper than their silica equivalent but offer an attenuation which is at least one hundred time higher (typically 140 to 180 dB/km at 650 nm) so they can only be used for short distances up to 50 m. Moreover their life expectancy is not yet well known.

5.3.3 Interface converter

When making the connexion between a teleprotection equipment and a telecommunication circuit it happens sometimes that both interfaces are of different kind or that the use of a NTU or optical modem makes it necessary to adapt one interface to another.
This conversion can give rise to different problems which, like most interface problems are usually handled neither by the telecommunication engineer nor by the user (i.e. the protection engineer) !
Those problems take their origin in the necessity to specify, as well for the data signals as for the clocking signals, who is the transmitter and who is the receiver. This is easy when only two equipments are used but becomes less evident when the circuits involves a whole chain of equipments. The classical base reference for a telecommunication circuit is given at fig. 5.2.
The user (in this context the teleprotection equipment) is known as Data Terminal Equipment (DTE); the equipment giving access to the communication network is known as Data Commmunication Equipment (DCE). When data are exchanged between DTE and DCE, the direction from DTE to DCE is refered as transmitted Data Circuit (TxD) and the opposite direction as Received Data Circuit (RxD). The associated clocking circuits have the same labels (Tranmitted Clock : TxC and Received clock RxC) regardless of the actual transmission direction of these signals.

(*) (typical/maximum)

Except for the G.703 interface which can be co or contradirectional (cf. fig. 5.3) almost all other interfaces are of the contradirectional type; this means that the clocking signals are always issued from the DCE and transmitted to the DTE.
Refering to CCITT - V.24 (EIA - RS-232) recommendation, each circuit between DTE and DCE has received a single number regardless of the chosen interface (and thus the pin allocation of the connector) and the type of this interfaces i.e. DTE (DCE oriented) or DCE (DTE orentied).

The main circuits used in synchronous transmissions are the following :

CCITT nr.	Label	definition	flow direction
103	TxD	Transmitted Data	to DCE
104	RxD	Received Data	from DCE
113	ExC	External transmitter clock	to DCE
114	TxC	Transmitter clock	from DCE
115	RxC	Receiver clock	from DCE

Common return, control or handshaking signals, though normally not used for permanent links have sometimes to be (locally) provided for correct working of some devices. The most important circuits are :

102	Gnd	Ground or common return	
105	RTS	Request to Send	to DCE
106	CTS (RFS)	Clear to Send (Ready for Sending)	from DCE
107	DSR	Data Set Ready	from DCE
108	DTS	Data Terminal Ready	to DCE
109	DCD	Data Carrier Detected	from DCE

For most applications however only three circuits are required : 103 (TxD), 104 (RxD) and 113, 114 or 115 (clock). This means that only three symmetrical pairs should be enough to make a permanent wide band interface. Those three circuits are even reduced to two with the G.703 codirectional interface.
It is also of common use to provide the DCE with a female connector and the DTE with an interface cable and a male connector or with a female connector; in this latter case an interface cable with two male connectors has to be provided.

Clocking problems

A first problem occurs when a contradirectional DTE (V.11, V.35...) has to interface a codirectional DCE (G.703). In this configuration the interface converter is charged to send back the clocking signals to the DCE and to build up two clocking signals (circuit 114 and 115) for the DTE.
When more than one interface converter is used between DTE and DCE (fig. 5.5) the co to contradirectional conversion is made in the last converter interfacing the DTE.

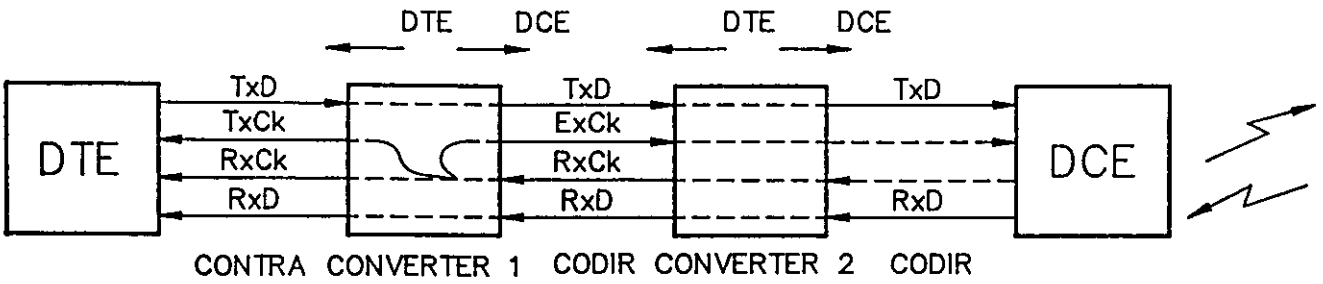

DTE
DCE
DTE
DCE
DTE
TxD
TxCk
RxCk
RxD
TxD
ExCk
RxCk
RxD
TxD
RxD
DCE
CONTRA CONVERTER 1
CODIR CONVERTER 2
CODIR

FIG. 5.5

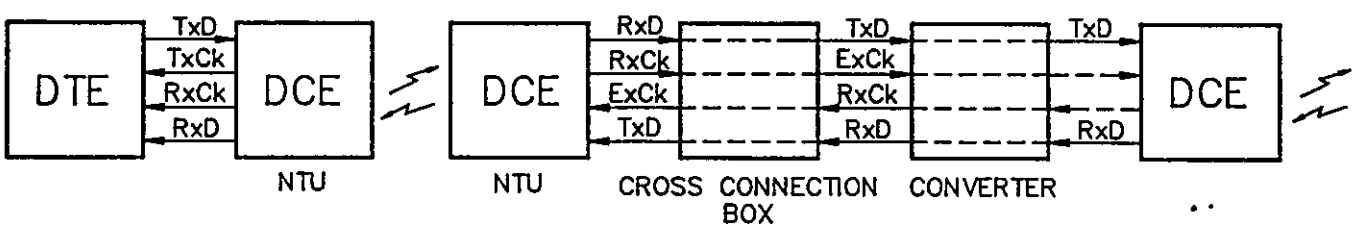

DTE
TxD
TxCk
RxCk
RxD
DCE
NTU
DCE
NTU
RxD
RxCk
ExCk
TxD
TxD
ExCk
RxCk
RxD
TxD
RxD
DCE
CROSS CONNECTION BOX
CONVERTER

FIG. 5.6

Each intermediate converter has a DCE interface (for connection to a DTE or DTE oriented) and a DTE interface (for connection to a DCE or DCE oriented). The clock signal coming from the DCE (with the received data) has to be returned to it via the external transmitter clock circuit 113. This can usually be made by removing strap connexions inside the interface converter.
A second problem is encountered when two NTU's or optical modems are used (fig. 5.6). Those NTU's are normally considered as DCE because the medium between them should be a telecommunication circuit. So it appears that two DCE interfaces (i.e. DTE oriented) are facing each other. This situation requires, beside the possible use of an interface converter, an extra junction box (or cable) which makes a cross connexion between the following circuits :

103 (RxD) - 104 (TxD)

113 (ExC) - 115 (RxC)

Control signals when used can be cross connected as follows

105 (RTS) - 106 (CTS)

or 105 (RTS) - 109 (DCD)

107 (DSR) - 108 (DTR)

If instead of two DCE facing each other it happens that two DTE have to be directly interconnected the same kind of cross connexion box can be used with the following interchange circuits :

103 (RxD) - 104 (TxD)

113 (ExC) - 117 (TxC)

105 (RTS) } - 109 (DCD)

106 (CTS) }

Such an interconnexion box - usually known as "Null Modem" can be helpful if an interface converter makes the good conversion but with the wrong interface type; for instance V.35 (DCE) to V.11 (DTE) instead of V.35 (DTE) to V.11 (DCE).
It is also of great importance to avoid the confusion between both opposite concepts :

DTE (or DCE) type interface/port/connecter, i.e. the equipment handles data as a DTE (or respectively a DCE)

and

DTE (or DCE) oriented interface/port/connector, i.e. the equipment is destinated to interface a DTE (or respectively a DCE)

Most time when the label DTE (DCE) is written on a connector it means DTE (DCE) oriented, so this port should be of the DCE (DTE) type !

5.4. Electromagnetic compatibility

Transmissions inside high voltage substations have to comply with severe disturbances due mainly to disconnector activity, lightnings and fault currents.
Disconnector activity is responsible of high transient electromagnetic fields whose frequency spectrum extends beyond 1 MHz and sometimes beyond 10 MHz for small shielded substations.
Lightning produces also high electromagnetic fields but it mainly causes high potential rises with destructive effects.
Faults are usually responsible for low frequency potential rises.
All those phenomena have been studied in detail by CIGRE SC 36.
IEC have established immunity levels and tests which the protection equipments should withstand.
CCITT has separated standards for telecommunication equipments.

Information about the specific insulation and immunity tests can be found in [1].
It is not the purpose of this document to reexamine those questions but well to emphasize some specific points which concern wide band transmissions within substations.

As stated in paragraph 5.3. most of these transmissions are made by symmetrical pair cables or by optical fibres. Unless the optical fibre starts directly from the teleprotection equipment and is prolonged by an optical telecommunication cable up to the remote teleprotection equipment, optical/electrical converter have to be used in order to interface the different equipments (DCE and DTE).
Those interfaces require classical wiring which like symmetrical pair cables has to comply with EMC requirements. In that context, the only but important existing difference between mixed optical/metallic wiring and classical wiring is the length of influence of the metallic part.

Indeed, it is an established fact that nor the teleprotection interfaces nor the telecommunication interfaces can stand the severe common mode transient interferences encountered in HV substations and specified by the IEC tests without the existence of a very good cabling system correctly screended and earthed.
Those EMC requirements already existed with classical low speed (i.e. voice band) transmission. However they are by far more acute with wide band communications. As an example, the G.703 co-directional 64 kbit/s signal occupies a frequency bandwidth of nearly 1 MHz at -30 dB with 90 % of the spectral power extending beyond 200 kHz. This bandwidth is practically 200 times larger than a classical FSK or PSK voice band signal (modems up to 19 kbit/s). This means that those wide band signals are also much more susceptible to electromagnetic interferences. It is particularly relevant, with this respect, to compare the CCITT recommendations about EMC requirement and testing method with those formulated by IEC :
IEC 801-4 and 255-4 specify immunity test levels of at least 1 kV (longitudinal).
IEC 834-2 dealing with test procedures for analogue protections refers to IEC 255-4 but explicitely excludes the 64 kbit/s interfaces !

As for CCITT, recommendation I.431 concerning the G.703 2 Mbit/s interface specifies a maximum tolerable longitudinal voltage of only 2 Vrms in the range 10 Hz - 30 MHz (*) !
The important discrepancy between those test levels is partly due to the fact that some recommendations don't take into account the wiring conditions (ex CCITT I.431) whilst other do (ex IEC 801-4). On the other hand wideband digital interfaces have originately been designed for the "PTT world" of which the environmental conditions are usually less stringent than in the "electrical world".
Nevertheless, the only way to make compatible such contradictory exigencies is to make use of screened cables with very low high frequency transfer impedance (lead sheath, braided-wires shield with high coverage factor, double wound metallic foil etc ...).

A great attention has also to be paid to the earthing method of those screens. Best results are obtained when the screens are directly connected to the equipment cabinets.
As the earthing network of most HV substation is generally of good quality it can be taken as common rule to recommend the earthing of the screens at each extremity cf [2]. Exceptions to this rule, in the context of wide band communications should be taken as low as possible.

(*) NB. CCITT recommendation K.20 deals with higher applied voltages but it cannot be considered as an immunity test as the equipment is not required to operate correctly during the test.

Appendix 1

The enlarged Shannon's theorem

It is not the purpose of this paragraph to discourse about information theory but only to highlight some important conclusions of this theory which has a lot of repercussions on the subject of this document.

When one tries to evaluate and compare the performances of different digital transmission systems it is necessary first to split them into systems with bandwidth limited channels (sometimes called analogue channels) and non bandwidth limited channels (sometimes called digital channels).
The first category needs some digital to analogue conversion in order to suit the characteristics of the transmission channel. This is often done by means of a modulation procedure like amplitude modulation (AM), frequency shift keying (FSK), phase shift keying (PSK) and, for very large bandwidth systems : pseudonoise (PN) or frequency hopping (FH).
Examples of telecommunication mediums which need some modulation technics are 4 kHz voice band channels or digital radio links.
The second category is that of baseband signalling on (relatively) wide band mediums like fibres optic, short distance metallic links (CCITT - V.24 - V.11 - G.703), local area networks (LAN)
After having made this discrimination it becomes possible to compare the systems together by putting on a diagram the bit error rate (BER) of the transmission in function of the disturbance level, the signal to noise ratio, or the attenuation (fig. A1). (*) (i.e. digital signal on analogue channel).
For the first category of systems the more sophisticated the modulation scheme is the better the system is but the more sensitive the system becomes towards noise.
For full digital systems (i.e. digital signal on digital channel) this sensitivity is still higher.
A step further is achieved in the comparison by taking into account the used protocol or more precisely the amount of redundancy included in the transmitted information (i.e. frame check sequences, repetition procedures etc.)
This leads to a second diagram giving the residual error rate (RER) of the transmission in function of the (BER) (fig. A2)
A better evaluation of the overall performance of the protocol is achieved by dividing the RER by the transmission efficiency (η) (i.e. the amount of correctly received data bits with respect to the total number of bits sent) as it is irrelevant to have a protocol that allows an error free transmission if the net information transmission rate is equal or near to zero (fig. A3)
By grouping both diagrams together on a third one we get a global view of the quality of the communication system with the RER (eventually related to the transmission efficiency) in function of the disturbance level (fig. A4).
On this latter diagram a vertical line has been drawn.
It corresponds to the behaviour of a "perfect" system approaching the limit of Shannon's theorem.
As already mentionned in § 4.1. Shannon theorem tell us that it is possible to transmit- with zero error - a rate of information R on a noisy channel of capacity $C = B \log_2 (1 + S/N)$ (bit/s), if $R \leq C$
(with B the bandwidth, S the signal power and N the noise power as already defined in section 4.1.)
The important features of that theorem is that the transmission may be accomplished without any error in the presence of noise but also that if $R > C$ or, if the disturbances exceed some predefined threshold, the probability of residual error becomes a certitude !

In other words systems approaching Shannon's limit will have a kind of go-no go behaviour.
This is a general theorem extending far beyond the telecommunication field and which can be resumed as follow :
"High performance systems : when they work, they work well, but when they fail they fail totally !
Or more simply :
The better the performances of system are, the worse they are when the system fails.

(*) All the graphics of this appendix are given as qualitative illustration and are intentionally simplified.

Schematic Representation of Telecommunication Performances.

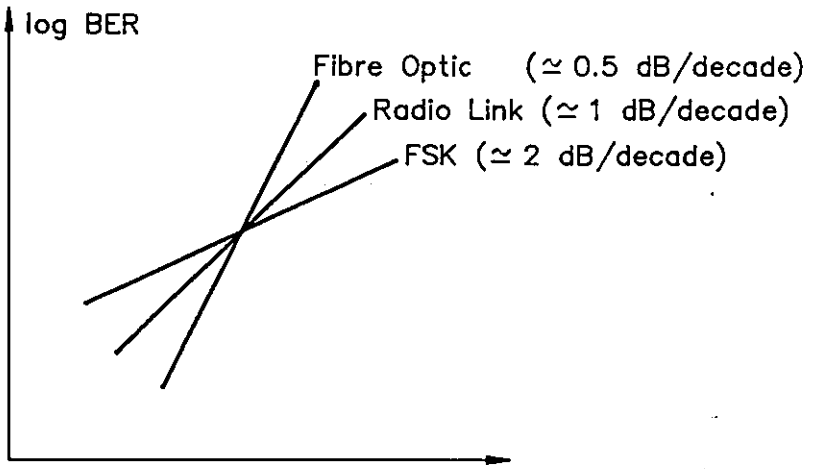


FIG. A1

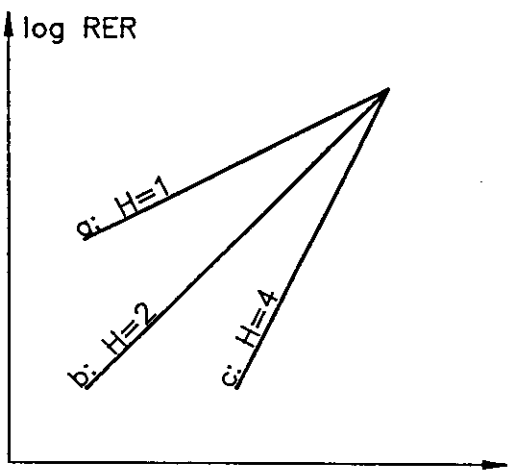


FIG. A2

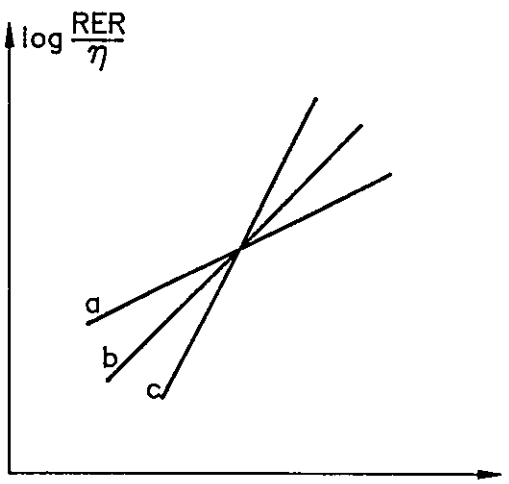


FIG. A3

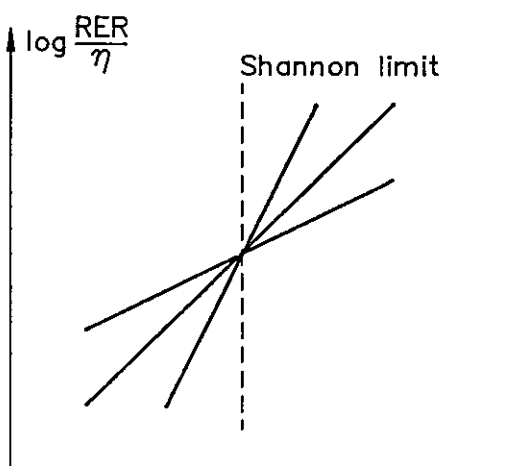


FIG. A4

Appendix 2

Telecommunication facilities for low speed digital transmissions

1°) PSTN

Transmission on the classical public telephone network will normally be done by modem. A wide variety of models exists ranging from the simple 300 bit/s equipment to the very sophisticated 9600 bit/s (full duplex) or 14 400 bit/s (half duplex) versions; all meeting CCITT V recommendations (V.21 to V.33) and sometimes offering special features like automatic speed selection, error correction and data compression.
Special procedures can be incorporated in the software of the equipments (protection and modem) in order to allow for the automatic establishment of the communication (auto-dialling/answering). Such a procedure is defined by CCITT V.25 bis recommendation. Another equivalent procedure called HAYES (T.M.), though not officially standardised has the advantage of being more widespread.
When more than one equipment has to be remotely controlled it is possible to install between the modem and the equipments a multiport programmable switch able to make an automatic connection to the selected port. Such a switch can usually recognize a pass-word or even hook on the line and recall at an nummer stored in memory.

2°) Private or leased analogue circuits

When a permanent voice graded circuit is available, possibility exists to use modems as on the PSTN. There is however no need for auto dialling and low cost or industrial modems can also be used on private circuits. Those modems can, of course, be FDM (frequency division) multiplexed according to CCITT R.31, R.37 and R.38 recommendation or other proprietary standards.
Use of TDM submultiplexers in association with a base band modem can sometimes be advised when a sufficient bandwith is available (metallic pairs, primary FDM group).

3°) CSDN

Circuit switched data network is the data equivalent of the PSTN.
Unlike this latter, CSDN is always a digital network usually based on a TDM hierarchy (cf § 6.2.2 - 2°). Like PSTN it is a switched network which means that the communication links and the transmission delays across the network are not permanent.
CCITT X.1 to X.21 recommendations deal with services, facilities, terminal equipments and interfaces for accessing this network. The most important among them is X.21 "General purpose interface between data terminal and data circuit terminating equipment for synchronous operation on Public Data Network".
The electrical characteristics of this interface are defined by the V.11 specifications (also known as X.27). Connector meets the 15 pin ISO 4903 standard.

4°) PSDN

Packet switched data networks are digital networks (public or private) that maintain high average utilization of transmission facilities by combining the traffic of many users, whose peaks do not occur simultaneously. This is done by using many geographically distributed switching centers, each of which dynamically routes traffic according to the current status of the network. Therefore messages are subdivided within the network into short packets whose maximum length is fixed. Each packet is sent individually through the network according to a special procedure and the whole message is then restored in the last node.
This special procedure is standardized by CCITT X.25 recommendation.
Low speed access (up to 19 200 bit/s) to an X.25 network is usually done by a DCE (data communication equipment) called PAD (Packet Assembler Desassembler) which supports the X.25 protocol and makes it transparent to the user.
As the transmission delay accross an X.25 network is not constant and quite high (typically 100 to 300 ms), PSDN can never be a suitable communication medium for teleprotection use but only for telecontrol.

5°) TDM networks

Time division multiplexed circuits (private or public) are discussed in detail in § 5.2.2. They offer the digital equivalent of voice graded circuits, i.e. 64 or 56 kbit/s channels.
Though the possibility exists to directly access those circuits it is recommended for telecontrol purposes to use a TDM submultiplexer that allows for a better utilization of the available transmission capacity.
CCITT R.111, X.50, X.51 and X.52 recommendation defines multiplexing plans for this kind of equipment. Statistical multiplexers are also of interest. They are based on the fact that the different low speed channels connected together are not permanently and simultaneously used, and allow higher individual transmission rate per channel by means of store and forward memories.

6°) ISDN

Integrated services Digital Networks whether public or private, are based on digital exchanges and digital paths which are able to establish end-to-end digital connections simultaneously for voice, data and other services. This implies that the last remaining analog section, i.e. between subscriber and local exchange, also has become digital.
Like CSDN of which it can be considered as an extension ISDN is basically a switched network.
The basic access to the ISDN, called 2 B+D, consists of one 64 kbit/s channel for voice, one 64 kbit/s channel for high speed data and one 16 kbit/s channel for signalling and low speed data. All those channels are multiplexed together in a 144 kbit/s bidirectional stream on the existing pair of copper wire between subscriber and local exchange. All the classical V and X interfaces will of course be supported by ISDN but a lot of other services usually handled outside the telecommunication network will now be integrated in it. Examples are : data bases, filing or archiving, data integrity, security and authentification etc ...

Appendix 3

Glossary

Analog signal 870-1-3

Signal in the form of a continuously variable value.

Analogue protection system CIGRE WG34/35-05

A protection system using telecommunication in which analogue power quantities are transmitted from one end of a power line by the telecommunication system either in analogue or digital form for comparison at the other end.
EXAMPLE: phase comparison protection system, longitudinal differential protection system.

Availability 870-1-3 (IEV 448)

The availability of a unit or system characterizes its ability to perform its required function at any given moment.

Baud CCITT

The unit of modulation rate; the number of bauds is equal to the reciprocal of the duration in seconds of the shortest signal element or of the unit interval in such signal.

Bit

1 A member select from a binary set CCITT
2 Unit of information. The quantity of information in bits is the logarithm to the base 2 of the number of possible states of an event

Channel 870-1-3 (ANSI)

A single path for transmitting electric signals, usually in distinction from other parallel paths.
NOTE - The word "path" is to be interpreted in a broad sense to include separation by frequency division or time division. The term "channel" may signify either a one-way path, providing transmission in one direction only, or a two-way path, providing transmission in two directions.

Circuit ITU

A means of both way communication between two points comprising associated "send" and "receive" channels.

Data integrity 870-4

Data integrity is defined as the unchangeability of an information content between a source and its destination. In telecontrol systems, data integrity concerns the probability of undetected errors resulting in wrong information about actual process states in the monitoring direction or unintended actions in the control direction of the system.

Degraded minutes CCITT G.821

A one minute period where the short term bit error rate, evaluated over one minute, exceeds $1*10^{-6}$.
Note - The one-minute intervals mentioned are derived by removing unavailable time and severely errored seconds from the total time and then consecutively grouping the remaining seconds into blocks of 60. The basic one-second intervals are derived from a fixed time pattern.

Dependability of protection [448-12-07] IEV 448

The probability of not having a failure to operate.

Digital

Discrete variable as opposed to continuous variable. Contrast with analog.

Digital protection CIGRE WG34/35-05

A static protection in which the characteristic response is developed by digital processing of the electrical input quantities.

Directional comparison protection [448-14-20] IEV 448

An overreach protection, usually not a distance protection, using telecommunication in which the directions of current flow, or changes in current flow using a locally derived voltage or current as a reference, are compared at each end of the protected section.

Distance protection [448-14-01] IEV 448

A protection the operation and selectivity of which depend on local measurement of parameters from which the equivalent distance to the fault is evaluated by comparing with zone settings.

Errored seconds CCITT G.821

A one second period that contains one or more errors.

Frequency division multiplex [55-15-050] IEV 55

A multiplex system in which the available transmission frequency range is divided into narrow bands, each used for a separate channel.

Hamming distance 870-1-3

The number of positions in which two code words of the same length differ from each other.

Information transfer efficiency
(in telecontrol) [371-08-12] IEV 371 (870-5-1)

The ratio of the information content of a message transferred from a data source and accepted as valid by a data sink to the total number of bits expended for the massage transfer.

Interface (870-1-3)

1.- A shared boundary defined by common physical interconnection characteristics, signal characteristics, and meaning of interchanged signals.
2.- The equipment which provides this shared boundary.

Jitter CIGRE SC34/35

Short-term variations of the significant instants of a digital signal from their ideal positions in time.

Link 870-1-3

The data transmission facilities among interconnected stations.

Longitudinal differential protection [448-14-16] IEV 448

A protection the operation and selectivity of which depend on the comparison of magnitude or the phase and magnitude of the currents at the ends of the protected section.

Maintainability 870-1-3 (870-4) (271A)

Maintainability is the ability of a system or equipment, under given conditions of use, to be restored to full working order after detection of fault and to be maintained during normal working operation.

Mean time between failures (MTBF) 870-1-3 (271)

For a stated period in the life of a functional unit, the mean value of the periods between consecutive failures of the unit under stated conditions.

Mean time to repair (MTTR) 870-1-3 (ANSI)

The arithmetic average of time required to complete a repair activity.

Network 870-1-3

A number of stations communicating with each other via transmission links.

Non phase segregated protection [448-11-13] IEV 448

A protection, generally unit protection, which is not phase selective.
NOTE - Non phase segregated unit protection generally employs a means of deriving a single phase quantityrepresentative of all three power phases such as a summation transformer or phase sequence network.

Non unit protection [448-11-11] IEV 448

A protection the operation and section selectivity of which are solely dependent on the measurement of electrical quantities at one end of the protected section.
NOTE - The section selectivity of non unit protection may depend upon its setting, particularly with regard to time.

Overall transfer time (in telecontrol) [371-08-15] IEV 371

The time duration by which information is delayed after the actual event in the sending station and until presentation at the receiving station.
NOTE - The overall transfer time includes the delays due to the input peripheral device in the sending station and the corresponding peripheral output device at the receiving station.

Path

Physical communication medium, e.g: radio link, optical fibre...

Phase comparison protection [448-14-17] IEV 448

A protection the operation and selectivity of which depend on the comparison of the phase angle of the currents at each end of the protected section.
NOTE - The principle of this protection is also applied to the comparison of the phase of the voltages.

Phase segregated [448-11-12] IEV 448

Normally used to describe phase selective unit protection.

Protection using a telecommunication system [448-15-01] IEV 448

A protection requiring a communication system between the ends of the protected section.

Protocol 870-1-3 (FED-STD)

The rules for communication system operation that must be followed if communication is to be effected.

Pulse code modulation (PCM) 870-1-3 (FED-STD)

That form of modulation in which the modulation signal is sampled, and the sample quantized and coded, so that each element of information consists of different kinds or numbers of pulses and spaces.

Reliability 870-1-3 (870-4)(271)(IEV448)(ISO)

The ability of a functional unit to perform a required function under stated conditions for a stated period of time.

Residual error rate
(in telecontrol) [371-08-05] IEV 371 (870-1-3)

The ratio of the number of undetected wrong messages to the total number if messages sent.

Security 870-1-3 (870-4)(IEV 448)

The ability of a telecontrol system to avoid placing the controlled system in a potentially dangerous or unstable situation. It applies to the consequences of failures arising out of malfunctions of the equipment and from undetected information errors.

Severely errored seconds CCITT G.821

A one second period where the short term bit error ratio, evaluated over one second, exceeds $1*10^{-3}$.

Signal quality detection [371-04-11] IEV 371

A measurement of the degradation in quality of the received signal, used for error control purposes.
Examples: - Signal to noise ratio falling below a given threshold.
- Pulse length exceeding a specified value.

Telecommunication network

An interconnection of telecommunication facilities consisting of lines and equipment to furnish telecommunication capability.

Teleprotection 870-1-3 (834-1)

An all-embracing expression covering the exchange of monitoring and command information between two or more stations in order to protect operational equipment. Further specific terms are: carrier protection system, microwave protection system, communication-aided distance protection system.

Time division multiplex [55-15-055] IEV 55

A system in which a channel is established in connecting intermittently, generally at regular intervals and by means of an automatic distribution,its terminal equipment to a common channel. Outside the times during which these connections are established, the section of the common channel between the distributors can be utilised in order to establish other similar channels, in turn.

Unit protection [448-11-10] IEV 448

A protection the operation an section selectivity of which are solely dependent on the comparison of electrical quantities at each end of the protected section.

Appendix 4

Bibliography

(1) CIGRE WG 35-02 - Guide for Planning of Power Utility Digital Telecommunication Networks

(2) CIGRE WG 36-04 (to be published) - Installation Guidelines for EMC Improvement of H.V. Open Air Substations.

(3) D Becam e.a.: - Error detection in operating digital systems : influence of error distribution. IEE proceedings Vol 134, Pt F, N° 5 August 1987

(4) American National Standards Institute - IEEE Standard Dictionary of Electrical and Electronic Terms (1984)

(5) CCITT Blue Book - Fascicle III.3 - Rec. G.821

(6) CIGRE SC 34/35 - Teleprotection (1969)

(7) CIGRE WG 34/35-05 - Protection Systems Using Telecommunication (1987)

(8) FED-STD 1037 (1982)

(9) IEC Publication 50(55) - IEV Chapter 55: Telegraphy and Telephony (1970)

(10) IEC Publication 50(271) - IEV Chapter 271,271 A: List of basic terms, definitions and related mathematics for reliability (1974) and Supplement 271 A (1978)

(11) IEC Publication 50(371) - IEV Chapter 371: Telecontrol (1984)

(12) IEC Publication 50(448) - IEV Chapter 448: Power system protection (1990)

(13) IEC Publication 834-1 - Performance and testing of teleprotection equipment of power systems. - Part 1: Narrow-band command systems

(14) IEC Publication 870-1-3 - Telecontrol equipment and systems. - Part 1: General considerations. - Section 3: Glossary (1990)

(15) IEC Publication 870-4 - Telecontrol equipment and systems. - Part 4: Performance requirements (1990)

(16) Standard ISO 2382: Data processing - Vocabulary: -Section 14: Reliability, Maintenance and availability (1978)

Appendix 5

Wideband communication practices in different countries

This appendix is a collection of short write up made by members of the working group and concerning their own country

CIGRE WORKING GROUP 34.05
WIDEBAND COMMUNICATIONS IN THE UNITED KINGDOM

Utilities in the UK depend heavily on PTT for telecommunication facilities. As reviewed in the 1988 CIGRE SC35 telecommunications statistics, about 61% of facilities are rented from the PTT, 20% from private pilot and telephone circuits, 16% from radio and 2% from power line carriers.

Protection trials using microwave radio in the UK so far have been unsatisfactory because of fading problems. Consequently for teleprotection, the choice is only between rented services, PLC, and more recently optical fibre circuits. There are also licensing difficulties with microwave channels and congestion problems with PLC. The decision of the UK PTT to withdraw rented metallic circuits from its services also has an impact on some pilot wire protection and d.c. signalling schemes. It forces utilities to consider alternative protection and signalling schemes.

THE CENTRAL ELECTRICITY GENERATING BOARD

An OPGW trial circuit was first installed in mid-1978 and a full scale system trial on a 21km 400kV line has been in operation at 34Mbps since 1982. The start of the main conductor refurbishment programme in 1985 by CEGB embarked on the first phase of a national optical communication network. The programme planned to refurbish about 100km of OHL circuits per annum and to replace conventional earth wires with OPGW where necessary. Wrap-on optical cables and self supporting optical cables have been on trial and are considered for retrospectively fitted systems. A problem with degradation of cable sheath of self supporting optical cables was reported but was proved to have been resolved in a more recent trial on a 2.2km section of the SSEB's 400kV network.

So far, economic justification of the use of optical cables has been based mainly on protection signalling requirements. The requirements are for a single protection system and one remote intertrip for each power circuit, i.e. four communication circuits in total for a common double circuit line. Although a second protection system is also required for each power circuit the current CEGB policy demands that an alternative communication medium is used. For a double circuit application, the optical cable option is cheaper than PLC up to about 22km. Since projected optical cable costs are lower and that future increase in demand for faster digital services cannot be met by PLC equipment, the economic range of the optical fibre solution will increase.

The current CEGB policy is to install cables containing 4 single mode fibres to carry signals at 140Mbps and at 1300nm wavelength. Some circuit can have optical systems of 8Mbps and 34Mbps if high data capacity is not required. G.703 co-directional interface is used.

A digital current differential relay system using 64kbps data channels has been on trial in a 400kV 3-ended circuit since 1985. Three 275kV

lines with OPGW are to be installed with this new digital current differential relay in 1990. All these lines are less than 20km long and two of them are three-ended.

OTHER UK UTILITIES

Other UK utilities also have carried out trials on optical cables and digital microwave links and some are busy in designing and developing their digital communication trunk networks.

Two trials have been made to apply wideband communications for teleprotection. One of the trials is on current differential protection and the other one on intertripping. Direct optical communications are used in both cases.

Two utilities will start to install a digital communication based current differential relay to their 132kV networks in 1990. The lines are to be provided with optical cables and the route lengths vary from 2km to 11km. Multiplexers at 2Mbps will be used in these lines but 8Mbps and 34Mbps ones may be used in future lines where needed.

TELECOMMUNICATION FOR PROTECTION IN FRANCE

Extract from:

Protection of the high and extra high voltage networks.
General principles - Equipment used - Future perspectives

by: J.L. BERGEROT and C. CORROYER
EDF Transmission Departement

3.4 Protection and telecommunications

As previously indicated, certain protection relays used in the new plans require systems necessitating signal exchanges, some of which are more elaborate and efficient than others, via telecommunication links.

It thus appears of interest to make a summary of the telecommunication means available, their constraints and the evolutions envisaged.

3.4.1 Microwaves

E.D.F. is going to establish a microwave network with the aim of having a safety network enabling the data transmission needs necessary for the following to be satisfied:-

- real time operation,
- high performance protection relays for the 400 kV network.

This network should, in the long run, cover approximately 270 sites: load control centres, major power stations, 400 kV substations and supervisory control substations.

A pilot network covering 20 sites in the Rhône-Alpes region should be put into service between now and the end of 1988. The practical means of extending its use will be decided in the future according to the first results.

3.4.2 Earth wires with incorporated transmission circuits

It has been decided to equip all the new 400 kV lines with earth wires having incorporated optic fibres.

In addition, the replacement of the earth wires of certain existing lines by cables with incorporated optic fibres is also being studied with a view to establishing a supplementary equipment programme.

The new 225 kV lines whose length does not exceed thirty or so kilometres, are equipped with an earth wire with an incorporated coaxial cable, or even a cable with incorporated optic fibres if the number of channels needed justify it.

Finally the other 225 kV lines and the HV lines are not theoretically equipped with such means.

To summarise, the transmission circuits incorporated in earth wires represent a very interesting means, giving performance and independence with regard to the French Telecommunication administration.
They will undergo a serious development in the next few years complementing the microwave network.

3.4.3 Special links rented from the French Telecommunication Administration and PLC

These classic transmission means at present represent nearly 80 % of the length of the safety network transmission circuits.

For their part, the PLC links (power line carriers) represent approximately 30 % of the former. These links constitute a precious means that is nearly saturated.

The aim is to try and use them on a priority basis for protection signals; however this use is limited to the transmission of simple information: protection signalling or wave phase at 50 Hz.

3.4.4

To complete the summary it must be remembered that private communication circuits do exist - particularly pilot cables positioned along power cables -.
These circuits are limited in number; they participate in cable protection.

WIDEBAND COMMUNICATION PRACTICES AND TRENDS IN SPAIN

0. This writeup includes information concerning seven of the biggest utilities in Spain; this including all of the 400 and 220 kV networks, 27.000 km total length, most of the 132 and 66 kV networks and an important part of the medium voltage network.

1. Spanish utilities operate a microwave network composed of 310 links with a total length of 10.500 km.

   Two utilities use microwave circuits for protection purposes (step acceleration and intertripping) in a small number of lines.

   A third one stopped using it after having a bad experience for reasons, not completely clear.

   In general, all utilities will install optical fibre on new lines or on the renewal of old ones. The prevision for the end of 1991 in the 400 and 220 kV network is around 4.000 km of lines furnished with optical fibre. On new lines optical fibre will be OPGW. One utility is considering the wrapping technique over the ground wire on existing lines.

   Over some 66 and 132 kV short lines, typically between generating stations and substations, there are installed line differental protections over pilot wires, coaxial cable or dedicated optical fibre.

2. There is some investigation being developped on teleprotections, phase comparison protections and longitudinal differential protections using 64 kb/s channels. There are four utilities involved. Future policy depends greatly on field test results. The other three utilities still have no definite ideas about the matter.

   One of these projects includes the installation, in mid-1991, of two differential protection systems, of different manufactures, on a 400 kV line of a double circuit, 80 km in length, with observational purposes. There is a digital multiplexed communication link over OPGW at 34 Mb/s between both line end substations, with a signal repeater half way. The communication for protection purposes will use 64 kb/s channels over the optical link. The communi-

cation for management purposes will go over several optical and microwave links to the Engineering Centre.

3. Several utilities will move into wide band communication if

   1) The overall quality of the telecommunication system is better from the protection user's point of view.

   2) The implications of the communication system maintenance on maintenance and management of protection systems are, at most, similar to the existing ones.

DIGITALIZATION OF THE TELECOMMUNICATION NETWORK AT ENEL ITALIAN NATIONAL ELECTRICITY BOARD

The digitalization process of the telecommunication network begun at ENEL with the installation of the 18 GHz radio system, which can provide capacities of 704 or 2048 kbit/s.

On the whole Italian territory ENEL has in operation about 300 hops at the frequency of 18 GHz.

At the moment this band is the only one authorized by the Italian PTT to be operated with digital equipments.

The next step will probably start in 1990 with the substitution of the present FM-FDM 2.3 GHz radio system, allowing 60 channel capacity, with digital equipments operating in the same band. The need to ensure compatibility between the existing 2.3 GHz radio network and the future digital one, implies for the latter a capacity of 2 + 2 Mbit/s with 16 QAM modulation.

ENEL network comprises also a few 34 Mbit/s links on optical cables ad some tenths of 2 Mbit/s carriers on pair cables, mainly used as connections between PABXs.

Beside the above mentioned multichannel radio systems ENEL will use even single channel 64 kbit/s radio systems at the frequency of 440 MHz which will operate with 35 kHz channel spacing.

These single channel systems will substitute the present single channel 300 hops operating in FM at 440 MHz.

The 2.3 GHz radio links are the main bearers in the higher network layers, while the 18 GHz and single channel radio links are mostly used in peripheral connections.

For peripheral links ENEL forecasts the possibility to convert into digital also Power Line Carrier equipments, for which a 64 kbit/s capacity has to be tested.

The ENEL communication network is mainly exploited for operational services and therefore it does not require high capacity except in a small percentage of all the routes. This, together with the presence of bearers capable of 64 kbit/s rate, requires the availability of communication nodes able to route a single 64 kbit/s stream, by means of suitable multiplex equipment.

Each single 64 kbit/s stream can be subdivided into many tributary flows at lower bit rates. Speech signals are coded at 64 kbit/s as well as at lower speeds, like 32 kbit/s ADPCM.

The network nodes which will be introduced into the digital network will operate justification and buffering processes on the elementary bit flows. This will allow plesiochronous operation without slips and avoiding any synchronization.

Dealing with the carried services, about 70 % of the 800 transit telephone exchanges in service at ENEL are already digital PCM, as well as about 60 % of the previously mentioned PABXs.

Channels of the network are also used as connections to the nodes of the packet switching X 25 network ENELPAC, based on more than 150 nodes and serving more than 15000 terminals.

No special separate digital network is envisaged for protection purposes.

Wideband Communication
- Status and Prospects in West Germany -

The German interconnection network consists of eight completely independent power supply utilities. According to this federalistic structure, each utility elaborates its special protection philosophy, with respect to the structure of its own networks and experience.
In case of interconnection links both partners have to coordinate their protection equipment.

Status:

380 kV network

total length:

about 11,000 km

first protection:

distance protection; more than 60 per cent of the line-protection is operated with a communication link:
37 per cent plc, 60 per cent pilot wire, 2 per cent microwave, 1 per cent fibre optics.

mostly used:
permissive intertrip underreaching scheme, acceleration scheme

redundant protection:

about 31 per cent of the network is equipped with a second protection system.

mostly used:
phase-comparison systems, distance protection

communication links:

34 per cent plc, 65 per cent pilot wire, 1 per cent fibre optics.

220 kV network

total length:

about 16,000 km

protection:

distance protection.
about 24 per cent of the line protection is operated with a communication link:
50 per cent plc, 50 per cent pilot wire.

permissive intertrip underreaching scheme only.

110 kV network

total length:

about 33,000 km (only the network belonging to the interconnection partners)

protection:

generally distance protection without communication links.

Characteristics of the communication links

plc :	signal	2.5	4 kHz
	carrier	50	490 kHz
pilot wire:	signal	2.5	4 kHz
	carrier (12-channel system)		
		6	54 kHz
		60	108 kHz
	carrier (60-channel system)		
		12	252 kHz
		312	552 kHz
microwave:	signal	2.5	4 kHz
	carrier	7 GHz	
fibre optic:	850 nm, 1300 nm		
	2.048 MBit/s		
	signal	bit rate 64 kBit/s, 128 kBit/s	

The demand for communication links of high capacity is rising continuously (data transfer, telecontrol, counting etc.). Therefore, the existing links have to be modified or even exchanged (analog -digital, wire - fibre optic etc.). There is a long-term process which will take perhaps five to ten years or even longer. Fibre optic links seem to be preferred because of the inherent advantages.

At the moment there is no need for wideband communication links as far as protection is concerned though one or two utilities think about possibilities and advantages of combining new protection types (digital) with digital communication links.

LABORELEC E2-203.8906/JH/chv

CIGRE WG 34-05

Wide band communications for the Belgian utilities

The main communication system at the power and transmission level is a private time multiplexed network based essentially on radio links.
The whole country is covered by about eighty links reaching directly most of the 380 kV substations, a large number of 150 kV substations, the power plants and the control centers (dispatching).

Those radio links use 8 frequencies in the range of 2,5 to 2,7 GHz.
The total length is 1525 km and the longest link 50 km (mean length about 30 km). Each link has an aggregate digital transmission rate of 8 Mbit/s consisting of four 2048 kbit/s channels each devided into 30 channels at 64 kbit/s according to the CCITT plan.

Most of those 64 kbit/s channels are used in PCM for analog transmissions (i.e. voice, telecontrol by low speed modems up to 1200 bit/s, telecounting, telemetering, teleprotections etc...) A few channels are used at 56 or 64 kbit/s for intercomputer transmissions.
In the near future new differential protections will be installed and use some of those 64 kbit/s paths. Later on ISDN communications will probably occupy some 2Mbit trunks. The radio network is sometimes extended by means of optical fibers (buried or incorporated within earth cables).

Some new optical fiber links are planned. One of them will have a length of 50 km without repeater. Other short length extensions will be based on 22 GHz microwave links.

In addition to this multiplexed network, the earth cables of most of the 380 kV lines are equipped with balanced pairs or quads. This kind of carrier has a bandwidth of about 120 kHz and is used, up to now, by FDM narrow band circuits. However it will probably be used in the future for 64 kbit/s transmissions.

ATTACHMENT

CIGRE WORKING GROUP 34.05

APPLICATION OF WIDE BAND COMMUNICATION CIRCUITS TO PROTECTION - PROSPECTS AND BENEFITS.

WRITE UP ON AUSTRALASIAN EXPERIENCE

There are a few optical fibre installations, 8Mb-15km and single mode 140Mb-7km. One authority has just commissioned an 8Mb-320km and 2Mb-480km digital radio link.

There are plans to extend the 8Mb optical fibre to replace existing analogue radio, to extend the 140Mb installation to 180km and to install 64Kb services over optical fibre and digital radio.

Reasons for moving to wideband communications are cost effectiveness, increased capacity and reliability, immunity to interference and faster operating times. It is perceived that all new broadband installations will be digital.

The prospects are enhanced protection particularly for multi-ended lines, the installation of digital differential protection where installation of metallic pilots was not economic, reduced exposure hazard in comparison with metallic pilots, remote interrogation and adaptive setting change, differential protection for long lines and generally more solutions for difficult applications.

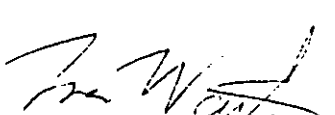
The benefits will be faster and more secure protection with increased selectivity and sensitivity.

No Australian authority rents protection circuits from the telecom authority but there is a limited amount of sharing services with other authorities (Railways and Police).

Australia has adopted the non US 64Kb and multiples hierarchy and the G.703 interface standard. There are varying requirements for bit error rate performance but it has been suggested that equipment should be able to operate down to a bit error rate of 10^{-4}.

Most authorities will use multiplexed circuits but a few indicated a preference for dedicated circuits.

Some reservations were expressed in using wideband digital communications covering the reliability and fading performance of radio links, the interface, the high cost of relaying compared to the reduced communication cost, the inexperience and need for training and the loss of control over the bearer.



Trev Watkins
PROTECTION ENGINEER

S. H. HOROWITZ

Consulting Engineer

3143 Griggsview Court Columbus Ohio 43026 (614) 876-0802

Mr. W. S. Kwong

Control and Communication Dep't.

The General Electric Co. Ltd.

St. Leonards Works

Stafford ST 17 4 LX

England

APPLICATION OF WIDEBAND COMMUNICATION CIRCUITS TO PROTECTION

Dear Wilson, Aug. 28,19898

This is in response to item 6.2 of your draft minutes of the meeting of WG 34-05 on 27-28 June,1989

As you know, there is no United States standard for all utilities; each utility is autonomous with regard to its protection and communication practices. Nevertheless. there are standards regarding the frequencies and bandwidth of the available communication media and there are fairly well defined preferences.

Pilot wire is used primarily on the subtransmission systems (69-138 Kv.). It is usually a private cable. Leased lines from the telephone company are used but to a less extent and decidedly not the preferred media for new insatllations. The bandwidth is from 0(dc) to 4 kHz.

Power Line Carrier is the most commonly used communication media for all HV and EHV lines (138-800Kv.) The most popular protection scheme is Directional Comparison Blocking, with a fair number of Phase Comparison and

Transferred Tripping schemes in use. Phase Comparison is used more in the western part of the U.S. where series capacitors are installed. The frequency reserved for PLC is from 30-300 kHz and one channel of 4 kHz bandwidth per function is the common provision.

Microwave is becoming more popular for use with administrative and monitoring communication. As more microwave channels are installed, provision is made for protection. The same protection application is used on microwave as on PLC, with Transferred Tripping taking some precedance over Directional Comparison.

Radio and Fiber optics have not been used to any great extent. Certainly Fiber optics will be used when more fiber cable is installed. At the moment this is not a significant factor in the application of protection communication.

LAN's are not used for protection in any way. As digital relays become more used they will undoubtedly be used to a greater extent.

I trust this information is useful.

Sincerely,

Stan Horowitz

cc J.W. Chadwick, Jr.

Le CIGRÉ a apporté le plus grand soin à la réalisation de cette brochure thématique numérique afin de vous fournir une information complète et fiable.

Cependant, le CIGRÉ ne pourra en aucun cas être tenu responsable des préjudices ou dommages de quelque nature que ce soit pouvant résulter d'une mauvaise utilisation des informations contenues dans cette brochure.

Publié par le CIGRÉ
21, rue d'Artois
FR-75 008 PARIS
Tél. : +33 1 53 89 12 90
Fax : +33 1 53 89 12 99

Copyright © 2000

Tous droits de diffusion, de traduction et de reproduction réservés pour tous pays.

Toute reproduction, même partielle, par quelque procédé que ce soit, est interdite sans autorisation préalable. Cette interdiction ne peut s'appliquer à l'utilisateur personne physique ayant acheté ce document pour l'impression dudit document à des fins strictement personnelles.
Pour toute utilisation collective, prière de nous contacter à sales-meetings@cigre.org

The greatest care has been taken by CIGRE to produce this digital technical brochure so as to provide you with full and reliable information.

However, CIGRE could in any case be held responsible for any damage resulting from any misuse of the information contained therein.

Published by CIGRE
21, rue d'Artois
FR-75 008 PARIS
Tel : +33 1 53 89 12 90
Fax : +33 1 53 89 12 99

Copyright © 2000

All rights of circulation, translation and reproduction reserved for all countries.

No part of this publication may be produced or transmitted, in any form or by any means, without prior permission of the publisher. This measure will not apply in the case of printing off of this document by any individual having purchased it for personal purposes.
For any collective use, please contact us at sales-meetings@cigre.org