52

AVAILABILITY OF TELECONTROL SYSTEMS

Part 1

Questionnaire on Availability

Summary Report
Part 2

by

Working Group 01 (Control Centres)
of
Study Committee 35(Communication and Telecontrol)

Part 1
Availability of Telecontrol Systems

Study Committee 35
(Communication and Telecontrol)

Working Group 01
(Control Centres)

Contents

Part 1
Availability of Telecontrol Systems

3.2 Example No 2

3.2.1. Technical System
3.2.2. Reliability, Maintainability and Supportability

3.2.2.1. Reliability
3.2.2.2. Maintainability
3.2.2.3. Supportability

4. Follow-up of Availability Functions

4.1. Methods of Determining Equipment Failures

4.1.1. Observation by the Operators
4.1.2. Automatically by the Telecontrol Equipment
4.1.3. As a result of Testing

4.2. Fault Reporting

4.2.1. Manual Fault Reports
4.2.2. Automatic Fault Reports

4.3. Availability Statistics

5. Maintenance Systems (Examples)

5.1. Example A

5.1.1. Background
5.1.2. Maintenance Staff and Policy

5.1.2.1. First Line Maintenance Section
5.1.2.2. Central Maintenance Section

5.1.3. Software Maintenance
5.1.4. Equipment

5.2. Example B

5.2.1. Maintenance Staff

5.2.1.1. Central Maintenance Section Staff
5.2.1.2. District Control Centres Maintenance Staff

5.2.2. Maintenance Principles

5.2.2.1. Use of Operational Staff
5.2.2.2. District Centre Maintenance
5.2.2.3. Central Maintenance Section

5.2.3. Equipment

APPENDIX 1 - List of Abreviations

APPENDIX 2 - Mathematical Definitions

APPENDIX 3-1 - System Configuration (Example 1)

APPENDIX 3-2 - Availability Requirements (Example 1)

APPENDIX 4 - Availability Requirements (Example 2)

APPENDIX 5 - Maintenance Organisation (Example A)

APPENDIX 6 - Maintenance Organisation (Example B)

APPENDIX 7 - Example of Availability Diagram

AVAILABILITY OF TELECONTROL SYSTEMS

1 INTRODUCTION

A Telecontrol System used in an Electricity Supply Network is an on-line real time system operating continuously. Ideally the system should be available 24 hours a day seven days a week and 52 weeks a year (ie 100%). This figure is of course unattainable.

The Availabilty of any system depends on two separate factors.

Firstly the Components of the system (ie both Hardware and Software) its design and its configuration. Characteristics such as Reliability Maintainability and Supportability are factors which determine System Availability. These factors are not separate entities but are interdependent and interrelated.

Secondly the maintenance and support organisation which has the responsibility for maintaining and repairing the equipment. They must be fully equipped with spares and testgear be well trained and be able to respond quickly to system failures.

A List of the Abbreviations used throughout this report is given in Appendix 1.

2 SOME BASIC DEFINITIONS

2.1 OPERATIVE PERFORMANCE

The Operative Performance is defined as the capability a system develops in its real operative environment with due consideration to system operation and operational constraints.

The operative performance is a combination of Techical Performance and Availability (sometimes also called Reliability Performance) as shown in figure 1.

2.2 TECHNICAL PERFORMANCE

The Technical Performance is defined as the capability a system develops in its real operative environment when there is no need for maintenance and support and when no faults and/or disturbances are interfering with the operation of the system.

The Technical Performance is obtained by correct system design of both Hardware and Software. The design must ensure that the system can fully meet its Specification.

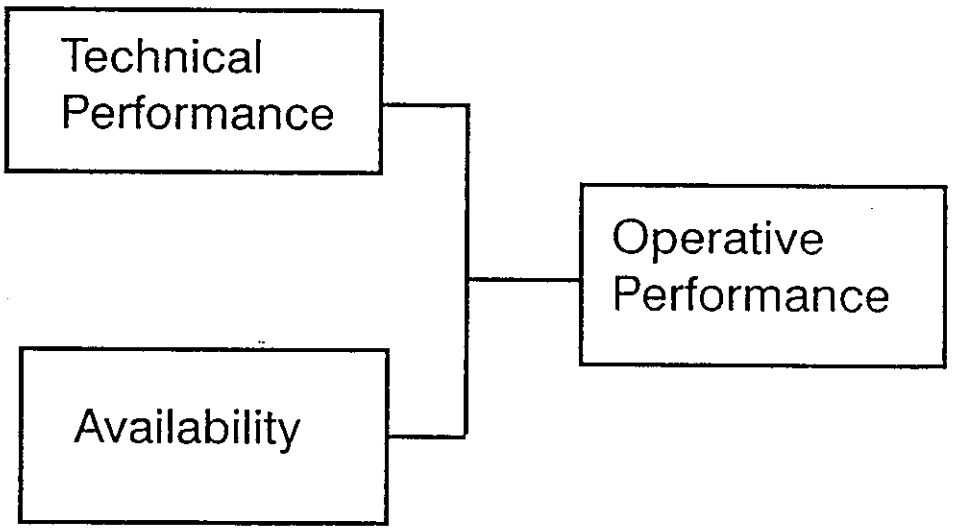


Figure 1 : Operative Performance

System Failures can be divided into three categories - Minor, Major and Critical.

Minor Failures

Minor failures can be classified as a failure of one or a group of non-vital functions. Time to repair these faults is variable and they can often be repaired without any system downtime.

Major Failures

Major failures can be classified as the loss of one or more vital functions. These can be caused not only by component failures and power supply faults but also by failures in the Communication Channels.

Critical Failures

The results of a major failure can vary greatly depending on the circumstances prevailing at the time of failure. If the failure takes place during a power system disturbance or while the user is carrying out or attempting to carry out some function the consequences can be much more severe than if the failure takes place during quiescent conditions. This type of system failure is classified as Critical.

2.3.1.2 Maintainability

Maintainability is the ability of a system under stated conditions of use to be retained in or restored to a state in which it can perform its required functions when maintenance is performed correctly using the prescribed procedures and resources.

It is a measure of the ease with which faults can be traced in both Hardware and Software and faulty modules replaced or repaired.

2.3.1.3 Supportability

Supportability is the ability of a system to be maintained and supported within a defined maintenance organisation.

It is a measure of the available resources such as special tools, test equipment, software fault tracing aids and spares.

2.3.2 Maintenance System Characteristic

Maintenance and Support Effectiveness is the ability of the maintenance and support organisation to prevent and correct faults in the technical system. The effectiveness may be expressed in different ways (eg risk of Line Replaceable Unit (LRU) shortage, time to correct software faults, availability of different personnel categories, logistic response time etc).

MTTR is a measure of maintainability, supportability and maintenance and support effectiveness.

3 AVAILABILITY REQUIREMENTS (EXAMPLES)

3.1 EXAMPLE No.1

The requirement on reliability maintainability and supportability of Telecontrol Systems shown here can be looked upon as an example of the demands which must be taken into account when designing a complete control system. It should be emphasised that the figures given are the user's requirements. The figures are suitable for presentation in a request for a proposal.

3.1.1 Technical System

The system configuration considered for Example No 1 is shown in Appendix 3-1. The 40kV and 130kV stations are connected to the DCC; the 400kV stations are connected to the ACC; part of the data for the 130kV stations acquired from the DCC is transmitted to the ACC.

The figures for the mean number of losses per year can have an impact on the technical solutions to be adopted for each element of the system. In particular on the characteristics and configuration (single or duplicated) of the RTUs to be installed in the stations, of the links between stations and DCC/ACC or between DCC and ACC of the District and Area Control Centers.

The MDT figures in Appendix 3-2 are dependent on the system configuration and the selected maintenance concept. This means that the tenderer in his proposal may also put forward requirements on the purchaser's maintenance organisation regarding out of hours working travelling time etc. It is however the desire of the purchaser to meet these requirements without the need for personnel alertness outside normal office hours.

The numbers given in Appendix 3-2 should be interpreted in the following way:-

Requirement No (1)

The mean number of faults per RTU or per RTU-DCC link causing loss of the telecontrol function from a DCC for a single 40kV station shall be no more than two per year per station.

Requirement No (2)

The mean number of faults per RTU or per RTU-DCC link causing loss of the telecontrol function from DCC and ACC for a single 130kV station shall be no more than one per year per station.

Requirement No (3)

The mean number of faults per RTU or per RTU-ACC link causing loss of the telecontrol function from ACC for a single 400kV station shall be no more than one per year per station.

Requirement No (4)

The mean number of system faults at DCC level causing loss of the telecontrol function from a DCC for all 40kV and 130kV stations within the DCC area at the same time shall be no more than two per year.

Requirement No (5)

It is the same type of fault as requirement No (4) but considers the loss of the telecontrol function from ACC for all 130kV stations in one DCC area at the same time.

Requirement No (6)

The mean number of faults in the DCC-ACC link causing loss of the telecontrol function from ACC for all 130kV stations in one DCC area at the same time shall be no more than two per year.

Requirement No (7)

The mean number of system faults at ACC level causing loss of the telecontrol function from ACC for all 130kV and 400kV stations at the same time shall be no more than one per year.

Requirement No (8)

The mean number of system faults causing loss of the telecontrol function from a DCC for a specific station (by name) shall be no more than three times per year.

The same requirement is valid concerning loss from ACC and DCC at the same time.

Requirements (1) to (7) must be fulfilled even if a single station (by name) has been lost three times in a year.

3.1.1.1 Constraints

Every solution is very dependent on the constraints applied. The model using trained non-specialised technicians (A-level) for the maintenance work and specialised engineers for the qualified maintenance work (B-level) is just one of several possibilities. Very often the solution has to take into account the existing maintenance personnel and organisation.

The overall availability requirements stated here are valid for the total operative system.

Mean Active Repair Time (MART) includes active time for FL1 and FL2.

Mean Logistic Down Time (MLDT) includes travelling time, transportation and waiting time for the required maintenance resources which depend on the purchaser's requirements and the local conditions.

MTTR (or MDT) = MLDT + MART

3.1.1.2 Reliability

A manufacturer has to configure a system in the way which will fulfill the purchaser's requirements. Therefore it is necessary for a purchaser to give figures like those mentioned in section 3.1.1. Possible ways to implement the required reliability are redundancy and quality control programs.

3.1.2 Maintainability

3.1.2.1 General

The design of the system shall be carried out in such a way that the required maintainability performance will be fulfilled. The following sections describe the detailed requirements of the system.

3.1.2.2 Detailed Maintainability Requirements

Modularisation

The product shall be modularised to units that are exchangeable at site (ie to Line Replaceable Units - LRUs).

LRUs shall when necessary be modularised to sub-LRUs to facilitate repair of faulty LRUs that have been replaced.

The modularisation shall be adapted to the reliability performance requirements as stated and to the suggested maintenance and support concept. It shall normally be possible for LRUs to be handled by one peerson during maintenance.

Marking

All LRUs and sub-LRUs including those delivered as spare material shall be marked according to the technical specification. LRUs andd sub-LRUs that are marked identically shall be replaceable at all places in the system.

Transportation of LRUs and sub-LRUs

Transportation of LRUs and sub-LRUs by road rail or air shall be made possible by utilising suitable packing. Packing shall be included in the delivery.

Calibration

Calibration adjustment address changes etc shall not be required on either the system or the LRU when performing maintenance at site. All such actions shall when required always be performed at the Central Maintenance Depot.

Exchange of LRUs

All LRUs shall be plug-in units. Soldering wiring etc shall not be needed in either the system or the LRU when maintenance is performed on site.

Injury to Personnel

The risk of injury to personnel caused by electricity shall be reduced by using protective devices and by marking the equipment appropriately.

Cable arrangement

Cable arrangements shall be designed so that the exchange of LRUs causes no inconvenience to personnel during maintenance. This also means that only one person shall be required to reach any LRU in the system.

Faulty exchange of LRUs

The risk of faulty exchange of LRUs or faulty connection of cables or incorrect plug-in of circuit cards etc shall be negligible (eg cable connectors - male and female - shall be marked). Jumpers shall also be marked and documented in the maintenance documentation, drawings etc.

Accessability

All the equipment and Hardware should be easily accessible (eg when noise reduction covers for printers are used accessability shall not be drastically reduced).

Probing

It shall be possible to do adequate probing and testing within important system interfaces.

Adverse impact of maintenance on the system

Product maintenance and support activities that will interfere with the total information system functions shall be kept to a minimum.

LRU handling

LRUs shall be easy to handle (lift, transport, store etc). If two people are needed this shall be stated and heavy units shall be pointed out.

Equipment for repair of LRUs on site

For LRUs that according to the contractor's advice shall not be transported to the Central Maintenance Depot, a special Site Test and Repair Equipment (STRE) shall be used. By using the STRE it shall be possible for the B-level maintenance personnel (trained by the contractor) to repair such LRUs on site. This means that the STRE shall be moveable (eg by car).

Configuration changes

Configuration changes in the system shall be easy to perform. Change from 'main' to 'standby' in redundant parts of the system should be performed automatically.

It shall however always be possible to perform manually configuration changes in the system.

It shall then be possible to override all automatic procedures used for configuration changes.

Configuration changes should not introduce new faults causing loss of a function or functions.

3.1.2.3 Supportability

An optimum level of supportability has to be evaluated in detailed discussions between purchaser and manufacturer.

3.1.2.4 Maintenance System Characteristics

3.1.2.4.1 General

Provisions could be made for two levels of maintenance procedures. The first level, FL1, shall be centred around the function of fault localisation. The second level, FL2, shall be centred around fault isolation and repair. The design of these functions should be adapted to the qualifications of the purchaser's maintenance personnel and in some cases both functions will be carried out by the same person.

3.1.2.4.2 Personnel Category Definition

The purchaser's A-level personnel do not require an engineering background. The main working task of this category of personnel is to maintain the high voltage transmission lines and the transformer stations and they need have no experience in the maintenance of electronic systems.

The purchaser's B-level personnel do in general have an engineering background and previous experience in the maintenance of electronic systems.

The A- and B- level personnel categories shall fulfill stated requirements properly trained as set forth in the Training Plan.They shall be provided with documentation as set forth in the Documentation Plan, the necessary handling equipment, special tools and diagnostic equipment.

3.1.2.4.3 Requirements on the FL1 Function

By using FL1 procedures it shall be possible to localise a fault to a faulty system part and the geographical place of that part (this shall also be interpreted as the room where the part is situated) in no more than 0.5 hours.

Automatic function monitoring shall be built into the system.

FL1 shall contribute to the following:-

- fault statistics concerning faults and disturbances

- alarms for faults that have occurred in the system

- informaation for fault localisation

The function 'fault statistics' shall perform continuous logging of faults and disturbances occurring in the information system. A daily status report of the statistics shall be printed out. The print-out shall be manually initiated.

The function 'fault statistics' shall cover equipment of concern in the system. Such equipments that will make repeated attempts (request, restart, fail-over, start etc) shall be covered by the fault statistics and each attempt shall be logged where the existing Hardware or Software provides this information. Not approved messages and unsuccessful readings of disc information are examples of such events that should be included in the fault statistics. In the print-out a logged event shall be identified together with the faulty or disturbed equipment.

Disturbances shall be logged by number.

Faults shall be logged by number and time for fault detection as well as time for fault elimination.

All Hardware units shall be included in the FL1 function.

The fault statistics report shall be edited in a suitable manner to enable follow-up evaluation of the Reliability Performance of the system.

Fault alarms shall be divided into categories. The alarm presentation device shall be placed close to or in the Computer Room.

An alarm shall be presented both visually and audibly.

If the fault has consequences on the operation of the Control Centre a general alarm should be presented to the Operator. This should cover all system reconfigurations (eg failovers).

This alarm function could be transmitted to maintenance personnel on standby.

FL1 shall also contain the function 'fault localisation'. This function shall localise a fault to a suitable section of the information system. The information system shall therefore be sectorised from the point of view of fault localisation in order to carry out the following:-

- direct maintenance personnel to the correct geographical place (this shall also be interpreted as the actual room where the faulty equipment is situated) for final fault isolation.

- select the LRU (from a number of LRUs) that is required to repair the faulty section as identified above.

The fault localisation function shall cover all faults that may occur in the system (ie also faults in redundant parts of the system).

The fault isolation function may be designed as an interactive procedure that will generate the required information in clear text.

Fault statistics and alarm and fault localisation information for such faults and disturbances that occur in the RC-part of the system shall be presented at the RC.

The corresponding is valid for each DC.

3.1.2.4.4 Requirements on the FL2 Fault Isolation and System Repair Procedures

FL2 shall include functions procedures and documentation for the following:-

- fault isolation to faulty LRU
- repair of the system
- check-out after repair
- restart of the system

It shall be possible to perform FL2 during normal operation in redundant parts of the system without disturbing other equipments in the system.

FL2 shall be possible to perform in such non-redundant parts of the system that are not primarily included in the telecontrol function in such a way that this function will not be affected.

3.1.2.4.5 Requirements on Equipment in Control Centres

The following requirements apply for all the equipment placed at the Control Centre:-

- at least 90% of the Hardware faults shall be possible to correct by utilising the purchaser's B-level personnel at a mean down time of no more than 3 hours (logistic delay time excluded).

- at least 90% of the remaining 10% of the faults shall be possible to correct by utilising the purchaser's B-level personnel at a mean down time of no more than 12 hours (logistic delay time excluded).

- the remaining 1% of faults shall be possible to correct by utilising contractor support at site.

3.1.2.4.6 Requirements on Equipment placed outside Control Centres

The following requirements apply for all equipment outside Control Centres:-

- at least 90% of the Hardware faults shall be possible to correct by utilising the down time of no more than 3 hours (logistic delay time excluded).

- at least 90% of the remaining 10% of the faults shall be possible to correct by utilising the down time of no more than 12 hours (logistic delay time excluded).

- the remaining 1% of faults shall be possible to correct by utilising contractor support at site.

For such cases where the A-level personnel will not be able to correct a fault according to the above requirements the FL2 manual intended for the A-level personnel shall provide clear procedures telling the A-level personnel when B-level assistance becomes necessary. The A-level personnel shall be able to decide if assistance from B-level personnel is required in no more than 3 hours.

3.1.2.4.7 Fault location in Software

Faults in the software can manifest themselves in many different ways (eg system failure, program crashes, calculation faults, lost alarms etc.). The faults can be there in their own right or can be related to hardware faults, handling faults or input data faults.

Definition

Software faults mean any form of deviation from the given specifications which cannot be assigned solely to the hardware. To enable the purchaser's own personnel to search for faults in the software the Supplier should prepare a training packet and fault-seeking documentation which will be included in the programming handbook. It shall be possible for personnel who have completed the training course and who have access to the documentation to find the reason for 90% of any manifested software faults within 2 hours. Only the faulty module need be identified for faults in software taken directly from a Computer supplier. For other faults the direct reason for the fault should be able to be defined in such terms as 'Underdimensioned data area', faulty stop in certain conditional logic', 'forgotten updating of the pointer table', etc.

The purchaser's personnel will be trained so that they can find software errors. However the time for finding an error has to be limited to reproduceable data errors. The debugging of possible remaining logic errors is affected by many factors which are out of the supplier's range.

3.1.2.4.8 Contents of the FL2 Manuals

FL2 shall be tailored to the needs of each category of personnel and shall be designed as step-by-step procedures with instructions provided for each step. Steps shall be performed in sequence. Documentation for FL2 shall contain descriptions of the important results from each step. Timing for each step in the step-by-step procedure shall be included in the FL2 manuals for the A- and B-level personnel. The procedures shall in general be automatic and contain a minimum of manual actions especially during fault isolation. The procedures shall include instructions for fault isolation to a faulty LRU, exchange of LRUs and system check-out.

Documentation of the FL2 procedures shall be provided according to the purchaser's standard.

3.1.2.4.9 Definition of the Elements of Equipment Mean Down Time

Equipment Mean Down Time includes, in general, time elements for the following:-

- preparation at site
- fault isolation to faulty LRU
- disassembly
- exchange of faulty LRU
- reassembly
- system restart
- putting the site back to its original shape
- system check-out

3.2 EXAMPLE No.2

The figures given in Example 2 are examples of what can be achieved by typical modern systems. Every one of these figures is for absolute worst case conditions.

3.2.1 Technical System

The figures given in Appendix 4 can be explained as follows:-

Requirement No.1

A station with a single RTU should have on average no more than two minor or one major fault per year. Minor faults should be repaired on average within 24 hours while major faults require much more rapid attention - no more than six hours on average.

As a general rule the time to repair major faults is dependent on the particular station and the prevailing system conditions.

Requirement No.2

In a station with more than one RTU whether or not they communicate with the same or different Control Centres the figures for Minor Faults apply to both RTUs (ie on average there will be two Minor Faults per RTU per year). In the case of Major Faults the figures apply to the loss of both RTUs simultaneously and for the time taken to repair one of them. Both should be repaired within the time given in Requirement No.1.

Critical Faults (ie Major Faults occurring during a Power System Disturbance) are statistically too remote to be considered.

Requirement No.3

All the figures given in this Requirement apply only to Hardware. The RCC will have complete redundancy and the figures given for Minor Faults are the total for all the RCC systems. The figures for major faults apply to complete failure of the RCC systems although a back-up system giving limited facilities should be available to cater for this situation.

Requirement No.4

The figures given in this Requirement include both Hardware and Software faults. Minor Software Faults although applying to both Computer Systems only count as one fault.

Requirements Nos.5 and 6

Requirements Nos 5 and 6 are similar to Nos 3 and 4 respectively. Although the figures for Dispatching Centres are the same as those for Remote Control Centres, the Telecontrol System Equipment in the Dispatching Centre is much more complex than the system in the Remote Control Centre.

3.2.2 Reliability Maintainability and Supportability

3.2.2.1 Reliability

This is the ability of the equipment to carry out its alloted tasks without fault or failure.

In order to achieve the required reliability some of the factors that should be taken into account are as follows. The equipment should be of a good design using the highest quality components and all the components should be operated well within their specifications. Where plug in sub-assemblies or modules are used the connectors should also be of the highest quality. A system using a small number of large sub-assemblies should be more reliable than one using a large number of small sub-assemblies.

All Modules used must have the highest possible reliability standards. They must be tolerant to their environment with particular reference to Temperature. Equipment requiring special environmental conditions such as close temperature control or a dust free atmosphere should only be installed in locations where these criteria can be met. They must also have a high noise immunity.

The equipment should be provided with a complex monitoring system in order that failures may be dealt with quickly and efficiently and to prevent certain less serious failures becoming more serious and giving rise to future problems. An example of this is a Battery Charger Failure which if not properly monitored and alarmed could eventually lead to a complete failure of part of the system.

As these Systems are monitoring and controlling the Electricity Supply network it is essential that all the equipment should be operated independent of a mains supply.

3.2.2.2 Maintainability

Equipment should be modular with the modules removable by disconnecting plugs and sockets and without any wiring to be altered although a small number of screws may have to be slackened. A balance has to be struck between the need to have a modular design with the requirement to have a high reliability by not introducing too many small units and thus too many connectors.

Spares should be kept at suitable locations. Where plug-in units are used care should be exercised to ensure that the fault is correctly diagnosed and that only the faulty card is replaced. A large proportion of faults in modern equipments are of a type that disappear while they are being worked on and in this type of fault care should be taken to localise the fault if at all possible. Only the suspect module should be changed. As far as possible address changes on cards should be avoided.

The more standardisation of equipment the less are the difficulties experienced not only in dealing with faults where familiarity with the equipment is of inestimable value but also in the numbers of different spare modules that have to be held.

Sufficient Test Points which are readily accessible should be built into the equipment and this should be clearly specified.

The maintenance staff should not only be well trained but they must also have adequate opportunies to get experience of the equipment by working on it at the installation and design stages of the work. Formal training although having an important part to play should certainly not be the end of training.

It is important that in the Maintenance Organisation a balance is struck between the requirement (due mainly to the complexity of modern equipments) to keep staff in centralised locations with the requirement (in order to reduce travelling time) to keep staff spread out over the network.

3.2.2.3 Supportability

The System should be provided together with the necessary documentation, drawings and testgear in order to allow the Maintenance Organisation to function correctly.

The provision of good documentation is an absolute necessity for the Maintenance of the Software. It is vital that this highly complex and very important function can be carried out by a number of personnel and that staffing changes do not cause too much disruption.

4 FOLLOW-UP OF AVAILABILITY

With any type of system employing a Maintenance organisation it is essential to have some method of determining the Operative Performance of the Telecontrol System.

The Technical Performance should normally become apparent very quickly (eg shortage of memory capacity, poor response times etc.) and this should not change unless functions or facilities are altered.

The Availability on the other hand is something that could alter and true figures for Availability can only be obtained over the lifetime of the equipment.

All modern Equipments using solid state components need little or no preventive Maintenance and do not generally deteriorate with age. Any components with a finite life (eg Reed Relays, Cooling Fans etc) should be checked regularly and where possible replaced before the onset of trouble.

Methods of determining the Availability of the Telecontrol Systems have to be employed in order that a quantitative judgment on the performance of the Equipment can be made. If these methods show that the Availability figures obtained fall outwith acceptable limits then appropriate steps should be taken to determine the causes of this and examine what action or actions should be taken to rectify the problems.

4.1 METHODS OF DETERMINING EQUIPMENT FAILURES

4.1.1 OBSERVATION BY THE OPERATORS

In many cases minor failures (ie the failure of one or more functions from a single station) are first detected by the Operators who are able by their training and experience to tell quickly if a telemetered value or status indication is incorrect.

The Operators will also become aware of major faults in a lot of cases before the alarm generated by the telecontrol equipment has been presented to them.

4.1.2 AUTOMATICALLY BY THE TELECONTROL EQUIPMENT

In some cases minor failures can be detected automatically by the Telecontrol Equipment itself but in most cases this is only possible where the system has built-in redundancy. Major failures (eg the loss of all the data from one or a group of outstations) should always be detected automatically. Once the fault has been detected an alarm is generated to warn the Operator of the situation.

4.1.3 AS A RESULT OF TESTING

Some form of systematic routine testing procedure should be carried out to confirm that the Equipment is functioning correctly. This testing may be carried out in such a way that the Telecontrol System forms only a part of the Equipment being tested. In general it is not possible to check every function individually and only a repesentative sample can be tested.

4.2 FAULT REPORTING

The Failure Statistics must be recorded collated and evaluated in order to derive figures for the System Availability. Recording of failures is absolutely essential if meaningful performance figures are to be attained. The methods of recording system failures are dealt with in the following sections.

4.2.1 MANUAL FAULT REPORTS

All faults detected by the Operators should be recorded manually by them either on a Log specifically designed for that purpose or preferably on one of the Control Centre Computer Systems.

4.2.2 AUTOMATIC FAULT RECORDING

All faults which are automatically detected (ie all major faults and some minor faults) should be recorded automatically by a Control Centre Computer System.

4.3 AVAILABILITY STATISTICS

Availabilty Statistics should be prepared on a periodic basis. These should be compared to the figures supplied by the manufacturer in his tender document. The periods covered being one or more of the following - daily, weekly, monthly, quarterly and yearly. The preferred periods being monthly and yearly.

The statistics should cover both Major and Minor faults but the figures should be split into different subsections covering such items as the Control Centre Equipment (ie Line Buffer Units, Computer System, VDUs etc) the Communication Channels, the RTUs and the peripheral equipment in the Outstations (eg Transducers).

The details of each fault should be collated with the consequences of it and the time taken to repair (TTR). The TTR should only be counted from the time that the repair procedure begins. Where a deliberate decision is taken not to deal with a fault immediately this time should not be counted in the TTR.

The time between a fault occurring and the fault being detected cannot in a lot of cases be measured and is not considered in this paper. It will not always be the case that because the Operator has not detected a fault it is of no significance.

It is important that the failure statistics like other aspects of the Telecontrol System are user oriented. The information should be produced in such a form that it can be easily assimilated and without a great deal of analysis it can provide details of the weak parts of the system where the MTBF is too low or the MTTR is too high.

5 MAINTENANCE SYSTEMS

A Maintenance and Support Organisation must be provided in order to maintain and repair the equipment. This Organisation should have a structure and policy which allows it to deal adequately with all types of system failures. Two examples of Maintenance Systems are given in the following sections.

5.1 EXAMPLE A

The System described in this example consists of a Dispatching Centre and seven District Control Centres. The Dispatching Centre has links to all the other Centres and has also direct links to the RTUs in the main Substations and Power Stations. The Telecontrol System and the Maintenance Organisation are shown in Appendix 5.

5.1.1 BACKGROUND

Over the last 20 years there has been a considerable change in the type and quality of the maintenance required for Telecontrol systems and Equipment. The replacement of Electro-mechanical systems by solid state systems has led to a sharp reduction in preventive maintenance and an increase in the skill required to find faults in the new types of equipment. As the early equipments have been replaced by more modern systems which are largely micro and mini computer based this maintenance trend has continued albeit more slowly.

During the 50s and 60s most of the staff employed on the maintenance of Telecontrol Equipment in this Example did not possess professional qualifications and relied on their usually vast experience to fix faults. Nowadays most of the staff have professional qualifications and have spent their working life in the Electricity Supply Industry. They therefore have the ability to assess equipment unavailability with regard to the prevailing system conditions and to take the appropriate action.

5.1.2 MAINTENANCE STAFF AND POLICY

Well educated Maintenance staff fully trained to deal with the equipment that they have to maintain are used.

In order that the staff have a sufficient knowledge of the equipment they are involved in some of the following phases of the work - design development specification and installation.

In the system described in this Example which covers a large area the staff are of necessity situated in a number of different locations. Each of these contains sufficient manpower in order to maintain a continuity of service. These first line maintenance locations are backed up by a central maintenance and repair section.

5.1.2.1 FIRST LINE MAINTENANCE SECTIONS

Each of the First Line Maintenance Sections has on average four Engineers one Technician and two Manual Staff.

The first line maintenance locations are able to clear all faults in both the RTUs and the Control Centres by changing Modules or Sub-Assemblies and for this purpose they are fully equipped with an adequate amount of spares. They do not normally repair faulty Modules but instead return them to the Central Maintenance Section.

The first line maintenance sections are only involved in the most basic of tasks with regard to the Software such as loading Programs (eg updates and in the event of Software 'crashes') and running simple diagnostic programs in an attempt to localise system failures.

All faults are normally dealt with within two hours (excluding travelling time etc). In certain circumstances (eg Sub-transmission or Distribution Substations or a Power station that is completely de-watered) action may be postponed until normal working hours (ie the following day).

These first line Maintenance Sections are specialist technical sections rather than specialist telecontrol sections and they also deal with a wide range of other technical problems. These include some or all of the following:- Communication Channels, Telephone Switching Equipment, VHF Radio and Protection. The particular range which is dealt with by any particular section is dependent mainly on its geographical position.

The Staff in these sections are only available during the normal working day as a standard eight hour day five day week is operated. For faults that occur outwith these times staff have to be called in to deal with them.

5.1.2.2 CENTRAL MAINTENANCE SECTION

In the Central Maintenance Section there are nine Engineers and two Technicians. The Engineers are highly educated and fully trained specialists and are able to deal with problems at great depth.

The staff of the Central Maintenance Section are responsible for repairing and returning all faulty Modules and Sub-Assemblies. They also provide specialist backup in the event of faults that cannot be cleared by the first line maintenance sections. In a lot of cases they also handle the first line maintenance themselves.

They are responsible for ensuring that there are always sufficient spares available to meet all foreseeable eventualities.

As in the first line maintenance sections the staff are only available during the normal working day but a 'Standby Rota' is employed to ensure that an engineer is always available immediately.

5.1.3 SOFTWARE MAINTENANCE

The Maintenance of the Software particularly in the Control Centre equipment is an extremely complex and difficult task and is carried out by a separate section which is not part of the Central Maintenance Section.

However the Software Engineers do have a good understanding of both the Hardware and the System to which it is applied.

5.1.4 EQUIPMENT

ACC - 2*PDP 11/34 (16 bit)
to be uprated to 2*VAX (32 bit)

DCC - Either 1*MP200 (16 bit)
or 2*(S20 + MP200) (both 16 bit)

RTUs - 104

5.2 EXAMPLE B

The Maintenance System described in this example handles a Telecontrol System which links a National Control Centre with eight District Control Centres which in turn communicate with the RTUs in the Outstations. The organisation of the Telecontrol System and the Maintenance Organisation are shown in Appendix 6.

5.2.1 MAINTENANCE STAFF

Specialised Maintenance Staff are based at the Central Maintenance Section and at each District Control Centre.

5.2.1.1 CENTRAL MAINTENANCE SECTION STAFF

At the Central Maintenance Section there are seven Engineers and nine Technicians.

5.2.1.2 DISTRICT CONTROL CENTRES MAINTENANCE STAFF

At each District Control Centre there are on average six Technicians and thirteen other non-technical staff who carry out maintenance on the Telecontrol System.

5.2.2 MAINTENANCE PRINCIPLES

The following Maintenance Principles are employed in this Maintenance System.

5.2.2.1 USE OF OPERATIONAL STAFF

Operational Staff are used to perform first line Maintenance Functions. These include the following:-

Configuration changes in redundant parts of the System

Fault Localisation

Fault Localisation is limited to restricted tasks under instruction from the specialised Maintenance Staff.

5.2.2.2 DISTRICT CENTRE MAINTENANCE

The specialised Maintenance Staff in each District Control Centre carry out a number of duties as follows:-

Preventive Maintenance

Fault Localisation

Repair of the system using LRUs

Only minor duties in the area of Preventive Maintenance are carried out by the District Centre Maintenance Staff

5.2.2.3 CENTRAL MAINTENANCE SECTION

The staff at the Central Maintenance Section carry out the following duties:-

Preventive Maintenance

Repair of the System in the case of complicated failures

Repair of faulty Units

Contacts with the Manufacturers of the Telecontrol System

The Central Maintenance Section also holds the Central Stock of Spares and organises the return of faulty items to the Manufacturers.

5.2.3 EQUIPMENT

ACC - 3*PDP 11/34 (16 bit) + 2*MODCOMP (EMS)

DCC - 2*PDP 11/35 (16 bit)

RTUs - 103

LIST OF ABBREVIATIONS

ACC	Area Control Centre
FL1	Fault Location - step 1
FL2	Fault Location - step 2
LRU	Line Replaceable Unit
MART	Mean Active Repair Time
MDT	Mean Down Time
MLDT	Mean Logistic Down Time
STRE	Site Test and Repair Equipment

MATHEMATICAL DEFINITIONS

AVAILABILITY

The availability of a system characterises its ability to perform the intended function at any given moment.

The essential difference between this and the concept of reliability is that reliability concerns operations over a given period while availability concerns operation at a given instant.

Availability can be stated as:-

$$A = \text{uptime}/(\text{uptime} + \text{downtime})$$

Downtime in the above equation normally includes corrective maintenance preventive maintenance and System expansion downtimes if such times compromise the user's ability to operate apparatus normally controlled by the equipment being expanded.

For design analysis and to determine an 'a priori' prediction of availability for sub-assemblies and units the following equation utilising MTBF and MTTR shall be used.

$$A = MTBF/(MTBF + MTTR), \text{ where}$$

A = Predicted Availability of a component.

The equation for A and the combinatorial equations associated with parallel redundant components (or sub-systems) are valid under the following conditions:-

(a) The failure of any component within a string or parallel set is independent of the failure of any other component. In other words component failures do not propagate failures of other components.

(b) Sufficient repair facilities and standby replacement parts are available in order to handle multiple simultaneous failures.

It is possible to specify the availability for each of the specific functions. However when trying to specify availability figure for the whole system a difficulty arises in judging which functions are essential for the whole system or not essential.

The impact of the outage of each system element or function on the availability of the total system should be mutually agreed upon between the user and the supplier.

RELIABILITY

Reliability is defined as a measure of an equipment's or system's ability to perform its required function under specified conditions for a specified period of time. It is a probability figure based on failure data and length of operating time. The reliability of system components is reflected in their respective mean-times-between-failure (MTBF) numbers. This 'figure of merit' is used in the calculation of the system availability

where $R = e^{-\frac{t}{MTBF}}$

MTBF = mean time between failure
t = the specified time interval

and

$$MTBF = \frac{I}{\sum_{i=I}^{n} \lambda i}$$

where λ_i = the failure rate of the components

MAINTAINABILITY

The maintainability of equipments or systems is reflected in their respective mean-time-to-repair (MTTR) number. MTTR values may include:-

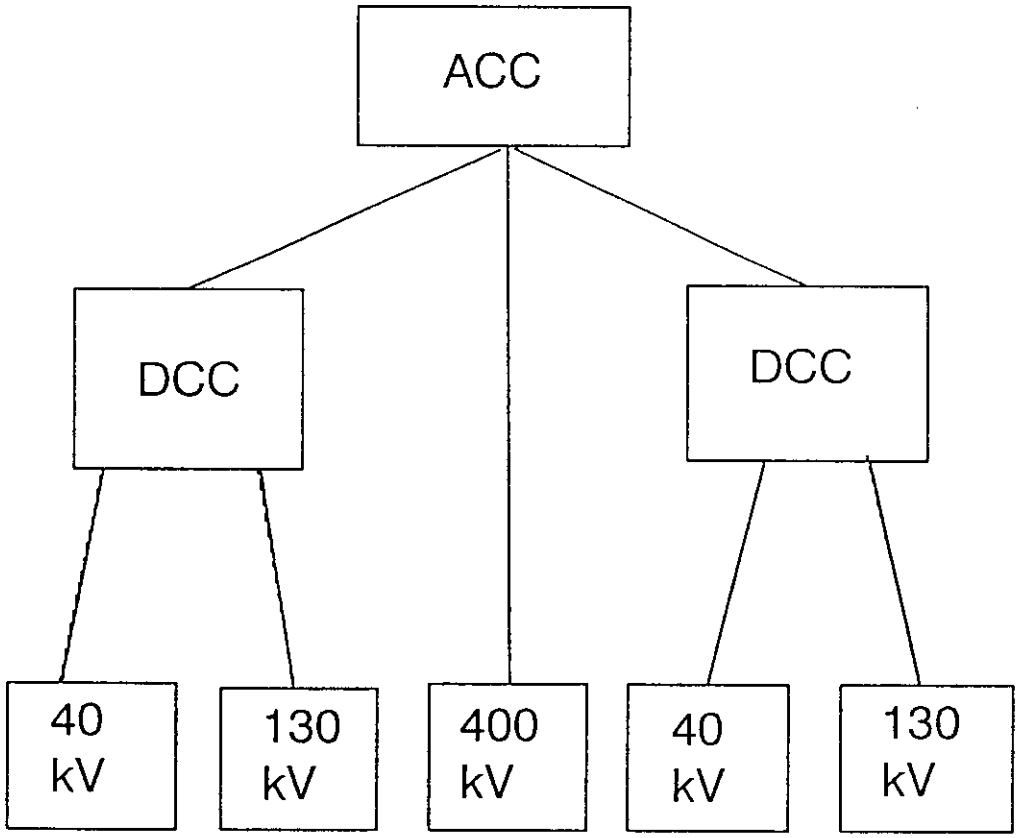
(a) Administrative time - the time interval between failure of a component and a call for maintenance service.

(b) Transport time - the time interval between the call for maintenance service and the arrival at the station of a maintenance technician and the necessary replacement parts.

(c) Repair time - the time required by a trained maintenance technician having the replacement parts and the recommended test equipment at the station to return the faulty system to normal operation.

The MTTR values used in availability computations should be based to the maximum extent possible upon maintenance experience.

SYSTEM CONFIGURATION (EXAMPLE 1)



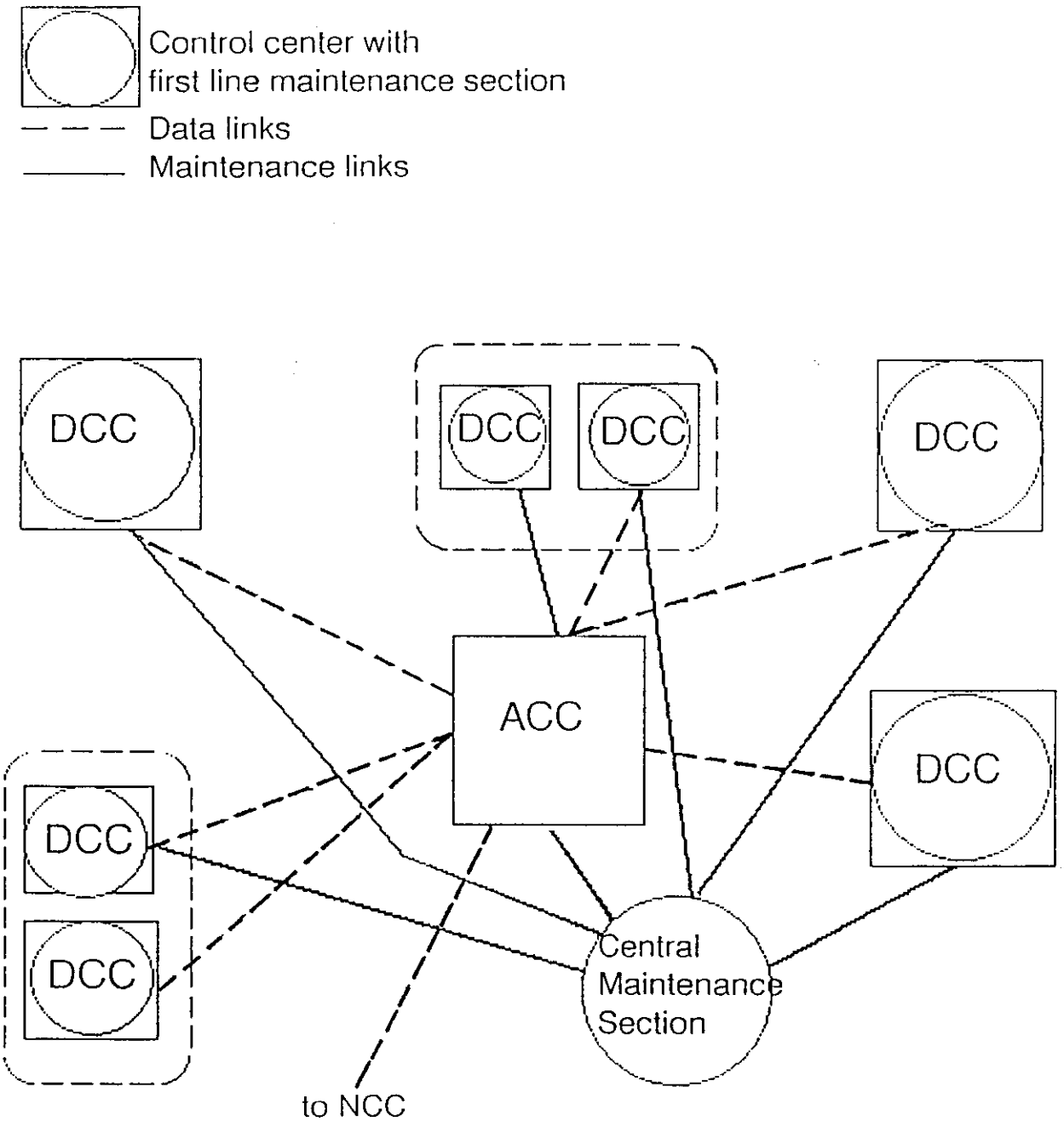
AVAILABILITY REQUIREMENTS - MAJOR FAULTS (EXAMPLE 1)

NO	TYPE OF CONTROLLED STATION	MEAN NUMBER OF LOSSES PER YEAR AND STATION/ALL STATIONS			
		Loss from DCC (per DCC area)	Loss from ACC	Loss from ACC and DCC	MDT(hrs) per loss
1	Any 40kV station	2	-	-	24
2	Any 130kV station	-	-	1	24
3	Any 400kV station	-	1	-	12
4	All 40kV and 130kV stations in one DCC area	2	-	-	12
5	All 130kV stations in one DCC area	-	-	2	12
6	All 130kV stations in one DCC area	-	2	-	12
7	All 130kV and 400kV stations	-	1	-	8
8	Any specific station (by name)	3	3	3	24

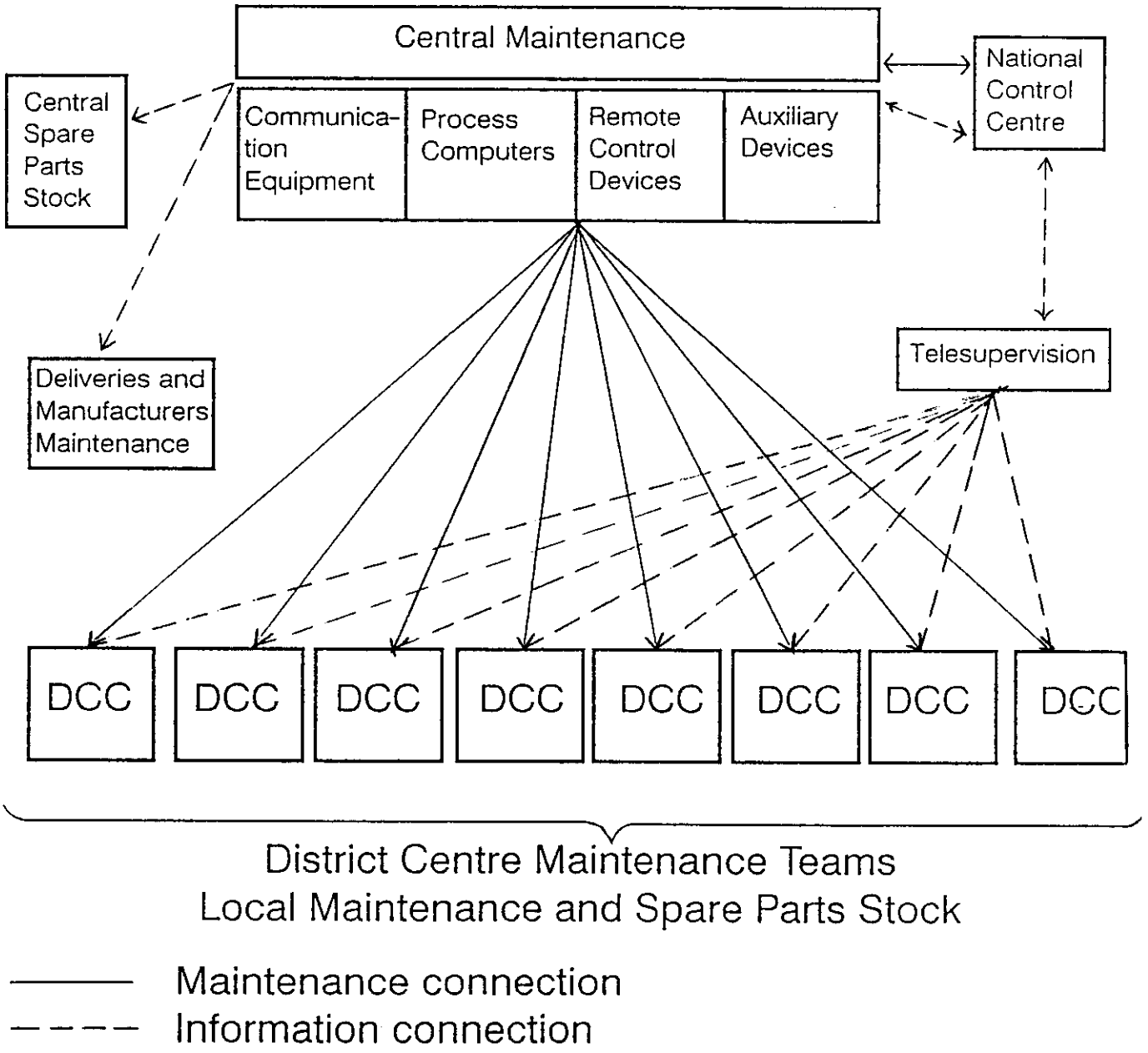
AVAILABILITY REQUIREMENTS - MAJOR FAULTS (EXAMPLE 2)

	TYPE OF FAULT					
	MINOR		MAJOR		CRITICAL	
	No	MDT(hrs)	No	MDT(hrs)	No	MDT(hrs)
1 Station with One RTU	2	24	1	6	0.1	3
2 Station with more than one RTU	4	24	0.1	3		
3 RCC	4	24	2	2		
4 RCC (including Software)	8	48	4	12		
5 Dispatching Centre	4	24	2	2		
6 Dispatching Centre (including Software)	8	48	4	12		

MAINTENANCE ORGANISATION (EXAMPLE A)



MAINTENANCE ORGANISATION (EXAMPLE B)



EXAMPLE OF AVAILABILITY DIAGRAM

HARDWARE CONFIGURATION

The Hardware Configuration of the Control System considered for the Availability Diagram is shown in Appendix 7-3. The Line Buffer Units are responsible for the communication with the RTUs.

The Computer System is a dual system with one acting as the Primary and the other as the Secondary System on 'Hot' Standby. Each Computer System consists of a Main Computer (MC) with the relevant Disks (DK) and a Front End Computer (FE).

The Man-Machine Interface consists of two consoles each one equipped with two VDUs and a Keyboard (KB) and two Printers (PTY). in addition there is a Mimic Board giving an overview of the network.

AVAILABILITY ANALYSIS

The Availability Block Diagram for the Control System shown in Appendix 7-1 is given in Appendix 7-2. The Block Diagram relevant to the 'vital' functions is based on the following concepts:-

- (n-1) LBUs out of n LBUs must be operative
- at least one FE must be operative
- at least one MC with the relevant Disks must be operative
- the switch between the MCs and the Man-Machine Interface must be operative
- at least one Console with at least 1 out of 2 VDUs must be operative
- at least one printer must be operative
- the presentation on the Mimic Board and the transmission to other Control Centres are considered as 'non-vital' functions.

AVAILABILITY COMPUTATION

ALBU = Availability of each LBU

AFE = Availability of FE1, FE2

AMC = Availability of MC1, MC2

ADK = Availability of DK1, DK2

ASW = Availability of the switch

AKB = Availability of each keyboard

AVDU = Availability of each VDU

APTY = Availability of each printer

The availability from A to B is:-

$$AAB = 1 - (1 - ALBU^{n-1})^{n}$$

The availability from B to C is:-

$$ABC = 1 - (1 - AFE*AMC*ADK)^{4}$$

The availability from C to D is:-

$$ACD = ASW$$

The availability from D to E is:-

$$ADE = 1 - \langle 1 - AKB*(1 - (1 - AVDU)^{2}) \rangle^{2}$$

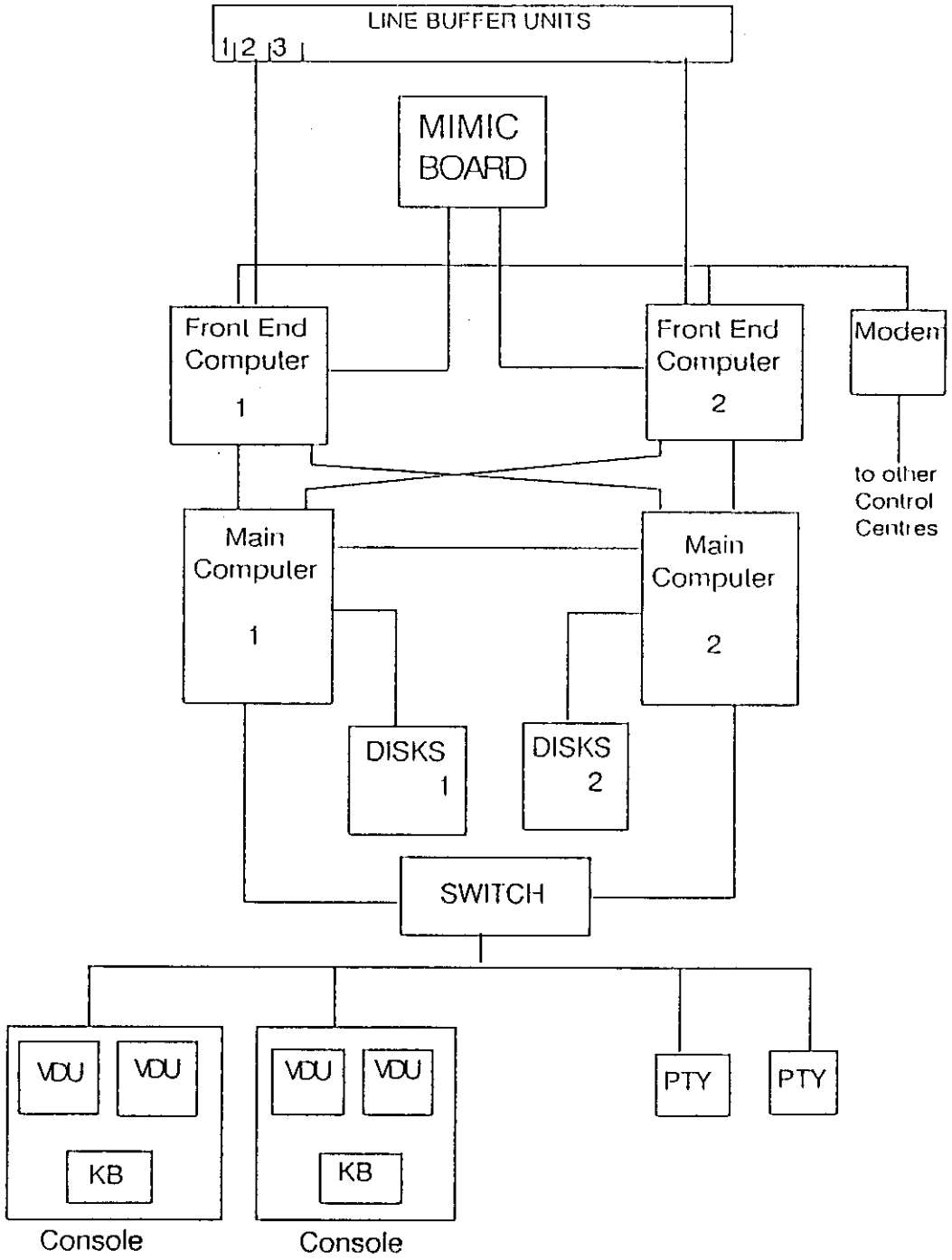
The availability from E to F is:-

$$AEF = 1 - (1 - APTY)^{2}$$

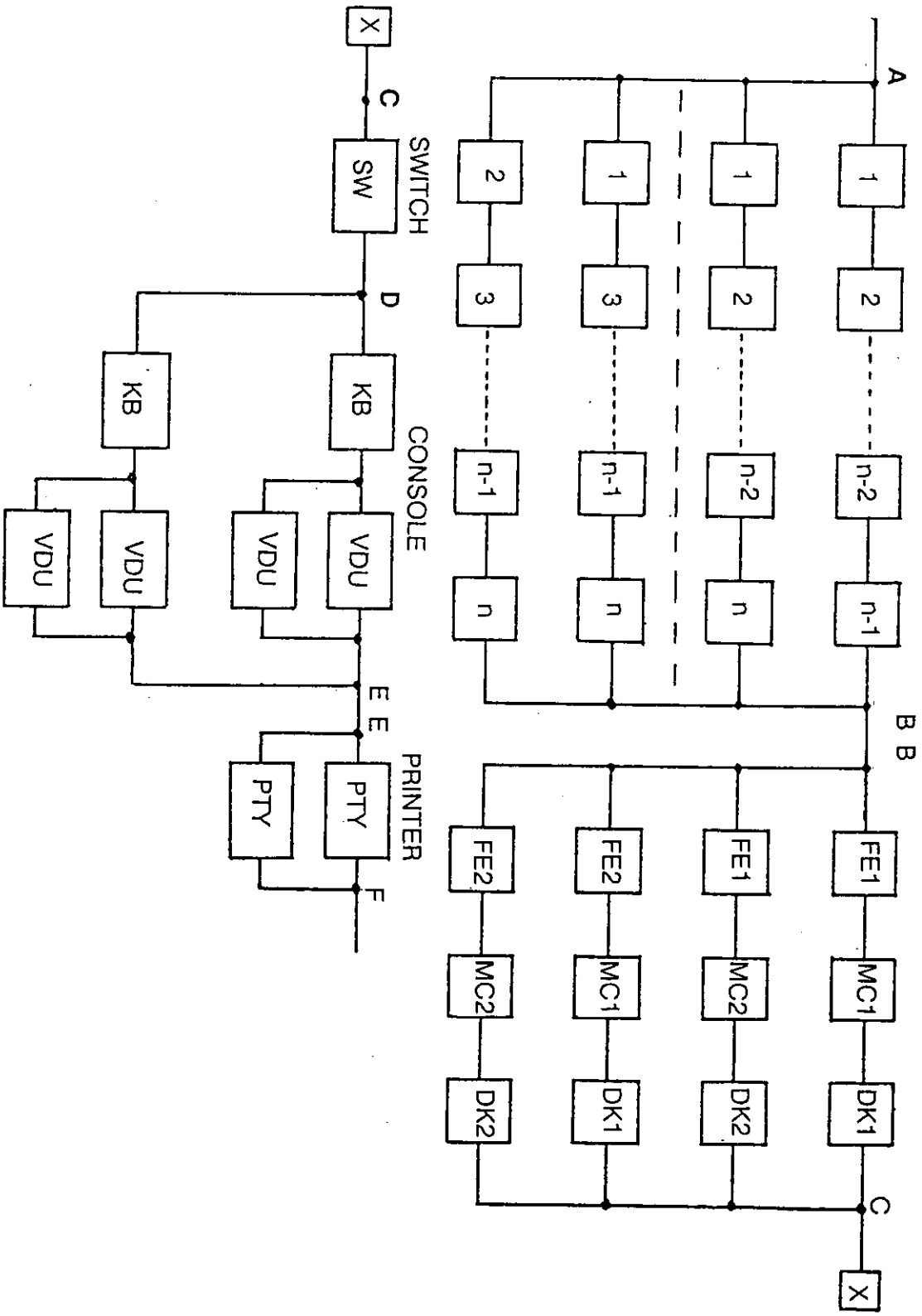
The availability figure for the vital functions of the Control System is:-

$$ATOT = AAB*ABC*ACD*ADE*AEF$$

HARDWARE CONFIGURATION



AVAILABILITY BLOCK DIAGRAM OF VITAL FUNCTIONS



Contents

Part 2
Questionnaire on availability
Summary Report

1. INTRODUCTION

A great number of computerized control systems have been put into operation all over the world during the last decades. They represent the use of computers on various hierarchical positions in power generation, transmission and distribution. They also represent a variety of technical designs from complex multicomputer configurations with hundreds of stations connected to the control system to the use of a single computer with only a few stations connected.

Experience shows that a good functional specification and system design including hardware, software and data base plays a large role in a successful control system project. A qualified design also provides the basis for the availability performance of the operational system at the required level. The main justification for introducing control systems is enhanced power system security. Therefore it is very natural to discuss availability related to the control system.

Working group 01 of Cigre Study Committee 35 has been carrying out a study on the availability of Telecontrol Systems and has produced a report and a questionnaire. The questionnaire was sent to all SC35 members in early 1987 so that they could distribute it to the power companies in their own country. Working group 01 has received 30 replies from 15 countries. The replies to the questionnaire were supplied by the following countries:

Australia	2
Austria	2
Belgium	1
Brazil	7
Denmark	1
Finland	2
France	1
Ireland	1
Italy	1
Japan	2
The Netherlands	2
Spain	4
Sweden	1
The United Kingdom	1
The United States	2

Although we did not get a 100 % response we feel that the replies we received cover a broad cross section and to a lot of cases give extremely detailed and comprehensive answers.

The objective of the questionnaire was firstly to gather data in order to be able to overview the maintenance arrangements in the power companies and utilities and secondly to set up a guide for the designers of telecontrol systems as far as availability and maintenance are concerned.

This paper is a summary report describing the results of the questionnaire. The topics covered by the report are the relationship of availability to control system structure and design requirements, discussions of maintenance policy and its follow-up, overview of the questionnaire replies, recommendations based on operating experience and finally discussions of future development trends.

2. CONTROL SYSTEM STRUCTURE

The configuration of the control system is always structured hierarchically because of the structure of the power system itself. Typical hierarchical levels can be recognized in the control system as follows:

- National
- Regional
- District
- Station

The configuration of the control system is also distributed, i.e. it is geographically widespread. On every hierarchical level three subsystem parts can be identified; the local power system interface, the communication system, and the control centre system. In this study the local system and the communication system are not examined in greater detail. The main attention has been paid to the central system due to its key role in the current operation of a power system.

A central system comprises the equipment in the control room (i.e. the man-machine equipment) and the central computer systems. The main task of the central system is to collect data received from the power system, analyze it and present the results to the operator. The most common computer system configuration classes are; single or nonredundant configuration, and double or redundant configuration. The different configuration classes have been generated by the different demands of the utilities. Typically a national and regional control system needs a redundant computer system configuration while a district control system having less onerous availability requirements includes only a single computer.

3. DESIGN REQUIREMENTS

The operator is responsible for the operation of the power system. The operator must be able to make decisions on the basis of the information received from the central system. The demands placed on the central system by the operator form the basis of the whole control system design. The fundamental requirements are:

- System performance (response time)
- Availability
- System maintenance

The system performance can be defined as the time from the instant the function is requested until the output is available. The system performance is obtained by correct system design of both hardware and software (computer architecture, operating system, database, software structure).

The availability of the system is the probability that the system is able to perform correctly one or more required functions under stated conditions when required. The availability requirement arises from the fact that the central system should always be in operation. A high availability requirement means duplication of the equipment so that at least one component is in an operable state.

The requirement on system maintenance and development is that the system must be so designed that the hardware and the software can easily be maintained and updated. During the lifetime of the control system it has to be maintained and adapted to the changes in the power network and to new functional requirements. System maintenance comprises in general three tools, e.g. facilities for hardware tests and maintenance, tools for data, display and report generation, and programs for software development. The user of these tools can be a hardware maintenance engineer, a system engineer, a hardware manufacturer or a system manufacturer depending on a power company's maintenance policy.

4. MAINTENANCE POLICY

A maintenance and support organization must be provided in order to maintain and repair the control system. The structure and facilities of a maintenance organization should have a capability which allows it to deal adequately with all types of system failures.

In the control system which usually covers a large area the staff and facilities are of necessity situated in a number of different locations. In general we can recognize a central maintenance section and district maintenance sections in every power company. In addition the operational staff of a control system are used to perform first line maintenance functions.

The staff of the central maintenance section are engineers and technicians. They are fully trained specialists to deal with problems at great depth and are responsible for preventive maintenance, repair of the control system in the case of complicated failures, repair of faulty units and for dealing with the manufacturers of the power control system. Usually the central maintenance section also holds the central stock of spares and organizes the return of faulty units and sub-assemblies to manufacturers.

The maintenance of the central station software is typically carried out by separate group of a central maintenance section or by specialists of a software manufacturer. In many companies the software maintenance group is the same one which has specified and commissioned the power control software during the manufacturer's delivery phase. This group has thus a thorough knowledge of all software details and the capability to utilize the manufacturer's software tools.

The staff of the district maintenance section are technicians and other professional technical experts. The district maintenance sections are able to clear all faults in RTUs, central station equipment and telecommunication equipment by line replaceable units and sub-assemblies. They are responsible for a fault localization and a repair of the control system by changing faulty units. The district maintenance sections are fully equipped with an adequate amount of spares.

Normally the staff do not repair faulty units but instead return the units to the central maintenance section. With regard to the control software the district maintenance section is usually involved in the most basic tasks such as loading programs, modifying displays and reports, changing database parameters and running diagnostic programs in an attempt to localize system failures.

The operational staff are used to perform basic maintenance tasks in all maintenance sections. These include configuration changes in redundant parts of the control system and fault localization, under instruction from the specialized maintenance staff. The operational staff also maintain certain database parameters which need changes in the day to day power system operation.

5. FOLLOW-UP POLICY

It is essential to have a method of monitoring the control system in its real time operation and to determine the operative performance of the control system.

The automatic on-line or off-line monitoring is continuous for all vital units. This is valid for all types of units in the entire system configuration, those normally in use as well as redundant ones. The true figures for the availability can only be obtained over the lifetime of the control system. If these figures show that the availability falls out with acceptable limits then appropriate steps should be taken to determine the causes of this and examine what actions should be taken to rectify the problems.

The methods of determining equipment failures are:

- Observation by the operators
- Automatically by the telecontrol equipment
- As a result of testing

In a lot of failure cases the operators are able to tell if a system operation is correct or not before the alarm generated by the equipment has been presented to them. The major failures should always be detected automatically and the operator be warned of the situation by an alarm.

Some failures need the use of systematic testing procedures to be carried out. A representative sample of system functions are tested at a time. Recording can be manual or automatic. All faults detected by the operators should be recorded manually by them on a control centre system. All faults which are detected automatically should be recorded automatically by a control centre system.

Availability statistics should be prepared on a periodic basis - weekly, monthly and yearly. These should be compared to the figures specified for the system in the design phase. The statistics should cover both major and minor faults and the figures should be split into different subsections such as the control centre equipment, the communication equipment and the RTUs.

6. OVERVIEW OF REPLIES

6.1. Question 1

All the respondents did answer this question with regard to the responsibilities at each level but only a few of them included a diagram of the Power System Control system configuration and/or the Hardware configuration at each level.

Most of the countries that replied gave information on a multi-level Control System although in four cases the answers applied to a single level system. Of the others fifteen gave results for a two level system, nine for a three level system and one for a four level system.

A number of systems were fully arranged hierachically. In some cases all the telecommand functions are carried out at the lower levels whereas in other cases the telecommand functions are carried out on all levels. Functions such as AGC, State Estimation, Economic Dispatch etc. are generally carried out only on the highest level.

Every system that was detailed had a dual Computer System normally with each system having a Main and a Front End Computer. The MMI usually consisted of a number of work stations which all had two or three colour monitors and a keyboard. There were also two or more hard copy devices and a Mimic Diagram in the Control Centre. In only one case was the Mimic driven independently from the computer system.

6.2. Question 2

Most of the answers included information on the Availability Requirements but everyone did not deal with it from the same point of view. In a number of cases the information was so extremely detailed that it was difficult to interpret while in other cases it was very basic giving only a global system or Control Centre figure. Therefore it is very difficult to compare the availability requirements between power companies. The availability requirements lie usually between 98.0 - 100.0. The availability requirements seems to be almost the same on all levels of the power system control hierarchy.

6.3. Question 3

About half of the answers included Availability diagrams. These came mainly from the users who have systems that are fully operational.

Of the 30 answers 17 gave no Availability Diagrams, some said that none were available, others said that they did not use them. One answer said that they were not available yet.

Of the 13 answers that were provided one was extremely simplified and it looked as if it had been provided purely in response to the questionnaire. The other twelve on the other hand were much more detailed, eight exceedingly so.

6.4. Question 4

Most of the answers included detailed information on the distribution of the Maintenance functions. The Maintenance arrangements vary widely from company to company with some companies doing virtually all the Maintenance themselves while others leave most of it to the System Manufacturer or the Hardware Supplier. Most of the companies fall somewhere in the middle. Local circumstances, e.g. distances, organization structure and the availability of local outside maintenance services are perhaps the main reasons for the wide variation in maintenance arrangements.

6.5. Question 5

It is obvious that at the present none of these systems employ a completely automated reporting procedure. Very few of the replies gave any information as to the intervals used for producing fault summary reports. It is obvious that most of the systems studied in the questionnaire have been commissioned in the late 70's or in the early 80's and therefore did not include self-diagnostic functions either in hardware or in software.

6.6. Question 6

Virtually all of the answers included detailed information on the Maintenance Organization including details of the numbers of personnel, their distribution and their qualifications. Details of how faults occuring after normal hours are dealt with were given along with the relationship with the suppliers and how spare parts are organized and located. Answers are presented in Appendix 1.

6.7. Question 7 In a lot of cases details of the "actual" results achieved were given and a few of the answers also put forward recommendations for improving the present Availability Figures. The actual availability numbers compared to the required ones are obviously difficult to interpret between companies because everyone has not dealt them from the same point of view. The availability numbers may also be kept as company confidential. Therefore the answers should be seen more as informative data than as a design guide. Detailed results are given in Appendix 1.

7. CONCLUSIONS

Using the information contained in the replies it is possible to put forward the following recommendations which will assist the User in achieving and maintaining a high Availability figure. They fall into four different categories as follows:

7.1. System Specification

- A good accurate system specification.
- A modular system design with good documentation.
- A fully automatic changeover system to cater for system failures should be provided.
- Fully duplicated separate power supplies should be available.
- As far as possible memory resident rather than disk resident programs should be used.
- The system should be expandable to allow new functions and/or extensions to the controlled network to be incorporated easily.

7.2. System Testing and Installation

- Very thorough extensive and meticulous factory testing using carefully detailed test procedures.
- All faults and errors found during the testing should be corrected before delivery.
- All the Ancillary services (eg. Air Conditioning, Power Supplies etc.) should be available before completing the Installation and Commissioning.

7.3. Maintenance

- Well trained and qualified maintenance staff with good system documentation available.
- Adequate supplies of spare parts should be available at the right time and in the right place. If the User is undertaking his own maintenance then spare parts at both the module and the component level should be readily available.

- A modular system design with well documented fault finding procedures.

- No "unnecessary" preventive maintenance should be undertaken.

- Clearly defined lines of responsibility for the equipment between the maintenance and operational staff should be established and adhered to.

- Adequate security for Software maintenance (eg. passwords etc.) should be provided.

- Comprehensive and reliable on-line software diagnostics should be available and the maintenance staff should be thoroughly familiar with their use.

7.4. Software

- The maximum use should be made as far as is possible of standard widely used Software packages rather than using ones that are dedicated to the specific system.

- Selective and Reliable on-line diagnostics should be available.

- The following software maintainability criteria should be observed:

  Top down design
  Structured Programming and Documentation
  Modular Programs
  High level Languages
  Standard Communication Procedures
  Segregation between Code and Data
  Flexible Database Structure

8. FUTURE TRENDS

The operation of power systems will be more and more dependent on the telecontrol systems. This means increasing demands on the availability of telecontrol systems. A total outage time of a few minutes will be required.

A local network concept will be utilized in control centre configurations as well as standardized (OSI) communication concepts in data communication between control centres.

New software tools (C-language) will be adapted when designing software packages for tomorrow's control systems. This opens up better structures and easier maintenance of control system software but requires still higher educated staff.

New technology will improve the availability of the control systems and allow more automatic means of supervising telecontrol systems thus improving the overall availability of a power system operation.

9. ATTACHMENTS

Appendix 1 - Analysis of Replies

Appendix 2 - Questionnaire

Appendix 3 - Definitions

Appendix 4 - Abreviations

Appendix 1

Analysis of Replies

REPLY SUMMARIES:

1. AVAILABILITY
(QUESTIONS 2 AND 7)

2. ORGANIZATION AND FOLLOW-UP
(QUESTIONS 5 AND 6)

3. PREVENTIVE MAINTENANCE HW
(QUESTION 4 A)

4. CORRECTIVE MAINTENANCE HW
(QUESTION 4 B)

5. CORRECTIVE MAINTENANCE SW
(QUESTION 4 B)

6. ADAPTIVE AND ENHANCING MAINTENANCE
(QUESTIONS 4 C AND 4 D)

REPLY SUMMARY: AVAILABILITY

REPLY NO.	REQUIRED AVAILABILITY			ACTUAL AVAILABILITY			REMARKS
	1ST LEVEL	2ND LEVEL	3RD LEVEL	1ST LEVEL	2ND LEVEL	3RD LEVEL	
1	99.6	99.6	-	100	100	-	
2	NA	NA	-	99.9	99.9	-	
3	-	-	99.0	-	-	99.3	
4	-	100	100	-	100	100	
5	-	99.99	-	-	NA	-	
6	-	-	-	-	-	-	NA
7	-	-	-	-	-	-	NA
8	-	-	-	-	-	-	NA
9	99.9	-	99.9	NA	-	NA	
10	99.9	99.9	99.9	NA	NA	NA	
11	99.8	-	-	99.45	-	-	
12	99.8	-	-	99.93	-	-	
13	99.95	-	-	NA	-	-	
14	99.9	99.9	-	99.97	99.98	-	
15	-	99.95	-	-	99.94	-	
16	-	100	-	-	99.95	-	
17	99.95	-	-	99.98	-	-	
18	99.95	99.95	99.99	99.75	99.88	NA	
19	-	99.99	-	-	99.90	-	
20	99.97	99.97	-	99.99	100	-	
21	-	-	-	99.95	-	-	
22	99.98	-	-	NA	-	-	
23	99.95	-	-	99.90	-	-	
24	99.99	99.99	-	99.51	99.92	-	
25	99.9	-	-	99.51	-	-	
26	-	-	-	99.95	99.88	-	
27	99.59	99.59	-	NA	NA	-	
28	99.9	99.9	-	99.98	99.99	-	
29	NA	NA	-	99.69	99.69	-	
30	98.0	99.5	-	99.2	99.5	-	

REPLY SUMMARY: ORGANISATION AND FOLLOW-UP

REPLY NO.	ORGANI-SATION		NUMBER OF STAFF			FOLLOW-UP		REMARKS
	CENT.	DEC.	ENG.	TECH.	OTH.	AUTO	MAN.	
1	x	x	4	6			x	
2	x	x	2	5	17		x	Three (3) systems
3	x		2		24		x	
4	x		4				x	
5	x	x	4	6	5	x	x	
6								NA
7		x	4			NA		
8	x		4	11		x		
9	x		NA			x		
10								NA
11	x		8	4			x	
12	x	x	NA				x	
13	x		4	8			x	
14	x	x	4	8	16	x	x	SW mainten. incl.; 7 systems
15	x		2	1			x	
16	x	x	18	5			x	7 systems
17	x	x	6			x	x	
18	x	x	12	25		x	x	Nine centers
19	x	x	2				x	In each control centre
20	x	x	1-3			x	x	In each control centre
21	x		6			x	x	
22	x		5				x	
23	x		4			x		
24	x		2	13	8		x	
25	x		10			x		
26	x			2	3	x	x	
27		x	5				x	
28	x	x	4			NA		
29	x		14	22			x	
30	x	x	25	10			x	

REPLY SUMMARY: PREVENTIVE MAINTENANCE HW

REPLY NO.	1ST LEVEL			2ND LEVEL			3RD LEVEL			REMARKS
	U	SM	HWS	U	SM	HWS	U	SM	HWS	
1	x	x		x	x					
2		x			x					System just commissioned
3					x	x				
4		x	x		x	x				
5	x		x	x		x	x		x	
6										NA
7	x			x						
8				x			x			
9	x			x						
10										NA
11	x									
12	x									
13	x	x								
14	x			x						
15				x						
16	x		x	x		x				
17	x		x							
18	x		x	x		x	x		x	
19					x	x				
20		x	x		x	x				
21				x		x				
22	x	x								
23	x									
24	x			x						
25	x									
26	x		x	x		x				
27										NA
28	x	x	x	x	x	x				
29	x	x		x	x					
30										NA

REPLY SUMMARY: CORRECTIVE MAINTENANCE HW

REPLY NO.	1ST LEVEL			2ND LEVEL			3RD LEVEL			REMARKS
	U	SM	HWS	U	SM	HWS	U	SM	HWS	
1	x	x		x	x					
2	NA			NA						System just commissioned
3					x	x				
4										NA
5	x		x	x		x	x		x	
6										NA
7	x			x						
8			x			x				
9	x			x						
10										NA
11	x									
12	x									
13	x	x								
14	x			x						
15				x	x					
16	x		x	x		x	x		x	
17	x		x							
18	x		x	x		x	x		x	
19					x	x				
20		x	x		x	x				
21				x		x				
22	x	x								
23	x		x							
24	x	x	x	x	x	x				
25	x	x								
26	x		x	x		x				
27										NA
28	x	x	x	x	x	x				
29	x	x		x	x					
30										NA

REPLY SUMMARY: CORRECTIVE MAINTENANCE SW

REPLY NO.	1ST LEVEL			2ND LEVEL			3RD LEVEL			REMARKS
	U	SM	HWS	U	SM	HWS	U	SM	HWS	
1	X	X		X	X					
2		X		X						
3					X					
4	X			X						
5		X	X		X	X		X	X	
6										NA
7	X			X						
8	X		X	X		X				
9	X			X						
10										NA
11	X									
12	X									
13	X	X								
14	X			X						
15				X	X					
16	X			X	X		X			
17	X	X	X							
18		X			X			X		
19				X	X					
20	X	X		X	X					
21				X	X					
22	X	X								
23	X	X								
24	X	X		X	X					
25	X									
26	X	X		X	X					
27										NA
28		X			X					
29										NA
30										NA

REPLY SUMMARY: ADAPTIVE AND ENHANCING

REPLY NO.	1ST LEVEL			2ND LEVEL			3RD LEVEL			REMARKS
	U	SM	HWS	U	SM	HWS	U	SM	HWS	
1	x	x		x	x					
2	x	x		x	x					
3					x					
4										NA
5	x	x		x	x		x	x		
6										NA
7	x			x						
8	x	x		x	x					
9	x			x						
10										NA
11	x									
12	x									
13										NA
14	x			x						
15				x	x					
16	x			x	x		x			
17	x	x	x							
18	x	x	x	x	x	x	x	x	x	
19					x					
20		x			x					
21				x	x					
22	x									
23	x									
24	x			x						
25	x	x								
26	x	x	x	x	x	x				
27										NA
28	x	x		x	x					
29	x			x						
30										NA

Appendix 2

Questionnaire

QUESTIONNAIRE ON THE AVAILABILITY OF CONTROL CENTRES

The growing use of computerized control systems for power networks has increased the importance and interest of their availability performance and maintenance arrangements. Therefore Study Committee 35/WG01 has undertaken to review the status concerning availability and maintenance efforts in the power companies and utilities.

The objective of this questionnaire is first to gather data in order to be able to overview the maintenance arrangements in the companies. Second and final objective is to set up a guide for the designers of telecontrol systems as far as the availability and maintenance are concerned.

Below you will find a set of questions intended to clarify the state of the art in your company. Please give your answers as small notes limited to 5-10 printed lines for each question. If the small notes are not enough for your presentation please use diagrams or the tables attached to this questionnaire.

Q1: SYSTEM CONFIGURATION

The main layout of the power system control organisation e.g.

- Dispatching centre (1ST LEVEL)
- Remote control centre (2ND AND 3RD LEVEL)

Please list and describe by using the table Q1 the functions and the main responsibilities at each level e.g.

Function	1ST LEVEL	2ND LEVEL
Telecommands		X
Telemetering		X
Teleindication		X
Reporting	X	X
Load flow	X	
State estimator	X	
Economic load dispatch	X	
etc.		

Please show diagrammatically the hardware configuration at each level and indicate the back-up facilities that are available. In addition indicate the number of RTUs and the power supply arrangement at each level.

Q2: AVAILABILITY REQUIREMENTS

Please list the specified user's requirements at each control centre e.g. the availability figure or the number of failures per year and mean down-time for vital (major) and nonvital (minor) functions by using the Table Q2 and assuming that all other parts outside of control centres such as RTUs and communication channels are always available.

Q3: AVAILABILITY DIAGRAMS

Please show for each control centre the availability diagram of vital (major) functions indicating for each unit or sub-system the reliability figure.

Please refer to the example given in Appendix A.

Q4: MAINTENANCE FUNCTIONS

Please list the functions which are in use in your company and at which levels they are available

A. Preventive (Hardware)

B. Corrective (Hardware, Software)

C. Adaptive (e.g. modification of displays and data base content using the existing hardware and software facilities)

D. Enhancing (e.g. augmentation of telecontrol functions)

Please use the Tables Q4A, Q4B and Q4C.

Q5: FOLLOW-UP FUNCTIONS

Please describe briefly your follow-up and reporting system for maintenance functions at each level and indicate if it is carried out automatically or manually.

Q6: MAINTENANCE ORGANISATION

Please describe and list your maintenance organisation

A. Centralised/Distributed

Please refer to the example given in Appendix B.

B. Number of personnel involved in control centre maintenance

- Number of people
- Number of full-time equivalent people

C. Educational background

D. How do you deal with failures occuring out with normal working hours?

- Technical qualifications

E. Manufacturer's support

F. Spare part organisation

Q7: ACTUAL RESULTS AND RECOMMENDATIONS

A. Please indicate actual availability results using the Table Q7.

B. Recommendations for improving availability?

TABLE Q1

NAME OF FUNCTION	DESCRIPTION	1ST LEVEL	2ND LEVEL	3RD LEVEL

TABLE Q2

NAME OF FUNCTION	1ST LEVEL	2ND LEVEL	3RD LEVEL	AVAIL. FIGURE	MEAN NR. OF LOSSES PER YEAR	MDT (HOURS) PER LOSS	REMARKS

TABLE Q4A

NAME OF FUNCTION	1ST LEVEL	2ND LEVEL	3RD LEVEL	USER	SYSTEM MANUF.	HW SUPPLIER	REMARKS
PREVENTIVE (HW) - CPU + memory - Discs - Printers - VDUs - Keyboards - Mimic Board - Power Supply - Modems - Others							

TABLE Q4B

NAME OF FUNCTION	1ST LEVEL	2ND LEVEL	3RD LEVEL	USER	SYSTEM MANUF.	HW SUPPLIER	REMARKS
CORRECTIVE (HW)							
- CPU + memory							
- Discs							
- Printers							
- VDUs							
- Keyboards							
- Mimic Board							
- Power Supply							
- Modems							
- Others							
CORRECTIVE (SW)							
- Operating System							
- Data Acquisition							
- M/M Software							
- Data Base Management							

TABLE Q4C

NAME OF FUNCTION	1ST LEVEL	2ND LEVEL	3RD LEVEL	USER	SYSTEM MANUF.	HW SUPPLIER	REMARKS
APAPTIVE AND ENHANCING - Modification of existing displays - Addition of new displays within available space - Adding or deleting data from existing RTUs - Modification of data from existing RTUs - Adding a new remote control centre - Adding new RTUs - Adding new devices e.g. VDUs, printers, etc. - Modification of data base structure - Adding new functions e.g. state estimation or economic load displatch							

TABLE Q7

NAME OF FUNCTION	1ST LEVEL	2ND LEVEL	3RD LEVEL	REQUIREMENTS			RESULTS			REMARKS
				AVAIL. FIGURE	MEAN NR. OF LOSSES PER YEAR	MDT (HOURS) PER LOSS	MTTR	ACTUAL AV. VALUE	OBSERV. PERIOD	

APPENDIX A-1

EXAMPLE OF AVAILABILITY DIAGRAM

HARDWARE CONFIGURATION

The Hardware Configuration of the Control System considered for the Availability Diagram is shown in Appendix A-3. The Line Buffer Units are responsible for the communication with the RTUs.

The Computer System is a dual system with one acting as the Primary and the other as the Secondary System on 'Hot' Standby. Each Computer System consists of a Main Computer (MC) with the relevant Disks (DK) and a Front End Computer (FE).

The Man-Machine Interface consists of two consoles each one equipped with two VDUs and a Keyboard (KB) and two Printers (PTY). in addition there is a Mimic Board giving an overview of the network.

AVAILABILITY ANALYSIS

The Availability Block Diagram for the Control System shown in Appendix A-1 is given in Appendix A-2. The Block Diagram relevant to the 'vital' functions is based on the following concepts:-

- (n-1) LBUs out of n LBUs must be operative
- at least one FE must be operative
- at least one MC with the relevant Disks must be operative
- the switch between the MCs and the Man-Machine Interface must be operative
- at least one Console with at least 1 out of 2 VDUs must be operative
- at least one printer must be operative
- the presentation on the Mimic Board and the transmission to other Control Centres are considered as 'non-vital' functions.

AVAILABILITY COMPUTATION

ALBU = Availability of each LBU

AFE = Availability of FE1, FE2

AMC = Availability of MC1, MC2

ADK = Availability of DK1, DK2

ASW = Availability of the switch

AKB = Availability of each keyboard

AVDU = Availability of each VDU

APTY = Availability of each printer

The availability from A to B is:-

$$AAB = 1 - (1 - ALBU^{n-1})^{n}$$

The availability from B to C is:-

$$ABC = 1 - (1 - AFE*AMC*ADK)^{4}$$

The availability from C to D is:-

$$ACD = ASW$$

The availability from D to E is:-

$$ADE = 1 - \langle 1 - AKB*\{1 - (1 - AVDU)^{2}\}\rangle^{2}$$

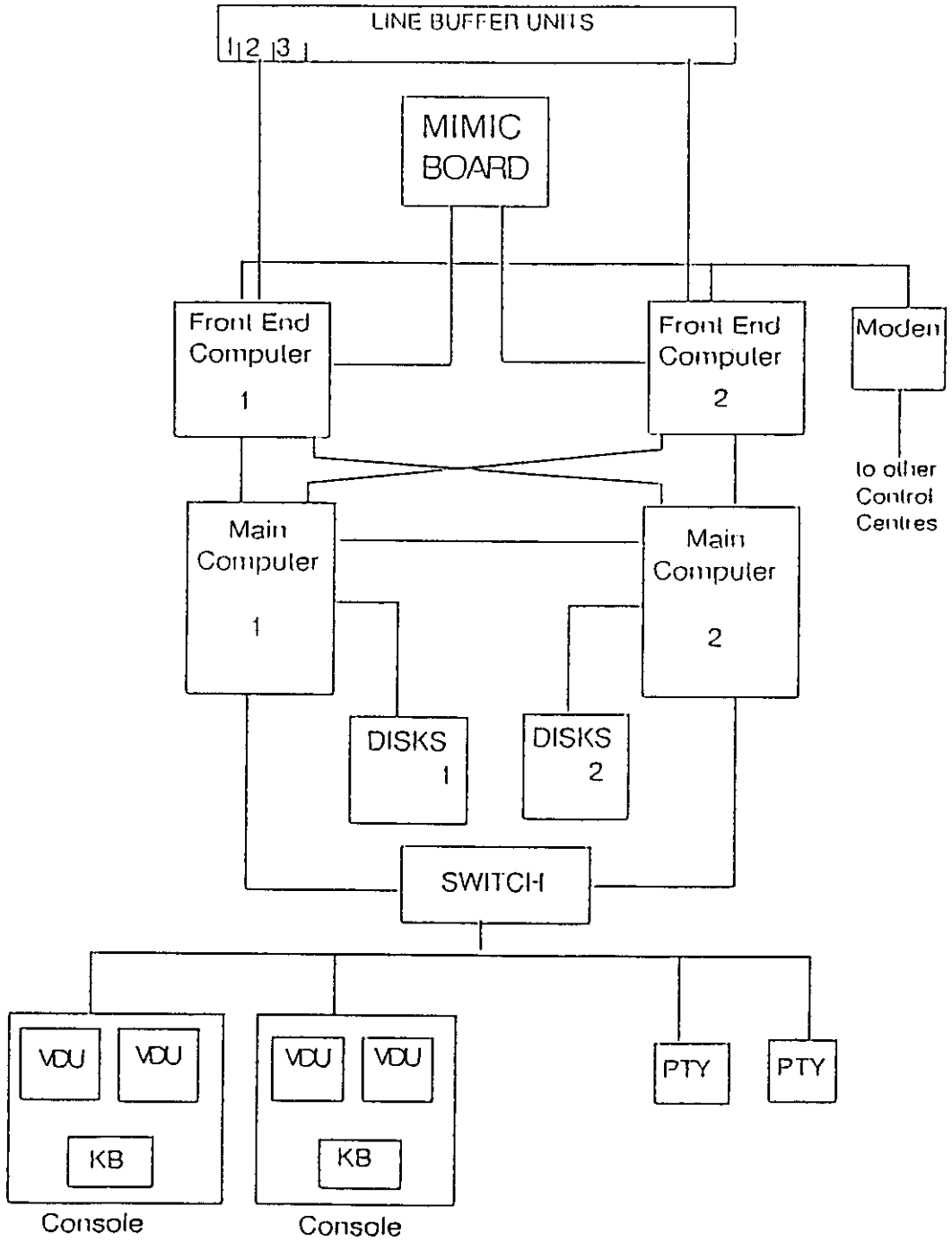
The availability from E to F is:-

$$AEF = 1 - (1 - APTY)^{2}$$

The availability figure for the vital functions of the Control System is:-

$$ATOT = AAB*ABC*ACD*ADE*AEF$$

HARDWARE CONFIGURATION



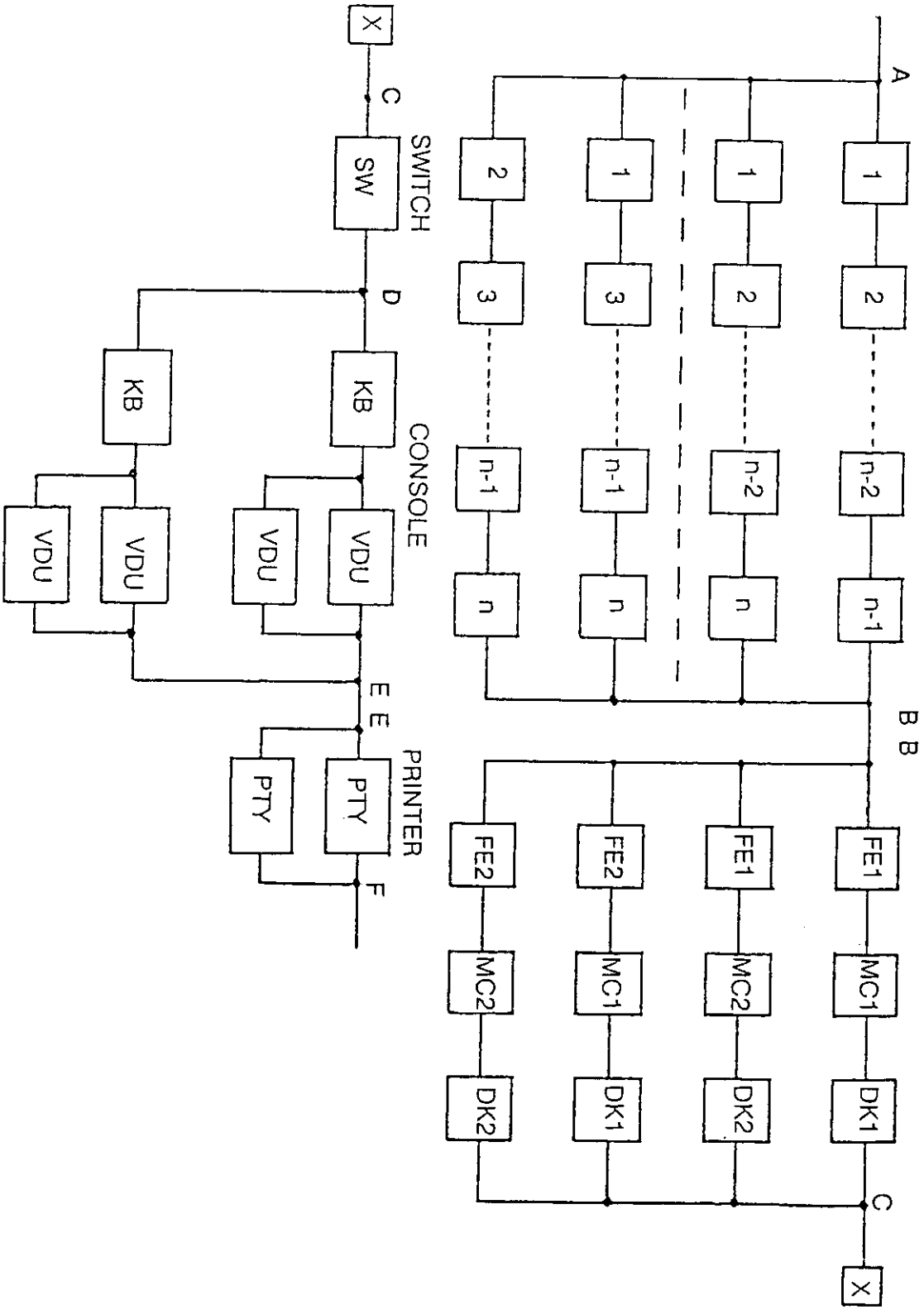
Part 2
Questionnaire on Availability

Summary Report

Study Committee 35
(Communication and Telecontrol)

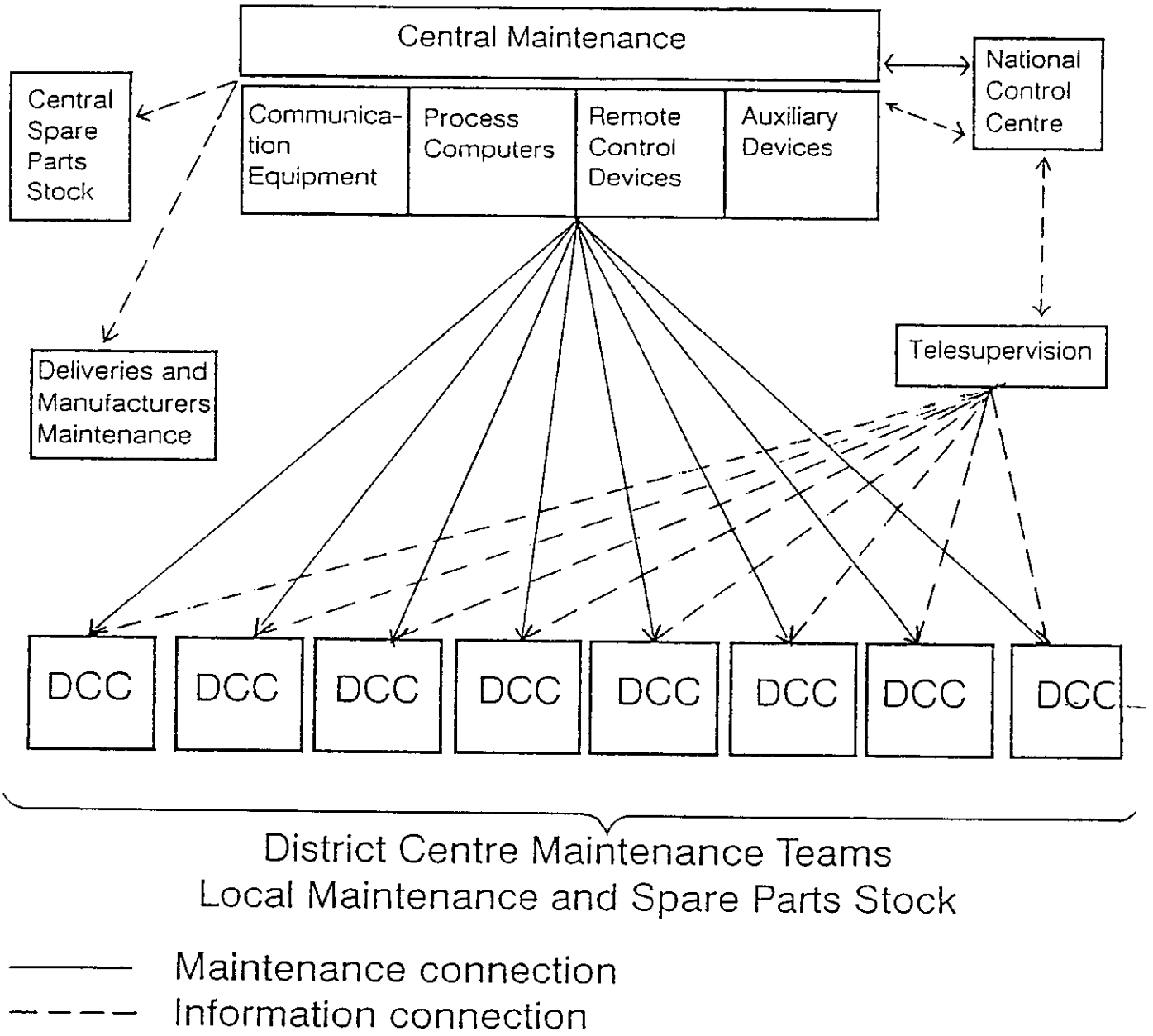
Working Group 01
(Control Centres)

AVAILABILITY BLOCK DIAGRAM OF VITAL FUNCTIONS



APPENDIX B

MAINTENANCE ORGANISATION (EXAMPLE B)



MATHEMATICAL DEFINITIONS

AVAILABILITY

The availability of a system characterises its ability to perform the intended function at any given moment.

The essential difference between this and the concept of reliability is that reliability concerns operations over a given period while availability concerns operation at a given instant.

Availability can be stated as:-

$$A = \text{uptime}/(\text{uptime} + \text{downtime})$$

Downtime in the above equation normally includes corrective maintenance preventive maintenance and System expansion downtimes if such times compromise the user's ability to operate apparatus normally controlled by the equipment being expanded.

For design analysis and to determine an 'a priori' prediction of availability for sub-assemblies and units the following equation utilising MTBF and MTTR shall be used.

$$A = MTBF/(MTBF + MTTR), \text{ where}$$

A = Predicted Availability of a component.

The equation for A and the combinatorial equations associated with parallel redundant components (or sub-systems) are valid under the following conditions:-

(a) The failure of any component within a string or parallel set is independent of the failure of any other component. In other words component failures do not propagate failures of other components.

(b) Sufficient repair facilities and standby replacement parts are available in order to handle multiple simultaneous failures.

It is possible to specify the availability for each of the specific functions. However when trying to specify availability figure for the whole system a difficulty arises in judging which functions are essential for the whole system or not essential.

The impact of the outage of each system element or function on the availability of the total system should be mutually agreed upon between the user and the supplier.

RELIABILITY

Reliability is defined as a measure of an equipment's or system's ability to perform its required function under specified conditions for a specified period of time. It is a probability figure based on failure data and length of operating time. The reliability of system components is reflected in their respective mean-times-between-failure (MTBF) numbers. This 'figure of merit' is used in the calculation of the system availability

where $$R = e^{-\frac{t}{MTBF}}$$

MTBF = mean time between failure
t = the specified time interval

and

$$MTBF = \frac{I}{\sum_{i=I}^{n} \lambda i}$$

where λ_i = the failure rate of the components

MAINTAINABILITY

The maintainability of equipments or systems is reflected in their respective mean-time-to-repair (MTTR) number. MTTR values may include:-

(a) Administrative time - the time interval between failure of a component and a call for maintenance service.

(b) Transport time - the time interval between the call for maintenance service and the arrival at the station of a maintenance technician and the necessary replacement parts.

(c) Repair time - the time required by a trained maintenance technician having the replacement parts and the recommended test equipment at the station to return the faulty system to normal operation.

The MTTR values used in availability computations should be based to the maximum extent possible upon maintenance experience.

Appendix 4

Abreviations

RTU	Remote Terminal Unit
AGC	Automatic Generation Control
MMI	Man-Machine Interface
OSI	Open Systems Interconnection
NA	Not Available
U	User
SM	System Manufacturer
HWS	Hardware Supplier

2.3 AVAILABILITY

The Availability of a system is the probability that the system is able to perform correctly one or more required functions under stated conditions when required.

Availability is the capability of the system with respect to Reliability Maintainability and Supportability and of its resources for maintenance and support to prevent the Operative Performance from degrading relative to the ideal Technical Performance.

The Availability is broken down as shown in figure 2. (for the mathematics and definitions see Appendix 2.1).

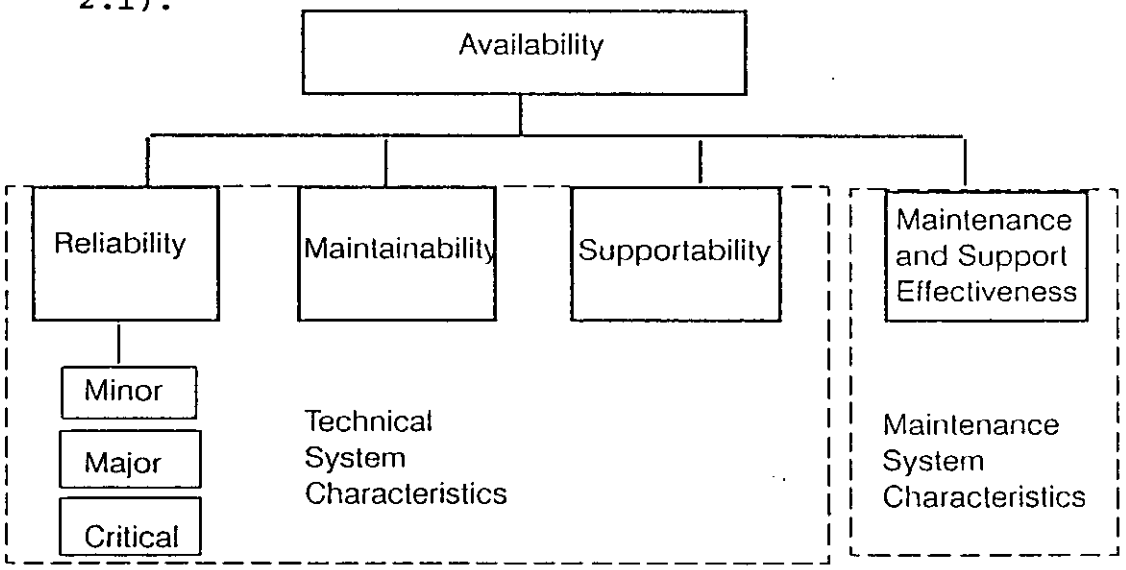


Figure 2 : Availability

2.3.1 Technical System Characteristics

2.3.1.1 Reliability

Reliability of a system is a measure that a system will perform one or more required functions under stated conditions for a stated period of time.

Therefore Reliability is a system characteristic determining the risk and distribution in time of malfunctions (failures faults etc) and deficiencies.

Reliability is related to the MTBF. In the examples that follow only major faults are considered.

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

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