Recommendation T/CS 50-01 (Montpellier 1984)

MAINTENANCE PHILOSOPHY FOR DIGITAL AND MIXED NETWORKS

Recommendation proposed by Working Group T/WG 11 "Switching and Signalling" (CS)

Text of the Recommendation adopted by the "Telecommunications" Commission:

"The European Conference of Postal and Telecommunications Administrations,

considering

— that the existing CCITT Recommendations on maintenance philosophy do not cover the whole network and only deal with some maintenance aspects;

— that there was no common understanding about what maintenance consists of;

— that there was no fundamental and logical description of what maintenance is;

— that system designers must be aware of the fact that maintenance is one of the major cost-factors of the total life time of a system,

recommends

that the members of the CEPT recognise the following considerations."

Table of contents

1. GENERAL

1.1. Introduction

Maintenance has to do with failures.

In a system where failures are not expected, no maintenance is necessary.

So failures are the cause of the maintenance.

The term maintenance covers all the aspects which have to do with failures, such as: supervision, detection, localization, information, repair, etc. All ideas concerning these aspects are contained in the maintenance philosophy.

In order to meet the requirements of availability performance and through that to meet the requirements of network technical performance, various actions related to failures are necessary. The combination of all these actions, with the intention to retain an item in or to restore it to, a state in which it can perform its required function, is defined as maintenance.

Maintenance can be performed according to different principles:

- Preventive maintenance
  The maintenance carried out at predetermined intervals or corresponding to prescribed criteria and intended to reduce the probability of failure or the performance degradation of an item.
- Corrective maintenance
  The maintenance carried out after a failure has occurred and intended to restore an item to a state in which it can perform its required functions.
- Controlled maintenance
  A method for sustaining a desired network technical performance by the systematic application of analysis techniques using centralized supervisory facilities and/or sampling to minimize preventive maintenance and to reduce corrective maintenance.

In general it is proposed for all three network types (analogue, digital and mixed) to use controlled maintenance principles wherever possible, that is to say that the maintenance actions are determined on the basis of information coming out of the system itself or from auxiliary equipment.

The maintenance philosophy in general is such that:
the right person can be sent to
the right place with
the right equipment at
the right time to perform
the right actions

In other words it allows the maintenance personnel to identify failed equipment, to restore the service and to repair the failed equipment.

Furthermore it is important that coherent maintenance principles are applied to the various constituent parts of digital networks (e.g. multiplexers, transmission systems, exchanges, etc.) so that satisfactory equipment interworking is guaranteed, unambiguous failure location is possible and unnecessary activities can be avoided.

To this end "maintenance entities", "failure information" and "means to assist in detecting and locating failures", etc., have been defined.

The maintenance philosophy and thus the maintenance functions are strongly linked to the availability performance parameters of the network, which parameters have to be defined and quantified.

For defintions of concepts and terms used, see Recommendation T/CS 10-13 [1].

1.2. Objectives

New technologies provide new possibilities for the maintenance not only of individual exchanges, but also of the whole network at low cost. The same technology for both transmission and switching will gradually render an in-built system of operation and maintenance possible.

The operation and maintenance functions should be implemented in such a way that the lifecost will be minimum for a stated service level. The total cost of the network consists of
— investment cost,
— operation cost,
— maintenance cost (for failures),
— cost of lost traffic.

It is especially the investment cost, the maintenance cost and the cost of lost traffic which depend on the requirements of availability performance of the network and of the network components and thus on the maintenance functions built-in or in separate equipments and the reliability (failure rate).

The operation cost is dependent on the requirements for the operation of the network and of the network parts and thus also on the operational functions built-in or in separate equipments.

1.3. Overall maintenance philosophy

1.3.1. *Maintenance entity concept*

In the maintenance philosophy, it is assumed that the different equipments of a telecommunication network are interconnected at easily identifiable points at which the interface conditions defined for these equipments apply.

The equipments which occur between two consecutive interfaces constitute a maintenance entity.

In an integrated digital network for example such points may be provided by digital distribution frames. Even in a location where no digital distribution frame is provided, an equivalent point where defined interface conditions apply can normally be identified.
Examples are given in Figures 1 and 2.

In defining the Maintenance Entities (ME) the following aspects are taken into account:

i. When a failure occurs within a network, a maintenance alarm indication must be generated identifying the failed maintenance entity.
ii. A failure occurring in an entity should not cause the generation of alarm indications in other entities.

If these two principles are met then the responsible maintenance personnel will be called into action, and usually no unnecessary maintenance activity will be initiated elsewhere.

Note: Several ME's can be assembled into a maintenance entity assembly (MEA) for operational and Maintenance reasons. Typical applications are digital exchanges, digital circuits and facilities.
ME can also be subdivided into Maintenance sub-entities (MSE) for operational and maintenance reasons. A typical example is a digital line system consisting of line terminals, repeaters and cable sections.

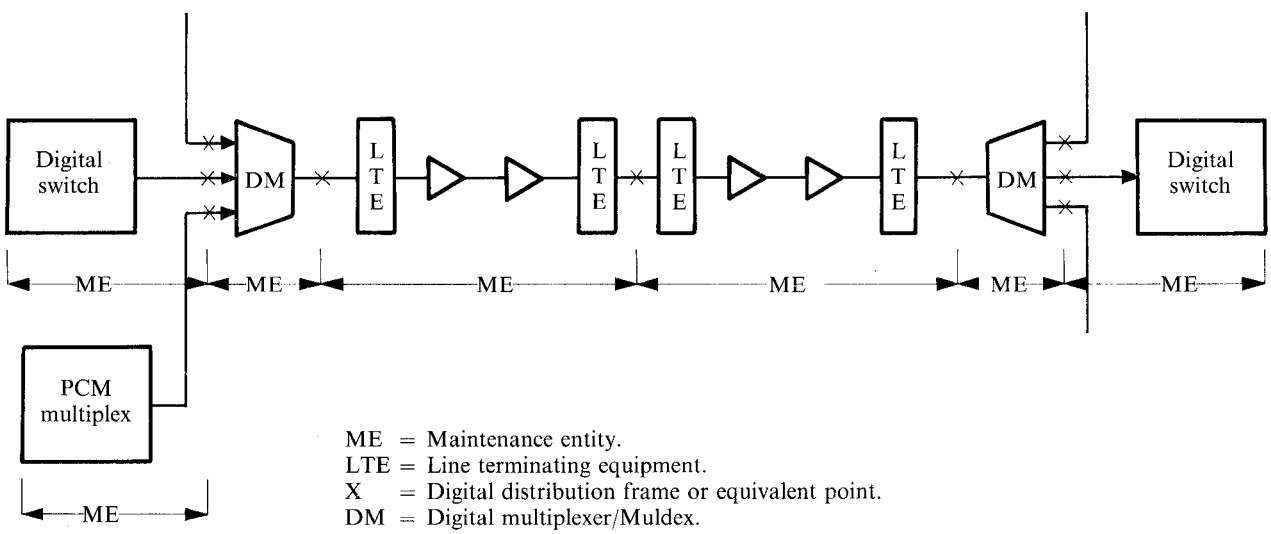
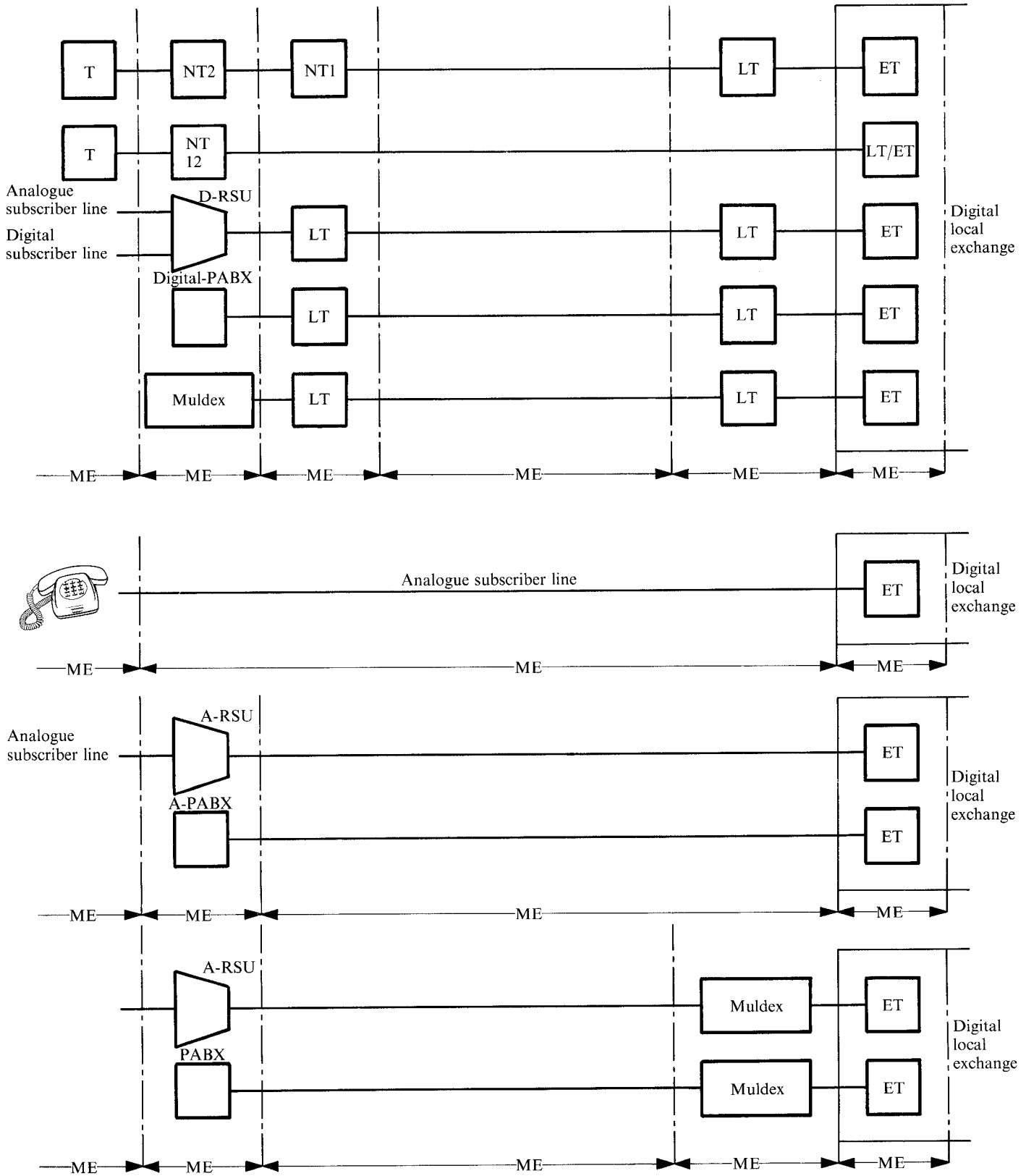


Figure 1. General maintenance entity concept for inter-exchange connections.



ME = Maintenance entity.
A-PABX = Analogue PABX.
D-PABX = Digital PABX.
A-RSU = Analogue remote switching unit.
D-RSU = Digital remote switching unit.

Figure 2. Subscriber's connection divided into maintenance entities.

1.3.2. *Classification of failures*

A failure is defined as the termination of the ability of an item to perform a required function.

The severity of the failure depends on the failure effect. This effect can be related to:

- The network service performance requirements as experienced by the subscribers;
- The probability that multiple failures will occur thus resulting in the deterioration of the performance as seen by the customer;
- Probable loss of revenue to the Administration.

The failures can also be classified according to their importance and consequences on the quality of service provided to the subscribers and on the network technical performance:

- failures which give a complete interruption of service(s) for one or several subscribers;
- failures which give a partial interruption of service(s) (e.g., degradation of transmission quality) to one or several subscribers;
- failures which decrease the availability performance of the equipment and/or the network, but do not affect the subscribers.

Another classification distinguishes between permanent and intermittent failures.

The severity of failures can be determined by measuring the down time, up time and failure rate of the ME. These terms are defined in Recommendations T/CS 10-13 [1] and T/CS 58-01 [2].

2. SUPERVISION

Supervision is a process in which the various functions of the various items in a network are looked at (supervised). This is done for operational as well as for maintenance matters.

For maintenance this supervision process has to include the following functions:

(a) Locating "failed" equipment or the equipment in which a failure is suspected. It is generally carried out by analytical or statistical identification processes.

(b) Report of failures to operating personnel.

(c) Transmission of data to the operating personnel, relating to specific functional features of the network (traffic, state of equipment, particular malfunctions for instance). These data are transmitted systematically or on demand.

(d) To protect the system by transmitting to all the concerned network equipment any necessary information for the automatic initialization of internal or external protection mechanisms, e.g., reconfiguration, traffic re-routing, etc.

3. MAINTENANCE PHASES

3.1. General

After the occurrence of a failure in the network, a number of maintenance phases are required to correct the failure and to protect, when possible, the traffic affected by the failure if it has been interrupted.

Figure 3 lists the maintenance phases which are involved after a failure occurrence in a ME. The parameters determining the different phases are indicated in the figure. It is intended to characterize different maintenance strategies with the aid of the maintenance phases.

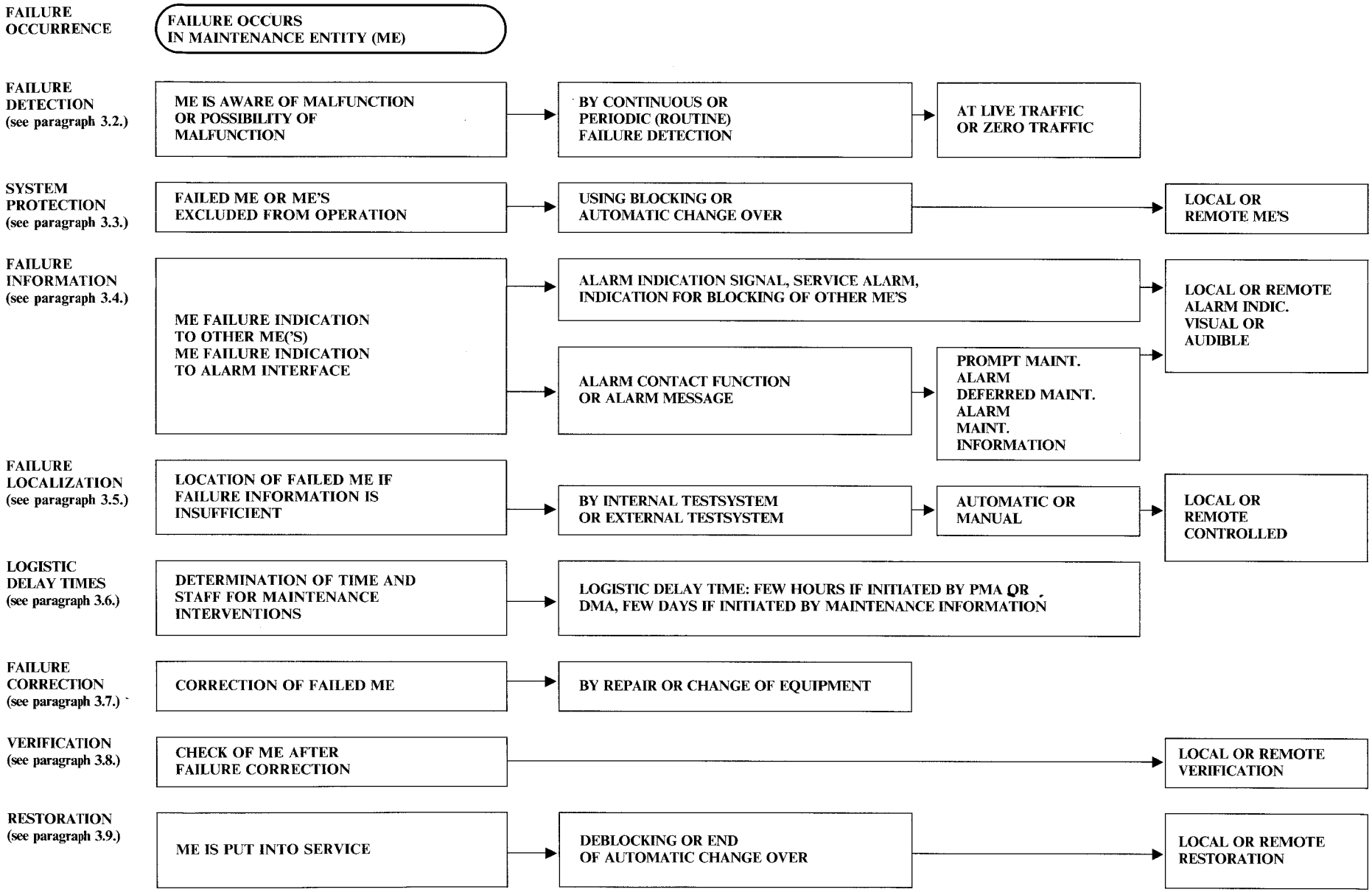


Figure 3. Maintenance phases.

Besides the maintenance phases the following aspects have to be dealt with:
* The recording of all failures = Failure statistics (see paragraph 5.).
* Preventive maintenance (see paragraph 6.).
* Maintenance logistics (see paragraph 4.).

3.2. Failure detection

3.2.1. *Introduction*

The discovery of failures must take place so quickly and with such security that the stated service demands are fulfilled.

Failures should be discovered by the telephone company, independent of and preferably before the subscriber, i.e. the majority of failures are both detected and remedied without the subscriber having been aware of the failures.

Different types of failure detection mechanisms can be used as follows:
(a) continuous checking;
(b) routine or periodic testing;
(c) checking under zero traffic conditions;
(d) checking of behaviour under live traffic conditions.

The rules governing the detection mechanism must be defined for a system, since intervention by the operating personnel should not be necessary. Under some conditions, however, personnel may control certain operations e.g. for periodical or casual checking, such as
— modifying the priority level of a checking process,
— modifying the nominal period in the case of a periodical checking,
— carrying out certain partial or recurrent checking (e.g. test on demand).

The choice of a particular detection mechanism depends on the performance requirements i.e. the "quality of service" as seen by the subscribers, the technical network performance and the nature of the equipment.

In addition, several mechanisms may be required in the same item.

3.2.2. *Continuous checking*

All the time an item is active, it will be checked for good performance.

If the item does not fulfil the test requirements it is considered to have failed.

3.2.3. *Routine or periodic testing*

Items will be tested periodically, either initiated by the system or initiated by the maintenance staff.

The frequency of the test depends on the importance of the item, the failure rate and the number of items of that type present in the element.

3.2.4. *Checking under zero traffic conditions*

Casual checking when traffic is nul, once a process is over, when a process has been initiated several times, for instance checking the coherence of n-plicated data, testing the equipment operation, using internal or external programs.

3.2.5. *Checking under live traffic conditions*

The checking of the behaviour under live (traffic) conditions can be
(a) analytical or
(b) statistical.

Type (a) e.g.:
If the checking mechanism in the item itself indicates that the performance of the item is faulty (parity fault, no acknowledgement of an action, etc.);

Type (b) e.g.:
The conclusion that an item has failed can be reached on the following statistical grounds, if:
— the number of times the item performs its function "normally" is compared with the number of times the performance of the item does not fulfil its requirements,
— the average time of functioning is compared with standard values,
— the number of times an item performs its function during a certain period.

3.3. Protection of the system

When a failure has been detected the rest of the system must be protected by actions like putting an item "out of service" or "under testing condition", changing to a configuration with minimal or degraded service or changing over to redundant spare units.

3.4. Failure information

3.4.1. *Introduction*

The failure information consists of alarm information transmitted to alarm interfaces for use by the maintenance staff and failure indications transmitted to other parts of the network.

3.4.2. *Alarm information*

The alarm shall be presented

(a) as an indication (e.g. DC signal), and/or

(b) as an alarm message on the man-machine interface.
This message will contain *et al.*:

i) header (name of maintenance entity concerned, date, time, etc.),
ii) category of failure (PMA, DMA, MI),
iii) description of failure,
— cause of failure
— location of the failed-item(s),
— other information which can be useful in locating the failed item(s),
iv) possible consequences of the failure,
v) the automatic actions performed by the network (internal protection and service actions).

3.4.2.1. Prompt maintenance alarm (PMA)

This information has to be generated as a consequence of a failure within an element in a maintenance entity when immediate action by the maintenance staff is necessary, because the system has been disturbed or is in imminent danger of being disturbed and the total performance is prevented or endangered (like S.O.S.). A PMA-signal is necessary for drawing attention to the failure (e.g. with a bell, lamp) and for the case where the man-machine interface is out of order (e.g. computers down, transmission link failed).

3.4.2.2. Deferred maintenance alarm (DMA)

This information has to be generated as a consequence of a failure within an element in a maintenance entity if the risk of total breakdown is small enough to allow maintenance actions to be carried out either directly, if the failure occurs during normal working hours, or later in the next working day, if the failure occurs outside normal working hours. This information will be given in the same way as with PMA.

3.4.2.3. Maintenance information (MI)

This information has to be generated as a consequence of a failure within an element in a maintenance entity when no immediate action by the maintenance staff is required, because the total performance is not in danger.

3.4.3. *Guiding the maintenance action after MI's*

To ensure that the maintenance people take the right action at the right moment in the most efficient way, two possibilities have to be distinguished:

(a) scheduled maintenance,

(b) accumulation of minor failures (MI's).

If a number of failures occur during a certain period in an element, which in themselves are not severe, a point will be reached where the performance of the element is no longer acceptable. Before this point has been reached the maintenance staff must be alerted. See also 3.6.

3.4.4. *"Alarm indication signal" (AIS)*

The information defined in 3.4.2. is necessary for the maintenance staff responsible for the maintenance entity concerned.

In order to avoid unnecessary maintenance action in adjacent maintenance entities, information must be sent to these entities. For this an AIS has to be generated. An "Alarm indication signal" (AIS) is a signal associated with a prompt maintenance alarm concerning a defective maintenance entity, indicating to other non-defective entities that a failure has been identified and that other maintenance alarms consequent to this failure should be inhibited. This AIS is a special pattern of the normal signal.

3.4.5. *Information to the user terminal*

When a failure occurs a user may also be informed.
This can be done e.g. in the following ways:

— By a "Service alarm" from the network where a particular service is either only partially available or completely unavailable.
The "service alarm" (SA) is related to a defect in the transmission between or within equipments in which the service originates and terminates. A "service alarm" is generated by the equipment providing the service, when the performance falls or is likely to fall below a level specified for that particular service. In order to generate a "service alarm" the information stream must be monitored by user-dependent criteria from end to end.

— By a Service action: e.g. in order to interrupt certain applications or transactions a request must be made to postpone some applications. This will lead to degradation and will limit the service provided.

— By giving information related to the state of the network such as routing traffic conditions on some routes, degradation of the quality of the transmission, interruption of some services, etc.

3.4.6. *Information for blocking or automatic change over*

When a failure occurs in a Maintenance Entity it may be better to block the originating (sending) ME(s) for the duration of the failure. Therefore information about the occurance of the failure must be sent to this (these) ME(s).

3.5. **Failure localization**

When the alarm signalling does not indicate the failure location, it will be necessary to initiate a localization process which will identify the failed item.

Automatic localization following an alarm indication, or manual intervention by the staff following an alarm or subscriber complaint, etc., is based upon:
— test programs for the failed item (internal or external),
— specialized devices (e.g. devices which measure the electrical characteristics of lines or subscriber's equipment or circuits).
It should be particularly noted that:
— the time for corrective maintenance action and
— the activity of the repair centers (which may receive unfailed items or sub-items) is strongly conditioned by the localization efficiency which has not yet been defined;
— for interchangeable items the failed item must be uniquely identified.

3.6. **Logistic delay times**

The logistic delay time is the period of time between being advised of a failure and the maintenance action.

The permissible delay time depends on the severity of the failure.

Thus the reaction on receiving a PMA, DMA or MI can be different. Following a PMA immediate action by the maintenance staff should be taken.

The reaction time following a DMA may be in the order of a few days (i.e. the first opportunity within normal working hours).

Following a MI the delay time may be several days.

Following a MI the maintenance action can be performed within the frame work of a maintenance-personnel trip schedule (scheduled maintenance) or by means of other guidance such as accumalation of MI's.

3.7. **Failure correction**

The failure correction will normally be done using a replacement item or by direct repair.

Failed items will be sent to a specialized repair centre, where appropriate test equipment will be available (the system itself should not act as a test machine).

The failure correction action is characterized by the active corrective maintenance time (active repair time).

3.8. **Verification**

After replacement by a good item, checks must be made to verify that this item is in good running order.

3.9. **Restoration**

The item will then either be put back into service so that it can offer the required service,
or
the service may be offered by other means.

4. MAINTENANCE LOGISTICS

Maintenance logistics, which are a sub-set of technical management, cover the functions necessary to support all of the actions described.

The following functions have been identified:

(a) management of information concerning network equipment in operation;
(b) management of operating data (routing data mainly);
(c) correction instructions for hardware and software;
(d) repair of removable items;
(e) management of maintenance stocks;
(f) network and equipment documentation.

A spare parts set is necessary, the quantity dependent on the:

— organization of maintenance entities,
— failure rate of item,
— turn around time (actual repair time + transport),
— number of items in operation,
— risk of a spare part not being available.

5. FAILURE STATISTICS

If all failures are recorded, this information, after processing, can serve the following organizational fields:

Management (e.g. comparing systems by their performance, comparing maintenance entities by their costs vs. delivered quality).

Organization of maintenance (e.g. use of test equipment [subscriber complaints vs. test results], amount of spare parts).

Maintenance activities (e.g. spotting weak components where preventive maintenance actions are necessary).

6. PREVENTIVE MAINTENANCE ACTIONS

(a) Mechanical parts (such as magnetic equipment heads) have to be cared for periodically.
(b) After analyzing failure statistics, decisions can be made to replace items even before failures have occurred, if they seem to be weak items.

7. SPECIAL ASPECTS OF THE MAINTENANCE OF VARIOUS NETWORK PARTS

Special aspects of the maintenance of the various network parts will be described in the following Recommendations still in study.

Special aspects of the maintenance of analogue subscriber lines.

Special aspects of the maintenance of digital subscriber lines.

Special aspects of the maintenance of digital trunk lines between digital exchanges.

Special aspects of the maintenance of analogue trunk lines between digital exchanges.

Special aspects of the maintenance of exchanges.

Special aspects of the maintenance of protocoles.

References

[1] Recommendation T/CS 10-13. *General maintenance concept and terms.*
[2] Recommendation T/CS 58-01. (Still in study.)