INTERNATIONAL TELECOMMUNICATION UNION

CCITT

THE INTERNATIONAL
TELEGRAPH AND TELEPHONE
CONSULTATIVE COMMITTEE

M.2120

(10/92)

MAINTENANCE: INTERNATIONAL TRANSPORT NETWORK

DIGITAL PATH, SECTION AND TRANSMISSION SYSTEM FAULT DETECTION AND LOCALIZATION PROCEDURES

Recommendation M.2120

FOREWORD

The CCITT (the International Telegraph and Telephone Consultative Committee) is a permanent organ of the International Telecommunication Union (ITU). CCITT is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The Plenary Assembly of CCITT which meets every four years, establishes the topics for study and approves Recommendations prepared by its Study Groups. The approval of Recommendations by the members of CCITT between Plenary Assemblies is covered by the procedure laid down in CCITT Resolution No. 2 (Melbourne, 1988).

Recommendation M.2120 was prepared by Study Group IV and was approved under the Resolution No. 2 procedure on the 5th of October 1992.

____

CCITT NOTE

In this Recommendation, the expression “Administration” is used for conciseness to indicate both a telecommunication administration and a recognized private operating agency.

Recommendation M.2120

DIGITAL PATH, SECTION AND TRANSMISSION SYSTEM[1] FAULT DETECTION AND LOCALIZATION PROCEDURES

(1992)

Abstract

This Recommendation provides procedures for digital path, section and transmission system fault detection and localization with and without in-service monitoring. Filtering and thresholding of performance informations are described for reporting to the TMN. Returning into service and long term trend analysis are considered.

Key words

– digital path;
– digital section;
– digital transmission system;
– fault detection;
– filtering;
– in-service monitoring;
– localization;
– long-term trend analysis;
– returning into service;
– thresholding;
– TMN.

Abbreviations

ES	errored second
ISM	in-service monitoring
ME	maintenance entity
MEF	maintenance entity function
RTR	reset threshold report
SEF	support entity function
SES	severely errored second
TMN	telecommunication management network
TR	threshold report

1 General

The TMN, as described in Recommendation M.3010 [5], is being progressively implemented by many Administrations. The maintenance procedures described here cover both the case where fulI ISM is available (as in the TMN) and the case where no ISM or partial ISM is available. The latter case is referred to as pre-ISM.

Information processing will then be more integrated or less integrated depending on the TMN's degree of development.

---

[1] Throughout this Recommendation the terms "path", "section" and "transmission system" should be understood as digital.

ISM should be understood as a situation where a dedicated performance monitor exists for each path and transmission system. This facilitates performance data collection, setting thresholds, and filing historical performance data in archives.

A pre-ISM situation exists if any condition does not meet the definition of ISM (e.g. existence of time shared monitoring, no monitoring at all).

2 Maintenance techniques with ISM

2.1 *Relationship with Recommendation M.20 [6]*

Recommendation M.20, "Maintenance philosophy for telecommunications networks", provides guidance for maintenance operations. This section expands on the principles given in Recommendation M.20 with specific application to transmission systems and ISM. Figure 1/M.2120 includes abridged versions of Figures 7/M.20 and 9/M.20 [6].

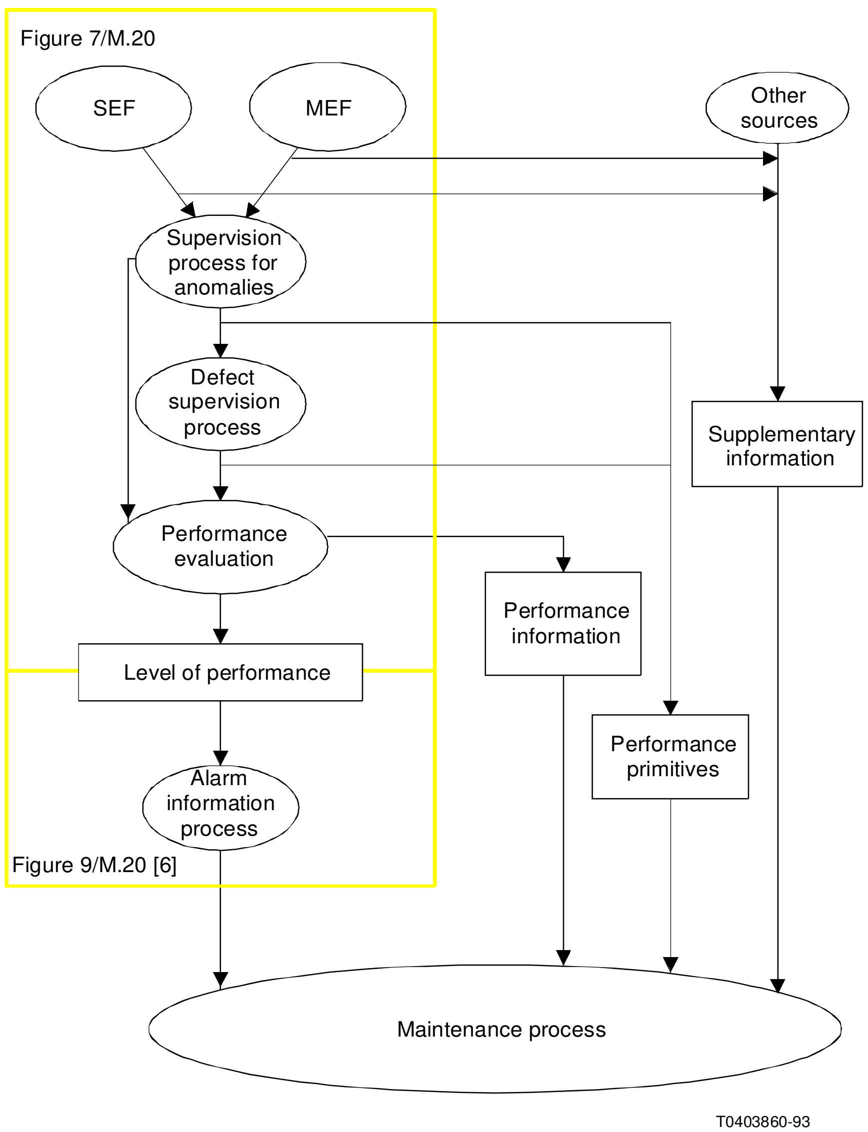

FIGURE 1/M.2120

Process of elaboration of information used for maintenance

2.2 *Fault localization information*

Once an alarm indication is received the fault localization process must begin. For this purpose several categories of information are required:

- performance information;
- performance level information;
- performance primitives;
- supplementary information.

2.2.1 *Performance information*

Performance information is in terms of the parameters of Recommendation M.2100 [7], and is used to calculate the performance levels. Normally it will be time-stamped and stored for correlation analysis and for long-term trend analysis (see § 7).

2.2.2 *Performance level information*

Performance level information [unacceptable performance level, degraded performance level, normal performance level] is derived from performance information (or the equivalent performance primitives). It is the information which will start the alarm information process as shown in Figure 1/M.2120 when a performance limit is reached. The performance limits are also referred to as alarm thresholds. The alarm generated (i.e. prompt maintenance alarm, deferred maintenance alarm or maintenance event information), determines the urgency of subsequent actions.

2.2.3 *Performance primitives information*

Performance primitives are the basic information in the form of anomalies and defects used to determine the parameter counts of Recommendation M.2100 [7]. Performance primitives depend on the type of entity being monitored.

2.2.4. *Supplementary information*

Supplementary information is information other than that obtained from monitoring. It includes derived information such as the identification of a faulty ME or sub-entity, or information from other MEs. It also includes administrative information such as the constitution of a path.

Supplementary information also includes such information as direct transmission restoration (protection switching) counts.

2.3 *Performance filtering, thresholding, reporting and historical storage*

The functions described in this section can be performed inside or outside the network element.

2.3.1 *Parameters*

The evaluation of error performance and availability performance is based on the processing of the two parameters ES and SES. The derivation of these parameters from standardized signal information is given in Recommendation M.2100 [7].

2.3.2 *Transmission states and threshold reports*

2.3.2.1 *Transmission states*

A path can be in one of two transmission states:

- unavailable state;
- available state.

The transmission state is determined from filtered SES/non-SES data (see §§ 2.3.3.1 and 2.3.4.1).

The SES/non-SES criteria for determining the available/unavailable states of the various network layers is given in Recommendation M.2100 [7].

2.3.2.2 *Threshold reports*

A TR is an unsolicited error performance report from an ME unless the TR capability has been disabled with respect to either a 15-minute or 24-hour evaluation period.

TRs can only occur when the transmission path is in the available state.

Six TRs are defined based on filtered ES and SES data:

2.3.2.2.1 *TRs based on a 15-minute evaluation period* (§ 2.3.4.2 gives precise details)

TR1-ES occurs as soon as the 15-minute "set" ES threshold is exceeded.

RTR1-ES optionally occurs at the end of a 15-minute period in which the ES count is less than the "reset" ES threshold. It can only occur subsequent to a 15-minute period containing a TR1-ES.

TR1-SES occurs as soon as the 15-minute "set" SES threshold is exceeded.

RTR1-SES optionally occurs at the end of a 15-minute period in which the SES count is zero. It can only occur subsequent to a 15-minute period containing a TR1-SES.

2.3.2.2.2 *TRs based on a 24-hour evaluation period* (§ 2.3.4.3 gives precise details)

TR2-ES occurs as soon as the 24-hour "set" ES threshold is exceeded.

TR2-SES occurs as soon as the 24-hour "set" SES threshold is exceeded.

There is no RTR for the 24-hour evaluation period. Instead, the 24-hour counters for the ES and SES parameters are always reset to zero at the end of each 24-hour period.

2.3.3 *Filter types used for evaluating transmission states and threshold reports*

Care needs to be taken with the ES and SES counters and the generation of TRs during changes in transmission states. Guidance on this issue is given in § 2.3.4.4.

2.3.3.1 *Unavailable and available state filters*

The unavailable state filter is a *P*-second rectangular sliding window, with 1-second granularity of slide. *P* represents the number of consecutive SES which defines the criterion for entering the unavailable state of a given network layer.

The available state filter is also a *Q*-second rectangular sliding window, with 1-second granularity of slide. *Q* represents the number of consecutive non-SES which define the criterion for terminating the unavailability state of a given network layer.

Values of *P* and *Q* are given in Recommendation M.2100 [7].

2.3.3.2 *TR1 and RTR1 filters*

The TR1 and RTR1 filters are 15-minute rectangular fixed windows. The start and end time datum for the 15-minute rectangular fixed window ES evaluation are the same as those for the 15-minute rectangular fixed window SES evaluation.

2.3.3.3 *TR2 filter*

The TR2 filter is a 24-hour rectangular fixed window. The start and end time datum for the 24-hour rectangular fixed window ES evaluation are the same as those for the 24-hour rectangular fixed window SES evaluation.

2.3.4 *Evaluation of transmission states and threshold reports*

2.3.4.1 *Evaluation of the unavailable and available states*

The unavailable state is detected at the end of *P* consecutive SES. Upon detection, a date/time-stamped unavailable state report should be sent to the performance management centre and a current unavailable second counter started. The time-stamp should relate to the first of the *P* consecutive SES. The occurrence of the unavailability event should also be recorded by incrementing an unavailability event counter by one in the network element historical performance registers for each ME.

The termination of the unavailable state (i.e. re-entry of the available state) is detected at the end of *Q* consecutive non-SES. Upon detection, a date/time-stamped termination of unavailability report should be sent to the performance management centre together with the number of current unavailable seconds recorded for the unavailability event which has just terminated. The current unavailable second count should be also added to a cumulative historical register unavailable second count. The date/time-stamp should relate to the first of the *Q* consecutive non-SES.

2.3.4.2 *Evaluation of TR1-ES/SES and RTR1-ES/SES*

The parameters ES and SES are counted separately, second by second, over each 15-minute rectangular fixed window period. There are two TR1s, one for ES called TR1-ES and one for SES called TR1-SES. The threshold values should be programmable over the range 1 to 900 with default values. The default values are given in Recommendation M.2100 [7].

A threshold can be crossed at any second within the 15-minute rectangular fixed window. As soon as a threshold is crossed (subject to the requirements given in § 2.3.4.4), a TR1-ES or TR1-SES as appropriate should be sent to the performance management centre together with a date/time-stamp. Moreover, parameter events should continue to be counted to the end of the current 15-minute period, at which time the count is stored in the historical registers and the rectangular fixed window ES and SES counts reset to zero.

If the optional threshold reset capability is used, then no more than one:

TR1-ES should be generated per direction of transmission until there has been a 15-minute rectangular fixed window with ≤ *W* ES events. The value for *W* should be programmable. The range and default values for *W* at each network layer is under study for inclusion in Recommendation M.2100 [7].

TR1-SES should be generated per direction of transmission until there has been a 15-minute rectangular fixed window with zero SES events (all network layers and all path lengths).

When the relevant above requirement is satisfied, the appropriate RTR1 (i.e. RTR1-ES or RTR1-SES respectively) should be sent to the performance management centre at the end of the 15-minute period. The generation of a RTR1 is only permitted subsequent to its respective TR1, and once generated re-enables the TR1 capability for the relevant parameter and direction of transmission.

2.3.4.3 *Evaluation of TR2*

The parameters ES and SES are counted separately, second by second, over each 24-hour period. There are two TR2s, one for ES called TR2-ES and one for SES called TR2-SES. The threshold values should be programmable with default values. The programmable range and default values for each network layer are under study for inclusion in Recommendation M.2100 [7].

A threshold can be crossed at any second within the 24-hour rectangular fixed window. As soon as a threshold is crossed (subject to the requirements given in § 2.3.4.4), a TR2-ES or TR2-SES as appropriate should be sent to the performance management centre together with a date/time-stamp. Moreover, parameter events shall continue to be counted to the end of the current 24-hour period, when the count is stored in the historical registers and the rectangular fixed window ES and SES counts are reset to zero.

No more than one TR2 should be generated per parameter and per direction of transmission during any 24-hour rectangular fixed window.

2.3.4.4 *Threshold report evaluation during transmission state changes*

Care should be taken to ensure that threshold reports are correctly generated and ES/SES available state counters are correctly processed during changes in the transmission state. This implies that all threshold reports should be delayed by P seconds (see § 5.1 of Recommendation M.2100 [7]).

2.3.5 *Performance history storage in network elements*

Requirements for ME performance history storage are

- Parameter counts to be stored are ES, SES, number of unavailability events and the cumulative unavailable seconds.
- There should be a current 15-minute register (which can also facilitate the TR1/RTR1 filter) plus a further $N \times$ 15-minute history registers for each parameter in each ME. The $N \times$ 15-minute history registers are used as a stack, i.e. the values held in each register are pushed down the stack one place at the end of each 15-minute period, and the oldest register values at the bottom of the stack are discarded. The value of N needs further study.
- There should be a current 24-hour register (which can also facilitate the TR2 filter) plus one previous 24-hour register for each parameter.

These requirements are provisional and subject to further study.

2.3.6 *Performance history reporting from network elements*

Performance data should be reportable to the performance management centre to suit various needs, for example:

- on demand, by request from the performance management centre;
- in a limited and targeted unsolicited format in the case of unavailability/availability transmission state change reports and, when in the available state, TR1/RTR1 or TR2 error performance reports;
- periodically, as part of a network-wide data accumulation task, by the network management centre(s). This may then be used for applications such as preventive maintenance (e.g. longer-term trend analysis) and “poor performer” analysis (see § 7 and Recommendation M.2100 [7] for further guidance).

The ME performance history reporting requirements to meet these needs are under study.

2.3.7 *Accuracy and resolution*

2.3.7.1 *Parameter counts*

All parameter counts should be actual count for the 15-minute filtering period.

Although all parameter counts should (ideally) also be actual for the 24-hour filtering periods, it is recognized that it might be desirable to limit register sizes. In such cases register overflow could occur. Should register overflow occur, the registers should hold at their maximum value for the parameter considered until the registers are read and reset at the end of the 24-hour period. An implementation involving setting and resetting an overflow bit may be used.

2.3.7.2 *Date/time-stamping of reports*

The date/time-stamping accuracy of reports, together with the method of maintaining the accuracy, is under study.

2.3.8 *Single ended monitoring capability*

Situations are envisaged where it could be desirable to carry out error and availability performance processing of both directions of path transmission from a single end. Recommendation M.2100 [7] details standardized signal information which could be used to facilitate this requirement.

3 Fault localization procedures on digital transmission system

Fault localization on digital transmission systems largely depends on the fault localization means available to the ME. However, the guidelines in §§ 3.1 and 3.2 can be used.

3.1 *Fault localization in a pre-ISM environment*

In a pre-ISM environment, a transmission system may not yield standardized parameters and may not have the capability to record performance history. In this situation the only opportunity is to monitor on a forward going basis, probably using proprietary test equipment.

Clearly, this strategy cannot guarantee identification of the source of the original performance problem, particularly if it is of a transient nature.

3.2 *Fault localization in an ISM environment*

When an unacceptable or degraded performance level is reached, the following should be done:

– immediately send a message to the control stations of the paths carried by the transmission system;

– store the message for access by those control stations which do not receive the message directly. The storage will normally be at the fault report point;

– initiate the ME's fault localization capability to find the faulty maintenance sub-entity. This should be done in a time frame appropriate to the prompt or deferred maintenance alarm levels.

Recommendation M.2100 [7], Table 3, gives the unacceptable and degraded performance level thresholds from the long-term perspective.

4 Fault localization procedures on digital paths

The efficiency of the fault localization procedure is largely dependent on the type of information available at each bit rate (i.e. CRC information, parity bit, known frame word, etc.).

4.1 *Fault localization in a pre-ISM environment*

In a pre-ISM environment, the fault localization process will usually start after a user complaint.

In this situation, the only opportunity is to monitor after the event. This process cannot guarantee identification of the source of the original performance problem, particularly if it is of a transient nature.

The control station responsible for the faulty path should

– determine path routing;

– sectionalize the path. If traffic is not totally interrupted, in-service measuring instruments as described in Recommendations O.161 [1] and O.162 [2] should be placed at various accessible points along the path to determine which part is faulty. These measurements are made at protected monitoring points (see Figure 2/M.2120);

– coordinate the measurement process so that sub-control and participating centres start and finish their measurements at the same time;

– centralize results, either at the control station or at the fault report point, and compare to determine the faulty section;

– ensure that there are no monitoring "blind spots" on the path. A "blind spot" is a portion of the path which exists between two monitored portions. For example, cross-connect equipment may not be covered by the monitors of the transmission systems connected to the input and output. Unless such a cross-connect has its own monitoring system, it may be overlooked.

If several sections are faulty, fault localization will normally concentrate first on the most severely degraded section. Where additional maintenance effort is available, the total out of service time may be reduced by utilizing this additional effort on less degraded sections. However, control is needed so that the efforts of one technician (or group) do not mask a problem being worked on by another.

If traffic is totally interrupted, or ISM instruments are not available, the same fault localization procedure as before will be used, but with a pseudo-random bit sequence injected (if possible, framed sequence - using an instrument as described in Recommendation O.151 [4]).

The points of injection and the monitoring locations should be chosen for efficiency of localization. This includes the possibility of loopback.

4.2 *Fault localization in an ISM environment*

4.2.1 The path control station is informed of problems by unacceptable or degraded performance level information (see Table 3/M.2100 [7]), trend analysis, and/or by a user complaint.

The path control station should

– undertake corrective action in a time-frame appropriate to the alarm level (prompt or deferred maintenance alarm or special instructions);

– confirm the unacceptable or degraded level of the path by consulting the history (BIS data, etc.) of the path.

4.2.2 Once the procedures of § 3.2 are initiated, the control station of the ME concerned is expected to provide supplementary information to the TMN data base.

The control stations of paths supported by the ME will be able to determine from the data base such information as the expected return into service time, taking into consideration information on any other faulty MEs which affect the path.

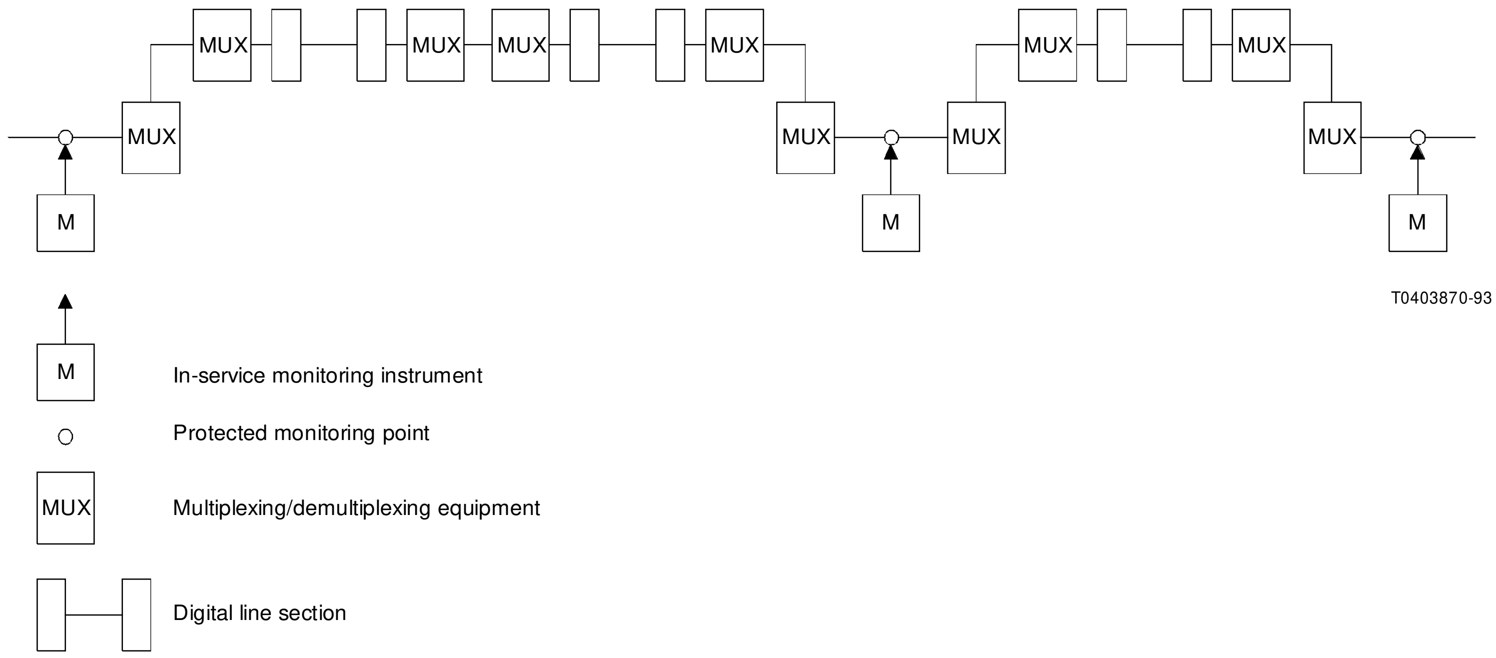

FIGURE 2/M.2120

In-service measurement along a path in the pre-ISM environment

4.2.3 If the above procedure cannot be implemented, path routing should be determined and the higher level path control stations interrogated to determine the origin of the problem. This interrogation can be carried out directly or by consulting data bases. The information exchanged must be expressed in terms of performance information as covered in Recommendation M.2100 [7], with all events date/time-stamped, and the affected direction indicated. This procedure must lead to assigning the problem to the control station of the ME where degradation exists.

5 Fault localization procedures on digital sections

If there is a fault in a section it may be that there is a path fault, in which case the localization procedures of § 4 apply. Alternatively the fault may be in a multiplexer which will be apparent if the path is good.

6 Returning an ME into service

When the repair action on a faulty ME is completed, an appropriate assurance of satisfactory performance should be made.

Depending on the type and cause of the fault and the repair process, this assurance may be as simple as the ability to carry a signal, or may be more complex.

The performance limits for returning an ME into service (after intervention) are given in Recommendation M.2100 [7].

In the extreme case it may be necessary to repeat the BIS tests as in Recommendation M.2110 [8].

When the path is returned to service it should be monitored on a reinforced basis.

7 Trend analysis and signatures

In the interest of providing superior service to users, many Administrations use, or intend to use, a preventive approach to maintenance and fault localization. Preventive maintenance implies locating and correcting faults before a performance impairment reaches an unacceptable or degraded performance level.

One of the tools of preventive maintenance is trend analysis. Information is gathered from many points in the network, date/time-stamped and stored. Continuing automatic comparisons of measurements from a particular point may indicate by the trend of the measurements that there is a potential fault. The results of the trend analysis may generate the equivalent of a low level deferred maintenance alarm. Economics will determine at what point an Administration may decide to take action.

An indication which may be useful in trend or comparison analysis is error performance. A path or section which has poorer error performance than similar paths or sections, or which is showing a trend of increasing errors may become the target of reinforced maintenance.

Trend analysis of this type implies a well developed TMN with wide deployment of ISM techniques.

A manual technique which may be useful for either preventive maintenance or fault localization is the analysis of signatures. A signature is a set of characteristics obtained by measurement, which can be interpreted to indicate the source of a fault or a potential fault.

As an example, experience on a path transported by TAT-8 has shown that a gradually increasing (over several days) number of ES in the absence of SES was indicative of a multiplexer fault which was not serious enough to generate an alarm. This signature may not appear on other systems.

As signatures may be equipment-dependant and configuration-dependant, and are often ambiguous, their development and use is a matter for consideration by local maintenance forces.

References

[1] CCITT Recommendation O.161 *In-service code violation monitors for digital systems*.

[2] CCITT Recommendation O.162 *Equipment to perform in-service monitoring on 2048 kbit/s signals*.

[3] CCITT Recommendation O.163 *Equipment to perform in-service monitoring on 1544 kbit/s signals*.

[4] CCITT Recommendation O.151 *Error performance measuring equipment for digital systems at the primary rate and above*.

[5] CCITT Recommendation M.3010 *Principles for a telecommunication management network*.

[6] CCITT Recommendation M.20 *Maintenance philosophy for telecommunications network*.

[7] CCITT Recommendation M.2100 *Performance limits for bringing-into-service and maintenance of international digital paths, sections and transmission systems*.

[8] CCITT Recommendation M.2110 *Bringing-into-service international digital paths, sections and transmission systems*.