INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

I.376

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(03/95)

INTEGRATED SERVICES DIGITAL NETWORK (ISDN)

OVERALL NETWORK ASPECTS AND FUNCTIONS

ISDN NETWORK CAPABILITIES FOR THE SUPPORT OF THE TELEACTION SERVICE

ITU-T Recommendation I.376

(Previously “CCITT Recommendation”)

FOREWORD

The ITU-T (Telecommunication Standardization Sector) is a permanent organ of the International Telecommunication Union (ITU). The ITU-T 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 World Telecommunication Standardization Conference (WTSC), which meets every four years, establishes the topics for study by the ITU-T Study Groups which, in their turn, produce Recommendations on these topics.

The approval of Recommendations by the Members of the ITU-T is covered by the procedure laid down in WTSC Resolution No. 1 (Helsinki, March 1-12, 1993).

ITU-T Recommendation I.376 was prepared by ITU-T Study Group 13 (1993-1996) and was approved under the WTSC Resolution No. 1 procedure on the 19th of March 1995.

NOTE

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

CONTENTS

SUMMARY

Teleaction in ISDN is a future alternative to dedicated alarm network and modem based solutions of today. The solutions for teleaction applications today are mostly proprietary. The harmonization of service parameters and classes of security has not been specified by ITU-T (former CCITT), but by the International Electrotechnical Committee (IEC). The dedicated teleaction network were made to offer a service with better security than the one offered by solutions based on PSTN technology.

The advantages of implementing such applications in ISDN are:

- the customer access is expected to be less expensive in the case where the ISDN access is used for several services;
- operation, administration and maintenance can be integrated more easily with other services;
- the user-network interface will be standardized;
- teleaction applications can be combined with other ISDN services into new applications (e.g. Teleaction and Videophony).

The purpose of this Recommendation is to describe the ISDN network capabilities required for the provision of teleaction teleservice in an ISDN environment.

Recommendation I.376

ISDN NETWORK CAPABILITIES FOR THE SUPPORT OF THE TELEACTION SERVICE

(Geneva, 1994)

0 Scope

The purpose of this Recommendation is to describe the ISDN network capabilities required for the provision of teleaction teleservice in an ISDN environment.

1 Introduction

Teleaction in ISDN is a future alternative to dedicated alarm networks and modem based solutions of today. The solutions for teleaction applications today are mostly proprietary. The harmonization of service parameters and classes of security has not been specified by ITU-T (former CCITT), but by the International Elctrotechnical Committee (IEC). The dedicated teleaction networks were made to offer a service with better security than the one offered by solutions based on PSTN technology.

The advantages of implementing such applications in ISDN are:

- the customer access is expected to be less expensive in the case where the ISDN access is used for several services;
- operation, administration and maintenance can be integrated more easily with other services;
- the user-network interface will be standardized;
- teleaction applications can be combined with other ISDN services into new applications (e.g. Teleaction and Videophony).

2 Abbreviations

For the purposes of this Recommendation, the following abbreviations apply:

CRF	Connection Related Functions
DSS1	Digital Subscriber Signalling System No. 1
EUT	End User Terminal
FMBS	Frame Mode Bearer Service
HLF	High Layer Functions
ISDN	Integrated Services Digital Network
SPT	Services Provider Terminal
TMF	Teleaction Management Function
USBS	User Signalling Bearer Service

3 Objectives of Teleaction

The Teleaction teleservice consists of a class of applications characterized by a number of basic properties:

- they are interactive applications;
- they have normally a low throughput as compared to the traditional information transfer rate of ISDN-channels;
- they involve very short messages between terminals and usually a single host;
- they involve a large number of low cost terminals;

– they require protection against unauthorized access and modification of messages;

– they require a supervised mode of information transfer providing at least some error protection;

– they have stringent requirements on the response time to individual transactions, and the availability/ reliability of the service.

The applications of the Teleaction teleservice in ISDN may be divided into two broad categories, each with its own network implications and specific security functions. These two categories are:

1) applications without other specific requirements regarding service reliability and security functions than those offered by the bearer service, called hereafter non-sensitive applications; and

2) applications with additional security and reliability requirements, called hereafter sensitive applications.

Applications of the Teleaction teleservice are for example:

– telemetry;

– remote process control;

– meter reading;

– alarm surveillance; and

– funds transactions.

Several levels of security will have to be regarded in providing Teleaction teleservice in ISDN, ensuring reliable communication paths between end-users and between end-users and service providers, preventing from unauthorized access to protected data. This may require the introduction of a Teleaction Management Function (TMF) within the basic ISDN-network. Clause 4 describes network-based basic functions and higher layer messaging transport protocols for this purpose.

4 Functional requirements

For some Teleaction applications, a separate unit called the Teleaction Management Function (TMF) within the public ISDN network, fulfils two major security requirements. The TMF ensures that the relevant application/terminal is functioning, and that any disruption of service is immediately reported to the Service Provider Terminal or to the associated end-user terminal. The TMF also authenticates both the user terminals and the service provider terminal. ISDN does not offer today any dedicated mechanism guaranteeing that the terminal (EUT or SPT) has not been replaced by a fake. In addition, network status information may be offered by the TMF to the SPT.

If the service provider operates through the Packet Switched Data Network or a dedicated network, the TMF is considered to be the interworking unit, and is required to perform adequate protocol translation. This clause outlines the functional requirements considered to be important to Teleaction applications, independently of where these functions are allocated. The following basic functions have been identified:

1) application-independent secure teleaction message delivery service from a terminal to a service provider and vice versa;

2) protection against active attacks such as terminal replacement, terminal emulation, message modification or deletion, or spurious connection intitiation;

3) message broadcasting from a service provider to a predefined number of destinations, e.g. for energy consumption monitoring and control;

4) notification to the service provider of any loss, modification or deletion of messages;

5) secure and permanent terminal monitoring, for example the detection of any deliberate disconnection by an intruder of the line between terminal and the TMF, with immediate notification to the service provider of a terminal being considered inactive;

6) fast message delivery according to predefined priority levels, ensuring for example the overriding of any alarm message over funds transactions or low priority alarm messages;

7) protection against disclosure of message content to a third party according to a predefined message sensitivity level;

8) alternative routing in case of failure of network equipment of any kind (CRF, TMF, transmission, etc.);

9) notification of an alternative service provider in case of failure to communicate with the primary service provider;

l0) traffic logging for audit and statistical purposes.

NOTE – Some of the distinctions between teleaction messaging and conventional X.400 messaging are the very short time-to-delivery which is normally required to be 10-30 seconds, the limited set of delivery services that shortens the length of the message header, the secure permanent monitoring of the terminals by the SPT or by the network that may impose a high level of traffic not carrying information and the stringent requirements in case of a single point of failure.

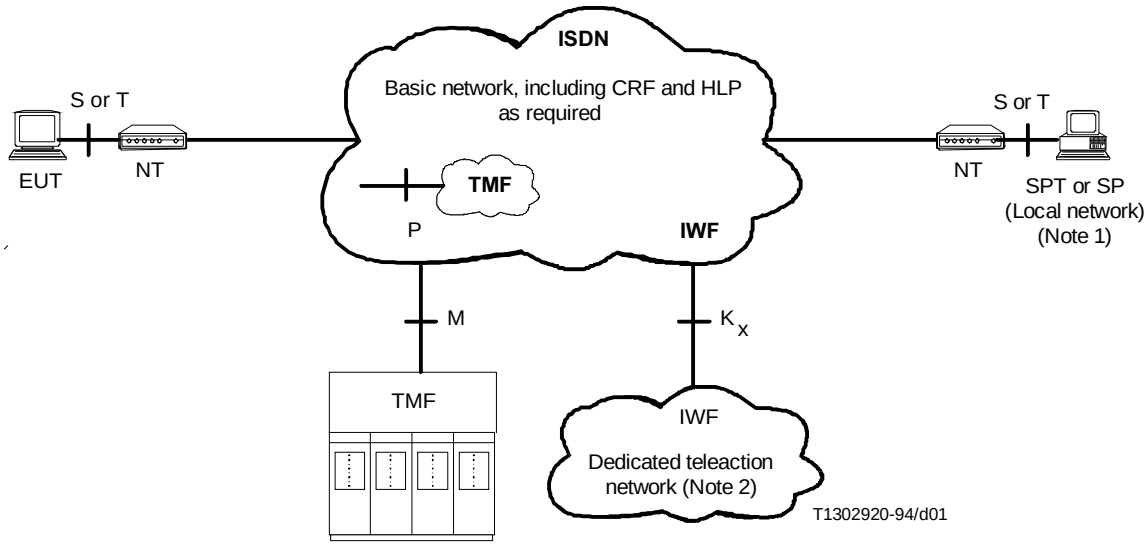
5 Functional architecture

This clause describes the functional architecture, the reference configuration, the interfaces and the service attributes of the Teleaction service, in accordance with the I.200 and I.300-Series Recommendations.

The reference configuration complies with the requirements of the basic architectural model of 2/I.324. The interfaces and service attributes comply with the requirements of Recommendation I.210.

5.1 Teleaction reference configuration

Figure 1 describes a generic reference configuration for the support of the Teleaction service by an ISDN. It describes the general functional arrangements involved, without going into the details of the many variations of the attributes of Recommendation I.340 that may lead to a large number of potential connection types.



NOTES

1 This figure does not preclude the SPT being connected to a dedicated teleaction network.

2 A dedicated teleaction network can be a physical or a virtual net based upon, e.g. PSTN or PSPDN.

FIGURE 1/I.376

Reference configuration for the support of the Teleaction service by an ISDN

The reference points are shown in Figure 1 above. In the case where no Service Provider outside the basic ISDN network is involved, the teleaction service would be supported by the concatenation of two connection types, one between the EUT and the TMF, and one between the TMF and the SPT. The logical/physical concatenation of these connections is realized by the TMF.

The TMF involves additional network resources that may be provided within the ISDN or outside of the ISDN, the reference point between ISDN and the TMF being, according to Recommendation I.324, P if the TMF is realized as an integrated specialized network resource, and M if the TMF functionalities are provided by a specialized service provider.

In any case, the End User Terminal (EUT) and the Service Provider Terminal (SPT) access the basic ISDN network at reference point S or T. Dedicated teleaction networks, private or public, basically used today for alarm surveillance and funds transfer, may interwork with the ISDN on the basis of the rules described in the I.500-Series Recommendations, the location of the interworking functions (IWF) being an implementation issue.

5.2 Service and management communication

Communication requirements of the Teleaction service should be clearly divided into two different categories:

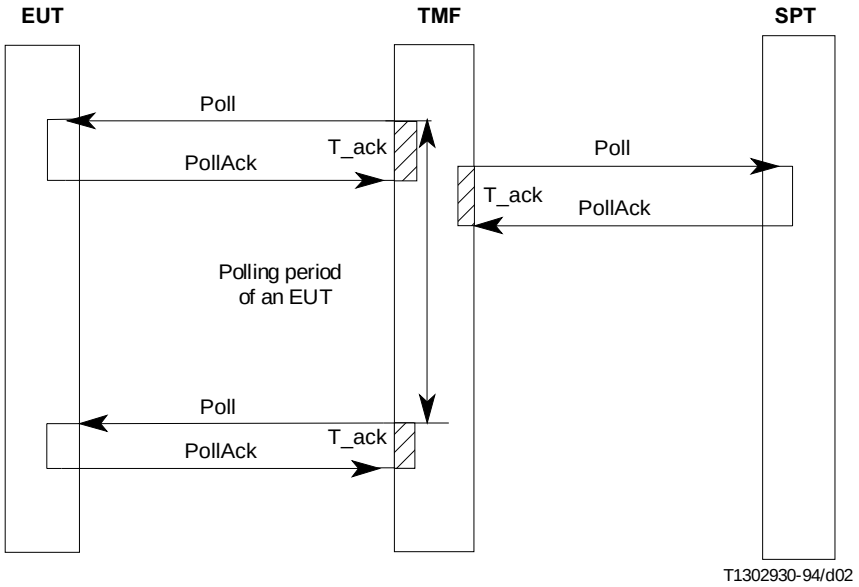
1) Management communication, i.e. supervision and monitoring of network elements to ensure secure and available access for the EUTs (and SPTs) to the network at all times. This is performed by TMF by polling EUTs (and SPTs) periodically.

2) Service information transfer communication, i.e. information exchange between EUTs and SPTs related to teleaction applications.

Management communication

The TMF executes management functions by polling the EUTs and SPTs. A simplified information flow chart for Management communication is illustrated in Figure 2.

Management traffic intensity can be so high and call establishments can be needed so frequently that e.g. PVC-type PMBS or FMBS services are most appropriate and should be recommended as the bearer services to be used. In the case where management traffic is low, switched bearer services may be used.



Poll	Polling message
PollAck	Polling acknowledgement message
T_ack	Time for polling procedure

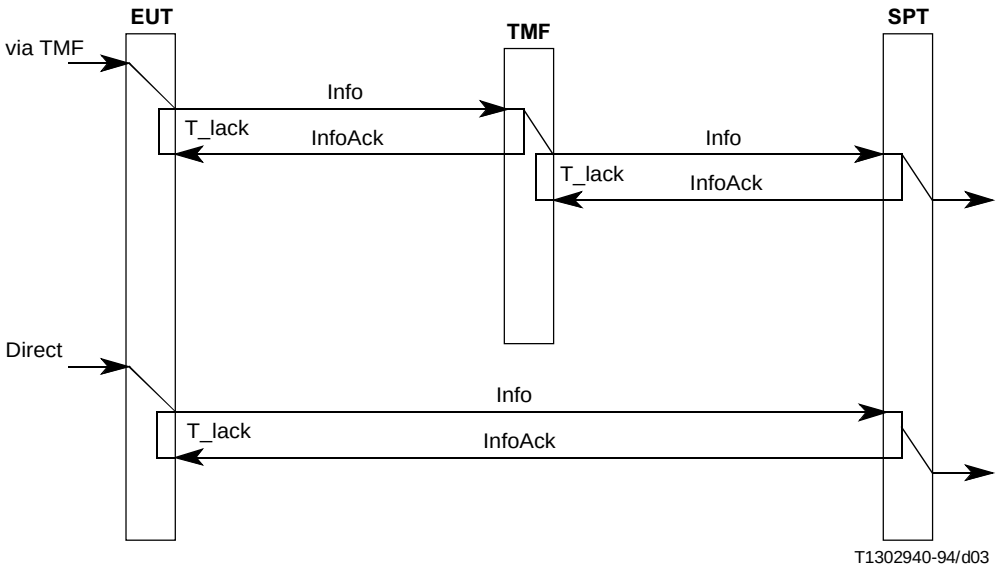
FIGURE 2/I.376

Management communication

Service information transfer communication

Service information transfer (between EUT and SPT) is normally routed via a TMF. This allows the TMF to verify that an EUT-SPT communication path is available. However, direct paths between EUT and SPT may also be used if the TMF can verify that such a path is available. See the simplified flow chart in Figure 3.

For information transfer communication, the appropriate bearer services are fully application dependable. The following ones could be considered: PMBS, FMBS and USBS.



Info	Information message
InfoAck	Information acknowledgement message
T_lack	Time for information transfer procedure

FIGURE 3/I.376

Service information transfer

5.3 Teleaction service attributes

For further study.

NOTE – Appendix I contains preliminary material.

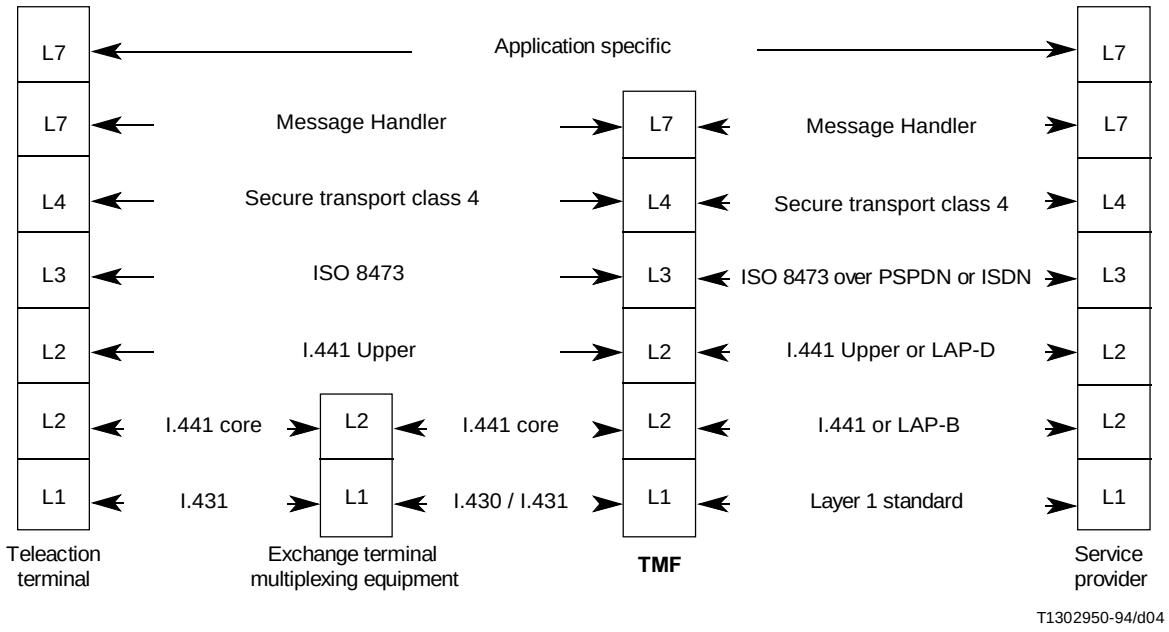
6 Service aspects

6.1 Bearer services and supplementary services

A distinction between the Teleaction service, using high layer functions in the TMF, and services based on network bearer services using only layers 1-3 of the TMF has to be made and reflected by the selected protocol stack, in order to:

- restrict the relatively heavy traffic between the TMF and the terminal, when permanent monitoring is required, to the local link between the TMF and the terminal, thus saving the significant cost of end-to-end secure inactivity control for all the terminals by minimizing the use of network resources;
- improve throughput due to priority-oriented service in the TMF;
- reduce system traffic by means of distributing broadcast capabilities within the network.

The TMF can be used as an OSI level 3 concentrator supporting for example ISO 8473 (connectionless protocol) encapsulated into X.25 PLP, thereby keeping only layers 1-3 of the TMF active, reducing the complexity of the terminal and traffic costs. In that case, the ELFs of the Teleaction teleservice can be based on a connection-oriented secure class 4 transport layer providing a network service in accordance with Recommendation X.213. These protocols can use connectionless network service, X.25 PLP or frame relay service. Figure 4 describes one possible implementation of the teleaction service protocol stack.



NOTE – The upper layers of the TMF may not always be used.

FIGURE 4/I.376

An example of the Teleaction service protocol stack

The functionality of the session and presentation layer protocols within a teleaction protocol are not within the scope of this Recommendation.

Several bearer services may support the Teleaction teleservice on the ISDN, for example:

- B-channel based circuit-mode bearer services, for example the circuit-mode 64 kbit/s unrestricted, 8 kHz structured bearer service category;
- B- or D-channel based packet-mode and frame-mode bearer services, and within this category, several sub-options are available:
  - *Option 1* – Virtual call or permanent virtual circuit bearer service (according to Recommendation X.31/I.462).
  - *Option 2* – User signalling bearer service on the D-channel.
  - *Option 3* – Frame relay/frame switching of teleaction data-frame according to Recommendations Q.922 and I.233.
  - *Option 4* – Connectionless bearer service.

The teleservice is the normal way of communication, also for EUT to SPT alarms. The polling and authentication of the EUT and SPT are offered as a supplementary service feature. The additional capability of receiving a status report from the TMF called Terminal Status Reporting, must be defined along with other supplementary service features like Broadcast.

6.2 Quality of service

The teleaction service shall provide a secure and reliable telecommunication and processing service to the end user. The service shall include facilities to:

- ensure available communication paths between EUTs and SPTs;
- prevent corruption, blocking, loss or tapping of information during transfer;
- prevent unauthorized data traffic and data sources (e.g. substitution of EUT or TMF);
- ensure that the time delay for information transfer does not exceed a specified limit.

The availability of a teleaction service does not only include the availability of communication paths, but also availability of support from the service provider.

Teleaction Management Functions (TMFs) are added to the basic ISDN network to reach the required quality of service for the teleaction service. The operation of the TMF is described below. The basic ISDN has to provide reliable and secure communication paths (bearer services, connections) between the EUT and the TMF, and between the SPT and the TMF. The attributes regarding the quality of service are described in this subclause and in Appendix II.

As specified in 5.2, communication is divided into two categories:

1) Management communication, often referred to as “polling”; and
2) Service information transfer communication, i.e. “application data”.

These two communication categories will probably have different security requirements.

All potential attack types should be evaluated against different security methods. One possible solution to the security problems is the so called “challenge and response” method based on standardized encryption algorithms. It is important that the autentication process will be performed both ways, i.e. the EUT authenticates the TMF and the TMF authenticates the EUT on a regular basis. Encryption also requires an effective and safe means of key management and distribution.

6.2.1 TMF operation

The main purpose of the Teleaction Management Function (TMF) is to increase the reliability and security of the Teleaction service. The main procedures between the EUT and the TMF are:

- after activation, the TMF will start polling the EUT if required;
- various polling intervals may be offered, depending on the type of application to be supported;
- polling is used for:
  - testing the end-to-end availability of the communication path between TMF and EUT, including the user-network access used by EUT;
  - authorization of EUT to ensure that the correct EUT is invoking a teleaction service, and to prevent sabotage;
  - checking that the EUT is not malfunctioning, keeping a log of status information received as answer to the polling procedures.

The main procedures between the SPT and the TMF are:

- after activation, the TMF will start polling the SPT;
- various polling intervals may be offered, depending on the type of application to be supported;
- the polling mechanism is used for:
  - testing the end-to-end availability of the communication paths between TMF and SPT, including the user-network access used by SPT;
  - the authorization and functionality check of SPT are for further study;
- on request from SPT, the TMF will forward EUT and network status information to the SPT.

NOTE – The TMF may acquire status knowledge both from polling and/or from the Telecommunications Management Network (TMN).

6.2.2 Quality of service attributes

The quality of service required by the Teleaction service is described in terms of the transmission delay, the availability, the fault report delay and the overall response time.

Additional quality of service parameters are for further study. The QOS attributes are specified as follows:

- *Transmission delay (sec):*
  - mean;
  - 95 percentile;
  - maximum delay.
- *Overall response time:*
  - mean;
  - 95 percentile;
  - maximum delay.
- *Availability:*
  - teleaction network (12-month period);
  - monthly availability.
- *Fault report delay:*
  - maximum delay.

6.3 Security levels

For further study.

7 Network capabilities

7.1 Connection related functions

Both connection oriented and connectionless bearer services may be used to support the Teleaction service. The type of connection may be both switched, semi-permanent or permanent. Two paths have to be established, not necessarily requiring a physical connection per path, if the TMF, for example, is integrated in the local exchange. The first path is from the EUT to the TMF, and the second path is from the TMF to SPT.

In case of switched connections, the TMF has to perform the necessary call acceptance procedure.

Both external and internal polling may be provided between the TMF and the EUT-terminal and between the TMF and the SPT-terminal. For example, an end-to-end service on top of USBS, can be realized without polling for applications like telemetry and meter reading. In other cases, where end-to-end supervision between the SPT and the EUT is necessary, the TMF has to be transparent to polling messages. The use of these capabilities for supervision purposes is optional. Two types of polling strategies have been envisaged, the external polling and the internal polling.

External polling implies that the TMF is considered being a separate node of the ISDN, e.g. using a permanent layer 2 connection on the D-channel. A frame handler performs the layer 2 multiplexing of the incoming frames at some appropriate network location and routes them to the TMF. In the case of internal polling, the EUT is polled by a specific TMF-module within the local ISDN exchange, either at layer 2 or at layer 3.

At layer 2, a DSS1 layer 2 connection can be established similar to the case of external polling. At layer 3, DSS1 procedures can be used on a signalling link not associated with a circuit switched call.

NOTES

1 Two alternatives are for further study:

i) USBS link (USERINFO) – Which can be used both for external and internal polling.

ii) Functional coding in FACILITY – Which can be used for internal polling.

2 All information transfer between an EUT and a SPT is routed via the TMF, unless a teleaction service is used directly end-to-end. In this case, the TMF can be viewed as coincident with the CRF.

3 The communication path between the TMF and the SPT may be used for several connections between the individual EUT's and the relevant SPT.

4 The communication paths between the TMF and the EUT/SPT is also used for "internal" traffic (polling) between the TMF and the EUT/SPT and may therefore be established even if no EUT-SPT communication is currently going on.

5 The following features of the layer 2 protocol on the D-channel may be needed, semipermanent layer 2 link and specific SAPI for teleaction messages. For management communication, continuous monitoring of layer 1 readiness and availability can be used.

7.2 End-to-end supervision and monitoring

By using an appropriate protocol stack, the teleaction network may support both the Teleaction applications requiring the TMF and the Teleaction applications not requiring the TMF, either by means of higher layer TMF functions or by means of network bearer services, i.e. with only layers 1-3 of the TMF remaining active. The choice may be left to the service provider according to national regulations. By these means, the following advantages can be acheived:

- the heavy traffic between the TMF and the terminal, in the case of permanent monitoring, could be restricted to the local link between the TMF and the terminal, thus saving the significant cost of end-to-end secure inactivity control for all the terminals by minimizing the use of network resources;
- improved throughput due to priority-oriented service in the TMF;
- reduction of system traffic due to distribution of broadcast capabilities in the network.

Figure 4 of clause 6 shows a possible implementation of the Teleaction service protocol stack.

7.3 Description of various polling techniques

Polling is needed for TMF-EUT and TMF-SPT Management communication (see Figure 2). The same polling techniques can be applied to both the External and Internal polling types.

Various aspects should be taken into account in choosing a polling method for Teleaction teleservice. Such aspects are economy, traffic, geography, topology, authentication and encryption.

Polling should be flexible for a wide variety of applications. For instance, if required, it should enable a bidirectional authentication on every polling transaction for a secure verification of the communication partners both ways. Polling should also follow strict rules in order to avoid any overload of the network. This requirement can be ensured by polling locally and keeping it at a low layer (layer 2) on a protocol stack.

Various polling principles:

1) *Polling Acknowledgement*
   - Single transaction acknowledgement.
   - Continuous acknowledgement (every polling message is an acknowledgement to the previous message).
2) *Polling Hierarchy*
   - Both ends can initiate the polling procedure.
   - Master/Slave polling (TMF starts the polling procedure).
3) *Polling Configuration*
   - Broadcast/Multicast polling.
   - Single point polling.
4) *Polling Frequency*
   - Random polling intervals.
   - Constant polling frequency.
5) *Encryption method*
   - Symmetrical encryption method (identical keys).
   - Asymmetrical encryption method (secret and public keys).

6) *Low/High layer polling*

- Low layer polling (layer 2).
- High layer polling (layer 3).

The permanent logical link (PLL) would be applicable to most of the described polling requirements. For security reasons a dedicated SAPI value should be specified for Teleaction purposes.

8 Interworking issues

8.1 Interworking with dedicated teleaction networks

For further study.

8.2 Interworking with private/public networks

For further study.

8.3 Interworking with mobile systems

For further study.

Appendix I

Teleaction service attributes table

(This appendix does not form an integral part of this Recommendation)

The Teleaction service has attributes distinguishing it from other telecommunications services. Depending on the type of bearer service used, both low layer attributes and high layer attributes may differ. Similarly, they have specific requirements regarding general attributes as the necessary supplementary services, the quality of service and the interworking possibilities with other networks or dedicated teleaction networks. These aspects are covered in Table I.1.

NOTE – For the purpose of the Teleaction service, the following features of the layer 2 protocol on the D-channel may be needed:

- semi-permanent layer 2 link;
- teleaction messages identified by a specific SAPI;
- continuous monitoring of layer 1 readiness and availability.

TABLE I.1/I.376

Possible values for Teleaction service attributes

Information transfer attributes 1. Information transfer mode	Circuit		Frame mode	Packet mode
2. Information transfer rate	Bit rate (kbit/s)		Throughput	Throughput
	64	Other values for further study	For further study	Network dependent access to X.2
3. Information transfer capability	Unrestricted digital information			
4. Structure	Service Data Unit (SDU) integrity		SDU integrity	SDU integrity
5. Establishment of communication	Asynchronous on demand			
6. Symmetry	Bidirectional symmetric			
7. Communication configuration	Point-to-point	Point-to-multipoint		Broadcast
Access attributes 8. Access channel and rate	B	D(16)	D(64)	Others for further study
9.1 Signalling access protocol layer 1	Recs. I.430 and I.431 (may use permanent activation)			Others for further study
9.2 Signalling access protocol layer 2	I.440 and I.441 (1)			Others for further study
9.3 Signalling access protocol layer 3	I.450			Others for further study
9.4 Information access protocol layer 1	I.430 and I.431			Others for further study
9.5 Information access protocol layer 2	I.440 and I.441			Others for further study
9.6 Information access protocol layer 3	X.25 layer 3 PVC			Others for further study
Higher layer attributes 10. Type of user information	For further study			
11. Layer 4 protocol	For further study			
12. Layer 5 protocol	For further study			
13. Layer 6 protocol	For further study			
14. Layer 7 protocol	For further study			
General attributes 15. Supplementary services	For further study			
16. Quality of service – transmission delay – availability – fault report delay	See subclause 6.2			
17. Interworking possibilities	For further study			
18. Operational and commercial attributes	For further study			

Appendix II
Specific applications

This appendix describes the main network capabilities required for the support of individual classes of Teleaction applications. It furthermore describes individual requirements that may be application specific within these individual classes. The following individual Teleaction applications have been identified:

- telemetry applications;
- meter reading applications;
- remote process control applications;
- alarm surveillance applications; and
- funds transaction applications.

II.1 Telemetry

Applications within the telemetry Teleaction service category are typically the continuous supervision of counters in order to detect malfunctioning or for accounting purposes. This type of Teleaction service is, as compared to meter reading, essentially addressing individual end-users of the ISDN network. As a consequence, it may imply a two-way communication between two endpoints within the network, as for example in the case where charging information is required to optimize the use of energy within a single home, or to route individual vehicles through the road network.

II.2 Meter reading

Meter reading is a category of Teleaction applications which requires specific congestion management safeguards. As opposed to telemetry applications, it involves normally a large number of end-users who are activated by a single broadcast request. Typical applications within this Teleaction service category are accounting for supply of electricity, water, gas, heat, meteorologic and environmental supervision. The applications are characterized by a very high, regional peak traffic, being primarily unidirectional namely from a large number of end-users towards a limited number of network endpoints.

II.3 Remote process control

Typical applications within this category of the Teleaction service are related to critical industrial and environmental productions, as for example cleaning centres for pollution purposes, chemical productions (oil-refinary, gas production, etc.), electricity and heating production and distribution, etc. Even the remote supervision of individual private installations as, for example, in the context of a private home heating control can be regarded as remote process control. This type of application is characterized by a requirement of very short and secure information transfer, typically in the order of few milliseconds.

II.4 Alarm surveillance

II.4.1 General aspects

Alarm surveillance is a range of Teleaction applications, of which typical applications are attack detection (banks, post offices, etc.), fire warning and detection, burglary alarm, and safety alarms. Common to all these applications are very stringent requirements regarding the individual line supervision of subscriber lines, the response time to individual messages and the repair time in case of breakdown. Logging of alarm messages may also be a requirement in some instances, but the acknowledgement of received alarm messages is always expected.

The delay of a single alarm message, from its occurrence at the EUT until its presentation at the SPT, as seen by some service providers, in some cases is required to be less than ten seconds. An additional requirement is seen for continuous and contiguous supervision of the teleaction line (EUT to SPT) which could result in a requirement for frequent or even permanent activation of the subscriber's access. A further requirement influencing the overall availability of the Teleaction service is the request for a repair time of all transmission equipment involved to be less than two hours.

II.4.2 Quality of service

II.4.2.1 Transmission delay

According to IEC Standard 839-5-l, the transmission system response delay shall not exceed the limits given in Table II.1. For the definition of delay categories, see IEC 839-5-1, Alarm systems – Part 5, Alarm transmission systems, General requirements for alarm transmission systems.

TABLE II.1/I.376

Transmission system response delay

	Transmission delay (seconds)				
Delay category	D0	D1	D2	D3	D4
Arithmetic mean of all transmissions		120	60	20	10
Upper 95 percentile for all transmissions	240	240	80	30	15
Maximum acceptable delay		480	120	50	20

II.4.2.2 Availability

According to IEC 839-5-l, Alarm systems – Part 5, the availability shall be equal to or better than the values shown in Table II.2.

For the definition of availability classes, see IEC 839-5-1, Alarm systems – Part 5, Alarm transmission systems, General requirements for alarm transmission systems.

TABLE II.2/I.376

Availability performance criteria

Class	A1	A2	A3	A4	A5
Availability of the total Teleaction network during a period of 12 months	97%	99.3%	99.5%	99.8%	99.99%
Monthly availability	75%	91%	95%	98.5%	99.95%

II.4.2.3 Fault report delay

According to IEC Standard 839-5-1, the maximum period from the instant the fault develops in the teleaction system until the fault information is reported to the alarm receiving centre shall not exceed the limits shown in Table II.3.

For the definition of fault report delay classes, see IEC 839-5-1, Alarm systems – Part 5, Alarm transmission systems, General requirements for alarm transmission systems.

TABLE II.3/I.376

Fault reporting delay

	Delay (s: seconds, m: minutes, h: hours, d: days)				
Class	T1	T2	T3	T4	T5
Maximum period	32 d	25 h	65 m	90 s	20 s

II.5 Fund transactions

Fund transactions involve the transfer of very short transactions identifying one of a limited number of transactions from network endpoints that are located far away from a centralized database (or databases), where the actual checking of transactions is performed. One transaction requires one acknowledgement. One derived important application is the verification of identity in relation to the control of access to given facilities, while other applications are credit card billing or teleshopping from a home terminal.

This category of Teleaction applications has stringent requirements regarding the response time to single transactions, and regarding the individual line supervision of subscriber lines, although the line supervision may not need to be performed quite so often as in the case of alarm surveillance. Various polling intervals for different kinds of funds transactions may be used.

The overall response time accepted by a user is in the order of 10 to 15 seconds (see Note 1). The overall response time is the sum of:

- transaction times in the EUT;
- transmission delays on the subscriber's loop (using the ISDN B- or D-channel bearer capability);
- processing time within the TMF;
- transmission delays between TMF and SPT via a second network (private or public ISDN/PSPDN/ CSPDN, etc.);
- transaction times within the SPT (see Note 2).

Considering the above, transaction times and transmission delays on the subscriber's access should be minimized to allow for sufficient processing time outside the ISDN and to support the acceptance by the user.

NOTES

1 The proper apportionment of the overall response time between the network and the SPT is for further study.

2 The SPT may include additional data processing equipment.