79

THE USE OF THE TRANSPORT LAYER IN TELECONTROL SYSTEMS

Working Group 03
of
Study Committee 35
(Communication and Telecontrol)

June 1993

THE USE OF

THE TRANSPORT LAYER

IN TELECONTROL SYSTEMS

Working Group 35.03

Convener : J. Hegge
Secretary : J.M. Selga

Members:
D. Bisci, R. Doster, M. Franc, R. Schnee, P.G. Visser
C. Bochu, J. Florêncio, G. Funk, V.-M. Jääskeläinen

June 1993

CIGRE-SC35-WG03-1993

THE USE OF THE TRANSPORT LAYER IN TELECONTROL SYSTEMS

by

Working Group 03

of

Study Committee 35 (Communication and Telecontrol)

LIST OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1.INTRODUCTION

Classically Telecontrol Systems used typically rigid network structures such are tree structures or double rings with no or limited possibility to use alternative types of communication.

More Recently, the evolution of Telecommunication has provided the possibility as well as the need of using several networking technologies to support Telecontrol Systems.

This new situation has created the convenience for some means of compatibilization of a unique applications software complying with some requirements and the need to use several technologically diverse telecommunication networks (X.25, Ethernet, token-ring, dial-up lines, ISDN, packet radio etc) with different performance levels.

Within this context the purpose of the Transport layer is to provide end-to-end data transfer capability in a transparent, reliable and efficient manner over a wide spectrum of possible networking technologies and presenting a unified interface and Quality of Service to the application.

This allows to view the Transport Layer (TL) as a hinge between the application and the network, that allows the former to be more independent and flexible with regard to the underlying network by hiding the network idiosincracies to the transport user.

This end-to-end transfer may even span several networks including LANs as well as WANs. For instance one end may be connected to an Ethernet LAN while the other is connected to an X.25 network.

The transport layer should bridge the gap between the requirements of the user or application and what the network can offer with regard to eg. availability and throughput.

Thus the introduction of a TL in Telecontrol Systems will open up for new networking technologies. The TL will hide the network differences, from the application entities and will make it easier the introduction of new types of network in the future.

The aim of this report is to give on overview of the possibilities and implications of the introduction of a transport layer in Telecontrol Systems in the context of a new architecture based on the ISO layered structure as well as to study several specific points of interest or possible concern in Telecontrol.

It follows a suggestion included in an IEC-TC57 Draft [1] in the sense of analyzing the adequacy for Telecontrol of the concepts and procedures described in the ISO transport protocols.

The most basic conclusion is that the ISO Class 4 Transport Protocol satisfies Telecontrol requirements although there are several undefined topics and points for further study.

2.LAYERING

To simplify the design, development and maintenance of data systems it is very convenient to partition them into functional modules.

This, that has been recognized even for systems with moderate complexity, becomes a necessity for complex systems.

For this reason modularity is a key concept in complex system engineering.

In the case of data networks the basic functional modularity is layering.

Data networks can be subdivided in concatenated layers with different functions and well defined interfaces between consecutive layers.

The interconnection of different systems and the desirability of compatibility between them, promoted the convincement that a world-wide agreement with respect to the modules or layers that form a data network was a necessity.

Today there is an international standard regarding modularity or layering in data networks that was first promoted by ISO and known as Open Systems Interconnection Basic Reference Model 2, and afterwards adopted by C.C.I.T.T. in its Recommendation X.200.

In this standard, data system are partitioned in seven layers with well defined interfaces and contents.

Most of the services provided by the seven layers and the corresponding protocols have been internationally standardized by ISO.

The names of the different layers starting from the lower level one are: physical,link, network, transport, session, presentation and application.

The Transport Layer, just in the middle of the 7 layers, is the meeting point between the upper,application oriented, layers and the lower,networks oriented layers.

3.SHORT DESCRIPTION OF THE TRANSPORT LAYER AND LAYERS BELOW AND ABOVE

A description of the layering principles and of each of the seven layers can be found in a companion CIGRE-SC35-WG03 Draft on "Computer Communication Architecture". Also a short description of the four lower layers can be found in the CIGRE-SC35-WG03 Paper on "Requirements and Performance of Packet Switching Networks with Special Reference to Telecontrol".

Here it is important to remember the services provides by the Transport layer and layers just below (Network) and above (Session).

3.1.THE NETWORK LAYER

The Network Layer provides the means to establish, maintain and terminate network-connections between open systems containing communicating application--entities and the functional and procedural means to exchange network-service-data-units between transport-entities over network-connections.

It provides to the transport-entities independence from routing and relay considerations associated with the establishment and operation of a given network-connection. This includes the case where several subnetworks are used in tandem or in parallel. It makes invisible to transport-entities how underlying resources such as data-link-connections are used to provide network-connections.

Any relay functions and hop-by-hop service enhancement protocols used to support the network-service between the OSI and open systems are operating below the Transport Layer, i.e. within the Network Layer or below. [2]

It also provides the functional and procedural means for connectionless-mode transmission among trans-

port-entities and, therefore, provides to the transport entities independence of routing and relay considerations associated with connectionless-mode transmission. [3]

3.2.THE TRANSPORT LAYER

The Transport-service provides transparent transfer of data between session-entities and relieves them from any concern with the detailed way in which reliable and cost effective transfer of data is achieved.

The Transport Layer optimizes the use of the available network-service to provide the performance required by each session-entity at minimum cost. This optimization is achieved within the constraints imposed by the overall demands of all concurrent session-entities and the overall quality and capacity of the network-service available to the Transport Layer.

All protocols defined in the Transport Layer have end-to-end significance, where the ends are defined as correspondent transport-entities.

The Transport Layer is relieved of any concern with routing and relaying since the network-service provides network-connections from any transport-entity to any other, including the case of tandem sub-networks.

The transport functions invoked in the Transport Layer to provide a requested service quality depend on the quality of the network-service.

The quality of the network-service depends on the way the network-service is achieved. [2]

So, the Transport layer provides a transparent, reliable and efficient end-to-end data transfer mechanism through a network or series of networks for the session layer and layers above.

It uses the services of the Network layer, shielding the upper layers from the details of the network and of the connections.

Error-detection and error-recovery mechanisms play important roles in the operation of the Transport protocol.

3.3.THE SESSION LAYER

The purpose of the Session Layer is to provide the means necessary for cooperating presentation-entities to organize and synchronize their dialogue and to manage their data exchange. To do this, the Session Layer provides services to establish a session-connection between two presentation-entities, and to support orderly data exchange interactions.

A session-connection is created when requested by a presentation-entity at a session-service-access-point. During the lifetime of the session-connection, session services are used by the presentation-entities to regulate their dialogue, and to ensure an orderly message exchange on the session-connection. The session-connection exists until it is released by either the presentation-entities or the session-entities. While the session-connection exists, session-services maintain the state of the dialogue even over data loss by the Transport Layer [2].

In case of connectionless-mode communication, the only purpose of the Session Layer is to provide a mapping of Transport-addresses to Session-addresses.

4.FUNCTIONS OF THE TRANSPORT LAYER [2,4,5]

The function of the TL are those related to the optimization of the use of the available network services and the delivery of the performance required by each application at minimum cost and taking into account the constraints imposed by the network and the overall demand of all concurrent session entities.

These functions are grouped below into those used at all times and those concerned with connection establishment, data transfer and release.

The list refers to all the possible functions taken into account by the ISO Transport Protocol. In a real situation only part of them are provided depending upon the selected class of Transport Protocol (TP) and options.

4.1.FUNCTIONS PROVIDED AT ALL TIMES

The following functions, depending upon the selected class and options, are provided at all times during a transport connection:

a) transmission of TPDUs

b) multiplexing and demultiplexing : a function used to share a single network connection between two or more transport connections.

c) error detection : a function used to detect the loss, corruption, duplication, misordering or misdelivery of TPDUs and network signalled errors.

d) error recovery: a function used to recover from detected and signalled errors.

4.2.FUNCTIONS PROVIDED DURING CONNECTION ESTABLISHMENT

The purpose of connection establishment is to establish a transport connection between two TS- users. The following functions of the transport layer during this phase match the TS-users' requested quality of service with the services offered by the network layer :

a) select the network service which best matches the requirement of the TS-user taking into account charges for various services.

b) decide whether to multiplex multiple transport connections onto a single network connection.

c) establish the optimum TPDU size.

d) select the functions that will be operational upon entering the data transfer phase.

e) map transport addresses onto network addresses.

f) provide a means to distinguish between two different transport connections.

g) transport of Transport Service user data

h) Negotiation of Quality of Service.

i) Establishment of the Transport connection.

4.3.FUNCTIONS PROVIDED DURING DATA TRANSFER

The purpose of data transfer is to permit duplex transmission of TSDUs between the two TS-user connected by the transport connection. This purpose is achieved by means of two-way simultaneous communication and by the following functions, some of which are used or not used in accordance with the result of the selection performed in connection establishment :

a) concatenation and separation :a function used to collect several TPDUs into a single NSDU at the sending transport entity and to separate the TPDUs at the receiving transport entity.

b) segmenting and reassembling : a function used to segment a single data TSDU into multiple TPDUs at the sending transport entity and to reassemble them into their original format at the receiving transport entity.

c) splitting and recombining : a function allowing the simultaneous use of two or more network connections to support the same transport connection;

d) flow control : a function used to regulate the flow of TPDUs between two transport entities on one transport connection;

e) transport connection identification: a means to uniquely identify a transport connection between the pair of transport entities supporting the connection during the lifetime of the transport connection;

f) expedited data transfer : a function used to bypass the flow control of normal data TPDU.

g) TSDU delimiting: a function used to determines the beginning and ending of a TSDU.

4.4.RELEASE

The purpose of the release function is to provide disconnection of the transport connection , regardless of the current activity.

4.5 OTHER FUNCTIONS

The International Standard for the transport layer does not include the following functions which are under consideration for inclusion in future editions of the International Standard.

a) encryption;

b) accounting mechanisms;

c) status exchanges and monitoring of QOS.

d) blocking;

e) temporary release

5 EXISTING STANDARDS AND RECOMMENDATIONS FOR THE TRANSPORT LAYER

Both ISO and the CCITT have been working inclose liaison and have produced the following Standards/Recommendations for the Transport layer. The differences between them are quite small.

I.S.O. Standards

ISO 8072:1986	Transport Service Definition
ISO 8072/ addendum1	Transport Service Definition Connectionless-mode transmission
ISO 8073:1986	Connection Oriented Transport Protocol Specification.
ISO 8602:1987	Protocol for providing the connectionless mode transport service.
ISO 8073:ADD1	Connection oriented transport protocol Specification of the Network connection management subprotocol.
ISO 8072: ADD2	ADDENDUM2
ISO 8073: ADD2	Connection oriented transport protocol Specification. Class four operation over connetionless network service.

Another work of ISO related to the Transport Layer is the Technical Report TR (Network/Transport Protocol Interworking Specification).

C.C.I.T.T. Recommendations

Recommendation X.214.- Transport Service Definition for Open Systems Interconnection (OSI) for CCITT Applications.- Red Book - 1984.It corresponds to the ISO 8072 Standard.

Recommendation X.224.- Transport Protocol Specification for Open Systems Interconnection for CCITT Applications. - Red Book - 1984. It corresponds to the ISO 8073 Standard.

Recommendation T.70.- Network - Independent Basic Transport Service for Teletex. CCITT - Yellow Book - Genève 1980.

Besides, the ECMA (European Computer Manufacturers Association), has produced the ECMA-72 standard for transport services which is aligned with the previous ISO and CCITT Standards/Recommendations

Another relevant standard for the Transport Service is the U.S. Military Standard MIL-STD-1778 or Transmission Control Protocol (TCP) and other related military standards. It has been designed to match military requirements, has been throuroughly tested during more than 10 years and is gaining acceptance by the industry.

This means that data integrity is a strong point of TCP, feature which is of prime interest in Telecontrol.

The TCP was originally developed for the ARPA network and today is an industrial de-facto standard supported by several vendors. It has influenced the posterior development of the ISO Transport Protocol.CP is not fully compatible with ISO's seven layer Reference Model.

ISO class-4 transport protocol may, theoretically, be as reliable as TCP though it lacks the backup of over 10 years of existence and field testing of the TCP.

Another protocol very similar to the ISO one is the NBS (National Bureau of Standards) U.S. Federal Information Processing Standard (FIPS) for the transport protocol [6].

The FIPS transport service definition contains some optional features that are not part of the ISO transport protocol.

6. ISO TRANSPORT SERVICES AND PRIMITIVES

Table I summarizes the ISO Transport services and primitives available to the TS user .

PHASE	PRIMITIVE	PARAMETERS
CONNECTION ESTABLISHMENT	T-CONNECT.Request .Indication	Called Address Calling Address Expedited Data Option Quality of Service TS User Data
	T-CONNECT.Response .Confirm	Quality of Service Responding Address Expedited Data Option TS User Data
DATA TRANSFER (Only in connection oriented protocols)	T-DATA.Request .Indication	TS User Data
	T-EXP. DATA.Request (Optional) .Indication	TS User Data
CONNECTION RELEASE	T-DISCONNECT.Request	TS User Data
	T-DISC.Indication	Disconnect Reason TS User Data
CONNECTIONLESS DATA TRANSFER (Only for the connectionless protocol)	T-UNITDATA.Request .Indication	Called Address Calling Address Quality of service Security Parameters TS User Data

TABLE I. SUMMARY OF ISO TRANSPORT SERVICE PRIMITIVES AND PARAMETERS.

The basic primitives are the general ones used in the ISO model (request, indication, response, confirm) and are represented in figure I.

The Transport service primitives are the following:

SERVICE PRIMITIVE	CHARACTERISTICS
T-CONNECT	mandatory, connection oriented
T-DISCONNECT	mandatory, connection oriented
T-DATA	mandatory, connection oriented
T-EXPEDITED DATA	optional, connection oriented
T-UNIT-DATA	mandatory, connectionless oriented

The TS connection-establishment primitives are indicated in figure II, the Transport service disconnection primitives are indicated in figure III and the primitives during data transfer are represented in figure IV.

From the previous primitives only the T-EXPEDITED DATA one is optional and in fact not supported by ELCOM and WSCC protocols.

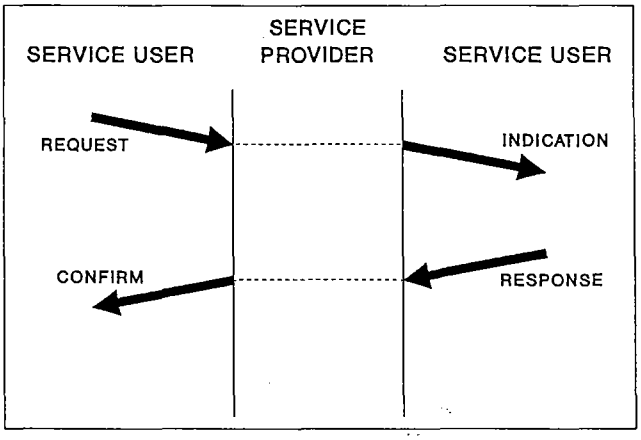

FIGURE I. BASIC ISO PRIMITIVES

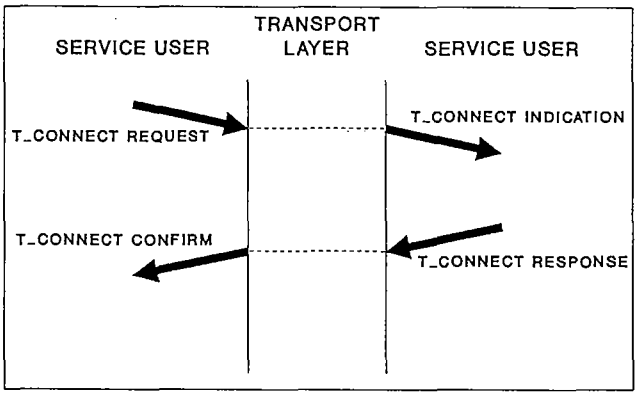

FIGURE II. CONNECTION ESTABLISHMENT TRANSPORT SERVICE PRIMITIVES.

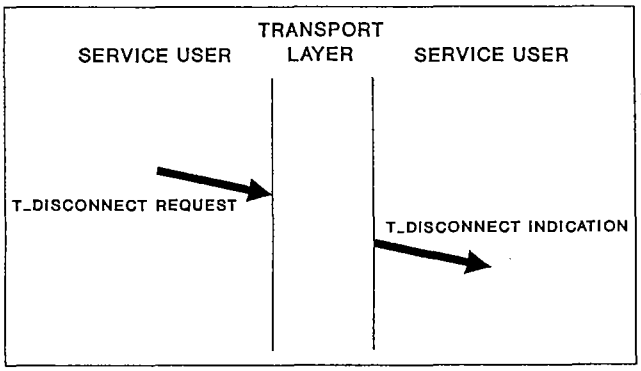

FIGURE III. DISCONNECTION BY THE TRANSPORT SERVICE USER.

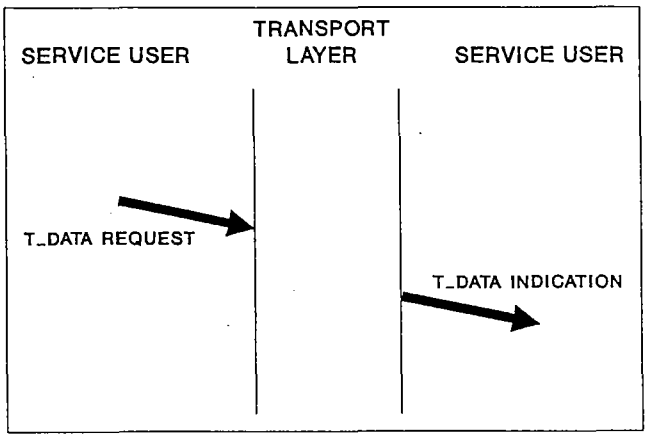

FIGURE IV. TRANSPORT SERVICE DATA TRANSFER PRIMITIVES

7.ISO PROTOCOL CLASSES

ISO classifies Network connections for convenience in three types, A; B and C, with decreasing quality.

Type A. Network connections with acceptable residual error rate and acceptable rate of signalled failures, eg. disconnect or reset.

Type B. Network connections with acceptable residual error rate but unacceptable rate of signalled failures.

Type C. Network connections with residual error rate not acceptable to the transport service user.

It should be noted that Types A, B, C have no absolute figures, and that what may be Type A for a given application may be Type B to another, according to the application requirements for Quality of Service.

Due to the lack of precision of these definitions, the same network may be considered of different type depending on the application requirements.

In order to interwork with these underlying subnetworks of different quality both CCITT and ISO have agreed on the following five classes for the Transport Protocol numbered from 0 to 4,suited to various grades of network service and with different functionality and complexity being the latter the one with more functionality.

Class 0: Simple Class (TP0)

Class 1: Basic Class. Error Recovery Class. (TP1)

Class 2: Multiplexing Class (TP2)

Class 3: Error Recovery and Multiplexing Class (TP3)

Class 4: Error Detection and Recovery Class (TP4)

ISO also defines a connectionless transport protocol (CLTP) that offers a best try approach to transfer the offered data and is, therefore, intended four use with high quality networks or with cyclical or query/response data.

Classes and options within classes are negotiated during the transport connection establishment phase. With the exception of Classes 0 and 1, transport connections of a different class may be multiplexer together onto the same network connection. Options define additional functions that may be associated within a class.

The choice of class will be made by the transport entities according to:

1) the users requirements expressed via T-CONNECT Request and T-CONNECT Response service primitives.

2) the quality of the available Network Service.

3) the user-required service versus cost ratio acceptable for the transport user.

The basic protocol unit is the Transport Protocol Data Unit (TPDU); TPDUs, in general are classified either as Data TPDUs or Control TPDUs.

All classes use the T-Connect Request/Indication and T-Connect Response/Confirm ISO Transport service primitives for connection establishment (See figure II). This protocol exchange provides for:

1 Identification of calling and called session entities by use of reference numbers.

2 Negotiation of classes and options.

3 Negotiation of size of Data TPDUs.

4 Connection identification.

5 Exchange of parameters.

Since the Transport Service Data Unit (TSDU: an arbitrary amount of data from the higher layer but which has to be treated as a single unit) is not constrained in size, it has to be segmented into manageable protocol sizes.

7.1. CLASS 0 - SIMPLE CLASS

Class 0 is for use over Type A Network Connections. It has the minimum functionality of all the classes and is fully compatible with an earlier CCITT Recommendation (S.70) for providing Transport Service to "Teletex Terminals".

Only functions for establishment, data transfer with segmenting, and error reporting are available. There are no functions for multiplexing, disconnection, flow control, error recovery, or expedited data transfer. Furthermore, no exchange of user data is permitted during connection establishment, and only address and TPDU size parameters are allowed.

There is no explicit disconnection procedure; therefore the lifetime of the Transport Connection is dependent upon, and the same as, the lifetime of the Network Connection. The transport disconnect is signalled to the other end as a Network Disconnect.

For class 0, the standard maximum Data TPDU length is 128 octets including the TPDU header.

7.2.CLASS 1 - BASIC ERROR RECOVERY CLASS

Class 1 is intended for use over Type B Network Connections.

The objective of this class is to provide recovery from network signalled errors (network disconnect or reset).

Class 1 provides Transport Connections with error recovery, expedited data transfer, disconnection, and flow control based on the underlying Network Service provided flow control. Data may be exchanged during connection establishment. No functions are provided for multiplexing.

Class 1 contains mechanisms to permit the use of the Delivery Confirmation (D-bit) and Interrupt mechanisms of the CCITT Recommendation X.25 [7].

7.3.CLASS 2 - MULTIPLEXING CLASS

Class 2 has been designed for operation over Type A Network Connections.

This class provides capability of multiplexing several Transport Connections over a single Network connection.

The use of flow control within the protocol is an option of Class 2. This option can be used to reduce congestion, optimize response times and resource utilization. This is required when the traffic is heavy and continuous and/or when there is a high degree of multiplexing taking place.

The non use of flow control can be useful for Transport Connections with noncritical response time requirements, or with infrequent short bursts of traffic with a predictable low total level of utilization of the underlying Network Connection.
Multiplexing can also be used when there is no flow control function.

Class 2 provides the following functions in addition to those available in Class 0.

1 Multiplexing
2 Flow Control
3 Exchange of user data during connection establishment
4 Credit mechanism (with flow control option)
5 Expedited data transfer
6 Explicit disconnection

No functions are provided for error detection or error recovery. If the network resets or disconnects, the Transport Connection is terminated without an explicit end-to-end exchange and the TS users are informed. (The transport connection will be terminated when the network connection is disconnected).

Since it assumes a reliable network, class protocol does not require an acknowledgement data unit to be transmitted during the connection phase.

7.4.CLASS 3 - ERROR RECOVERY CLASS

Class 3 is intended for use over Type B Network Connections.

Class 3 enhances Class 2 with the additional functions to permit recovery from network signalled errors (network disconnect or reset).

7.5. CLASS 4 - ERROR DETECTION AND RECOVERY CLASS

Class 4 is designed for use over network connections considered to have an unacceptable residual error rate relative to high-level requirements. i.e. a Type C network connection.

It provides all the functionalities of the lower classes plus protection against errored, missequenced, duplicated or lost control and data TPDUs. This class also provides for increased throughput capability and additional resilience against network failure by allowing a TC to make use of multiple network connections.

The main differences from Class 3 are the addition of time-out mechanisms and resultant extra procedures and the protection of TPDUs with a checksum.

ISO Class 4 transport protocol is a connection-oriented protocol combining all functions required for reliable transmission on top of an unreliable network service.

TP4 may provide all the functions listed in chapter 4. Among them, several specific features of TP4 not offered by the rest of ISO transport protocol classes are the following.

- Possibility of splitting of one TC into several NCs or routes. A very interesting feature that allows to increase availability, resilience and throughput.
- In-sequence delivery of user data over misordering networks.
- Recovery of errored, duplicated or lost data.
- Possibility of increasing data integrity.
- Negotiation of a large number of QOS parameters.
- Detection of unsignalled network failures.

For doing so the basic protocol mechanisms used by TP4, among others, are the following:

- Go-back-N windowing scheme with only Positive Acknowledgment with Retransmission upon timeout (PAR). This means that it is not possible to request retransmissions of corrupted or lost data frames by means of negative or selective acknowledgment and that retransmissions occur only upon timeout.
- Connection establishment by means of the procedure known as "Three-way hand-shake".
- Optional checksumming of TPDUs
- Cyclical transmission of "void" acknowledgements combined with inactivity timers.

8.ISO CLASS 4 - TRANSPORT PROTOCOL

8.1.TRANSPORT PROTOCOL DATA UNITS

Ten TPDUs have been defined for use with the Transport protocol class 4. They are the following:

TPDU type	Code	Amount of Data Carried
CR, Connection Request	1110	<=32octets
CC, Connection Confirm	1101	<=32octets
DR, Disconnect Request	1000	<=64octets
DC, Disconnect Confirm	1100	None
ERR,TPDU error	0111	None
DT, Data	1111	Up to negotiated length
ED, Expedited Data	0001	<=16octets
AK, Acknowledgement	0110	None
EA, Expedited data Acknowledgement	0010	None
UD, Unit Data	0100	Up to maximum value of Network Service Data Units

8.2.FORMATS AND OVERHEAD

Since in Telecontrol many transport connection will be permanently established, the most relevant format is the DT (data) TPDU format.

The DT TPDUs format is the following:

Concept	Number of octets
Length Indicator	1
DT indentifier (11110000)	1
Destination reference number	2
TPDU number + EOT	1 or 4
Checksum	3
Data	Variable

So the transport header of the DT TPDUs has a length of 8 or 11 octets (depending whether 7-bit or 31-bit numbering is used

Besides this, the AK (acknowledgment) TPDU which are transmitted in the contrary direction of DT TPDUs, up to one for each of them, has a total length of at least 6 octets up to a 12 or even more.

This will also impact efficiency greatly.

From the previous numbers, and given the typical short length of Telecontrol data, it is apparent that the Transport layer will have a large impact on the efficiency of the system (by lowering it).

8.3.ERROR-DETECTION AND ERROR-RECOVERY MECHANISMS IN ISO CLASS-4 TRANSPORT PROTOCOL

Mechanism 1: Three-way handshake

Description: The Connection Confirm TPDU is Acknowledged. It is exemplified in figure V.

Use: It ensures that the connection is established correctly. It avoids deadlocks and situations where the receiver waits for ever. This mechanism is also used by TCP.

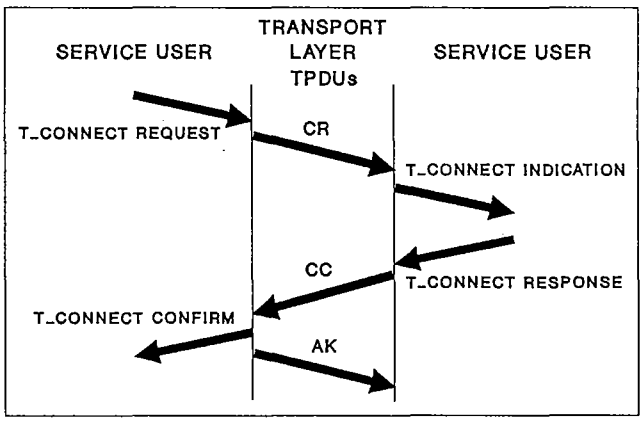

FIGURE V. CLASS-4 TRANSPORT PROTOCOL SUCCESSFUL CONNECTION.

Mechanism 2: Checksum

If the checksum is incorrect (detects an error), the TPDU is dropped. Then, the retransmission mechanism for lost TDPUs is invoked. The type of checksum used is the one known as "Fletcher's checksum" [8], and is two bytes long.

Mechanism 3: Retransmission on time-out plus positive acknowledgment

Used to cope with unsignalled loss of TPDUs by the NS-providor.

If no acknowledgment is received and the time-out expires, the TDPU is sent again.

There are positive self-standing acknowledgments from the receiver to the sender.

The acknowledgment carries the number of the next expected TPDU and implicitly acknowledges receipt of all TPDUs with lower number (See figure VI).

Because there are several types of TDPUs, there are also several types of acknowledgments and timer settings.

Used to recover from lost packets

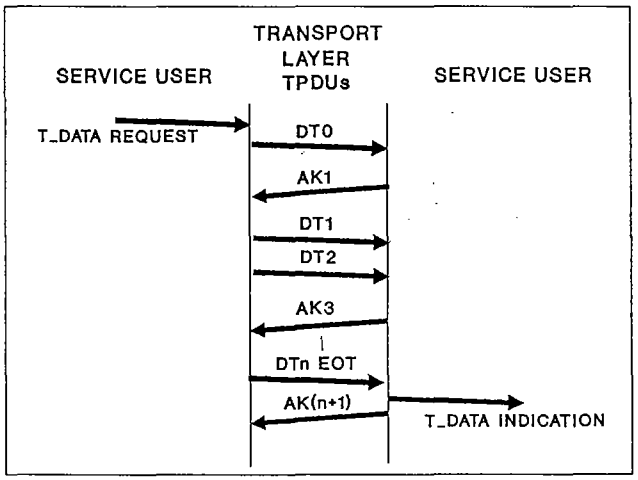

FIGURE VI. CLASS-4 TRANSPORT PROTOCOL NORMAL DATA TRANSFER.

Mechanism 4: Give-up procedure

There is a limit on the number of times a TDPU can be retransmitted. Then, the sender gives up.

It is used when no acknowledgments are received by the TDPU sender.

There is also a timer (persistence timer) providing a bound for the maximum tense for which a TDPU requiring positive acknowledgment can be retransmitted.

It is a way of closing the connection when data units are not getting through the network.

Mechanism 5: Inactivity control

Used to cope with unsignalled termination of a network connection.

There is an inactivity or acknowledge timer that upper limits the time between successive arrivals in a connection. Useful when the peer entity is dead or when the network is broken. It is a way to disconnect in case of such failures.

This mechanism is a reachability mechanism very interesting for Telecontrol, keeping track of the connection continuously and informing the upper layers in case of undue disconnection.

Mechanism 6: Credit (CDT field)

It allows the receiver to control the sending window according to the congestion at reception. This field is appended to data acknowledgements and may vary during a connection. So it allows to exercice a flow control action on the sender. This mechanism is by-passed by expedited data.

Mechanism 7: Large, negotiable, sequence number space

Two values can be used: a 7-bit sequence number and a 31-bit sequence number. Clearly the second value prevents the numbering wrap around in any environment while the first can only be used in networks with short packet life time.

Numbering allows detection of duplicated and lost packets as well as resequencing at the receiver.

Mechanism 8: Use of source and destination reference numbers

These numbers are two bytes long and greatly reduce the probability of taking delayed packets of old connections as good ones.

8.4.QUALITY OF SERVICE PARAMETERS AND MANAGEMENT IN ISO TP4.

The quality of service parameters in ISO TP4 represent the user's requirements for throughput, transit delay, integrity, protection and priority of this connection, relative to other connections.These parameters are transmitted in the TP4 T-CONNECTION request, indication, response and confirm service primitives to allow negotiation of QOS at the connection phase.

The transport protocol uses these parameters to determine the network services required, to decide splitting over several NCs or multiplexing of several TCs over one N; to choose among one of the five transport classes; to adjust the size of the sequence number space (7 or 31 bit); to decide whether a transport layer checksum is needed; to establish the maximum TPDU size (which in turn decides the concatenation of TPDUs and the segmentation of TSDUs); to select functions and flow control strategy; to assign priorities to TCs and to use the expedited data transfer option.

The quality of service parameters are in turn passed down to network services.

The user throughput requirements are given in terms of average and minimum values for each direction of transmission. The transit delay is expressed as average and maximum allowable values. The integrity parameter refers to an acceptable residual error rate (including errors, duplication and loss of data).

Throughput requirement may influence the decision on which network connection to use and whether to split or multiplex connections.

The delay requirement also may influence the type of NC chosen.

The Residual Error Probability requirement is the basis for deciding whether to use a checksum at the TL or not. It also may influence the type of NC used.

The priority requirement may influence the way (the order) in which TPDUs of different connections are processed within the TL, but of outmost importance for the priority requirement is the ability to pass the priority requirement down to the network.

The problem is that the procedures to make such decisions are not yet specified and many times are difficult to devise. Also monitoring of QOS during the data transfer to ensure the agreed QOS values phase is not specified.

Normally what is done is to compare the requirements for QOS received by the transport user to the a priori known performance of the different networking options available. This is a poor and rigid way of operating that raises concern for Telecontrol.

In the case of the Residual Error Rate of the network the measurement/monitoring of it is very difficult since the required probabilities are very small. Probably the a priori knowledge is the only way.

But in the case of throughput and delay there are other options such as the measurement of the throughput achieved in previous network connections or the sending of a round trip fictitious data TPDU to estimate the delay.

This error rate is used to determine whether or not a checksum at the transport layer is to be used.

This assumes that the network integrity levels are known and that the improvement achieved by the use of the transport checksum is also known, something that as far as we know has not been yet investigated.

The priority option has an effect on allocation of buffer resources, the type of transmission strategy to be used, and the allocation of connection resources.

During the negotiation phase the quality of service requested by the transport user may be reduced but not augmented by the transport service provider. This means that the quality of service parameters appearing in the request may be different (better) than those in the corresponding response and confirm primitives.

The negotiated QOS values then apply throughout the lifetime of the Transport Connection and the TL is responsible for ensuring the maintenance of the negotiated QOS values. In case of not being able to do so the Transport Layer should disconnect the Transport Connection by issuing a T- DISCONNECT to the Transport user.

If class 4 is selected as the protocol class, the Connection Confirm (CC) sender may choose to reduce it to class 2. But if class 2 is initially selected, the CC sender must agree with this choice and so state in the CC.

8.5 LIST OF QOS PARAMETERS IN ISO TP4 [2]

The QOS parameters are included in the variable part of the Connections Request (CR) TPDU and are the following:

a) Throughput
   Parameter code : 1000 1001
   Parameter length : 12 or 24
   Parameter value :

1st 12 : maximum throughput,as follows:

First 3 octets: target value, calling-called user direction
Second 3 octets : minimum acceptable, calling-called user direction.
Third 3 octets : target value, called-calling user direction
Fourth 3 octets : minimum acceptable, called-calling user direction.

2nd 12 octets (optional): average throughput, as follows:

Fifth 3 octets : target value, calling-called user direction

Sixth 3 octets : minimum acceptable, calling-called user direction.
Seventh 3 octets: target value, called-calling user direction
Eight 3 octets : minimum acceptable, called-calling user direction.

Where the average throughput is emitted, it is considered to have the same value as the maximum throughput Values are expressed in octets per second.

b) Residual error rate
Parameter code : 1000 0110
Parameter length : 3

Parameter value:

1st octet: target value,power of 10

2nd octet: minimum acceptable, power of 10

3rd octet : TSDU size of interest, expressed as a power of 2.

c) Priority
Parameter code : 1000 0111

Parameter length: 2

Parameter value : integer (0 is the highest priority)

d) Transit delay

Parameter code : 1000 1000

Parameter length : 8

Parameter value :

First 2 octets : target value, calling-called, user direction.

Second 2 octets : maximum acceptable, calling-called user direction

Third 2 octets : target value, called-calling user direction.

Fourth 2 octets : maximum acceptable, called - calling user direction.

Values are expressed in milliseconds, and are based upon a TSDU size of 128 octets.

In the connectionless case the quality of service parameters are carried by the T-UNIT-DATA primitive. They are the same as in the connection oriented case except for the throughput, concept not applicable to connectionless transmission, and are used by the transport layer to select appropriate protocol options specifically to determine if a checksum should be used, and are passed on to the network layer as well. The Unit Date TPDU does not carry any QOS parameter except for the checksum if used.

9. TCP/IP

Due to its marketing importance today it is necessary to mention the Transmission Control Protocol (TCP),a pioneering USA Department of Defense transport protocol on which experience ISO Class 4 TP is based.

TCP is very important in the market today because many LANs use it and there are many products, experience and studies available.

The functions offered by TCP/IP are very similar to those of ISO TP4/CLNP.This is not surprising, since TCP has greatly influenced the ISO Class 4 transport protocol which has incorporated a number of its features. With regard to the transport service, TCP can not offer the same as ISO TP4. The most important difference is the lack of the TSDU concept. Data is sent as a byte stream over a TCP connection. This means that the ISO Transport Service primitives indicated in chapter 6 (figure I) are not supported by TCP.

Another difference is that TCP does not have an expedited data transfer mechanism, although an urgent pointer is available.

The TP does not have a graceful "drain-and-close" mechanism for connection release.

In most cases IP is run over LANs, ie. ethernet and token ring. However, it is possible for a host connected to X.25 to use IP over X.25. Serial line IP (SLIP) makes it possible to communicate over asynchronous dial-up and leased lines. The possibilities are:

- TCP/IP over LANs.
- TCP/IP over X.25 networks
- TCP/IP over asynchronous lines

It is possible to build networks based on TCP/IP. Specifications as well as products are mature since TCP/IP has been around for more than 10 years.

10.MIGRATION FROM TCP/IP TO TP4

It is expected that TCP and ISO Transport Protocols will coexist for some time, but that, as more manufacturers and users begin to adopt the ISO suite of transport protocols, use of TCP will begin to decrease.

The de-facto situation makes interesting to find ways to allow interoperation between TCP and ISO protocols to allow to operate ISO applications an top of TCP/IP LANs and to allow global migration towards ISO.

Although TCP does not offer the same transport service as ISO there are several ways to support the added functionality.

One possibility is to use a convergence protocol consisting in operating TPO over TCP at both ends, thus supporting full ISO Transport Service.

This interesting possibility for solving the move from TCP to ISO protocols is described in IAB (Internet Activities Board) RFC (Request For Comments) 983 and 1006 "ISO Transport Services on Top of the TCP".

However, if a subset of the ISO Transport Service is needed, it is possible to use a simpler mapping.

Also, to provide the TSDU concept a PPDU length field can be used preceding the PPDU.

Another possibility for migration from TCP/IP to TP4 is the interconnection of both systems by the use of TCP/IP-ISO GATEWAYS including the whole stacks of the

DoD and ISO up to the application layer. In this way both systems are completely independent and an application relay function tailored at will can be placed on top of both. The problem may be the definition of the Application Service.

All this may be useful for Telecontrol, for instance for linking market TCP/IP based LANs to ISO based Wide Area Networks or Applications.

11. INTERCONNECTION OF SYSTEMS

11.1 THE RELAYING ISSUE

Today, Network service (layer 3 of the OSI Reference Model - ISO 7498) can be offered through two different standardized protocols :

- the Connection-mode Network Protocol (CONP) based on the X.25 standard (ISO 8208/ISO 8878) and
- the Connectionless-mode Network Protocol (CLNP) based on the Internet standard (ISO8473).

Unfortunately those two protocols cannot interoperate, making it necessary to add above them a relaying function. This way, communication can take place between an end system connected to a "Connection-mode Subnetwork" and another end system connected to a "Connectionless-mode Subnetwork". Such a function can be performed either in the Network layer or in the Transport layer, as described below.

11.2 APPLICATIONS IN TELECONTROL SYSTEMS

Telecontrol systems generally are implemented on a number of equipments dispatched in distant sites (control centres, substations, power plants,etc..) interconnected via a wide area transmission network.

In some sites, telecontrol applications have become so complex that they often have been distributed on several equipments linked together by a local area network (see Figure VII).

For various reasons, the trend today at least in Europe) is to use a Connection-mode Network Protocol (e.g. X.25) on wide area networks and a Connectionless-mode Network Protocol (e.g. Internet) on local area networks. This brings forth the issue of LAN/WAN interworking . Other solutions, like the generalized use of X.25 (or Internet) on both LANS and WANS, allow this issue to be skipped, although they are less frequently implemented.

Within a site, at least one equipment has to communicate both with other equipments of the same site and with equipments of other site(s). For example, if a control centre application is distributed in such a way that processing functions are grouped into one equipment and man-machine interface into another, the processing equipment has to communicate with the man-machine interface equipment and with RTUs as well.

It can also happen, perhaps more and more frequently today, that another equipment of the same site (e.g. the configuration machine in our control centre example) will have to communicate with totally different distant sites (e.g. a database management centre). This leads to a situation where, like in Figure VIII, several equipments in a site have to communicate between each other and with various distant equipments.

A given application equipment can access both a local and a distant equipment either :

- directly, meaning that it would have to implement both the CONP ant the CLNP, or
- via an intermediate equipment of the same site, that can access both local and distant equipments directly.

The first solution is more straightforward but will become expensive in a tangled situation like the one in Figure VIII. The second solution can lead to the Figure IX configuration where an unique equipment has the task of relaying the communications entering and/or leaving the site.

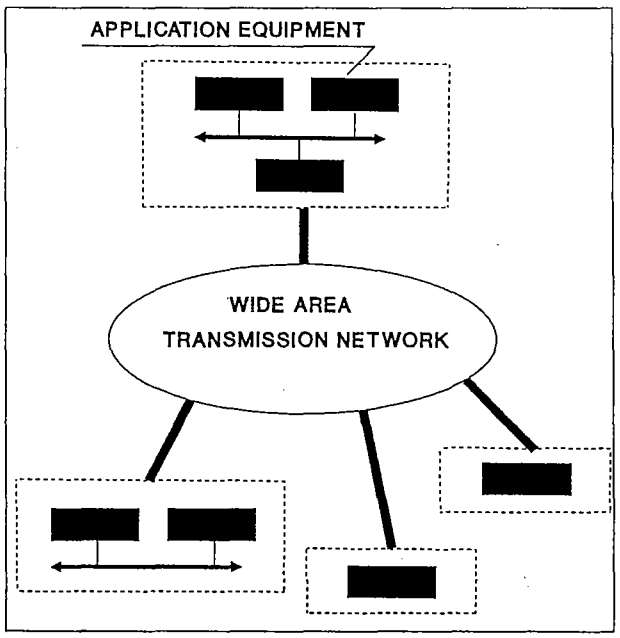

FIGURE VII. A GENERAL EXAMPLE OF TELECONTROL SYSTEM.

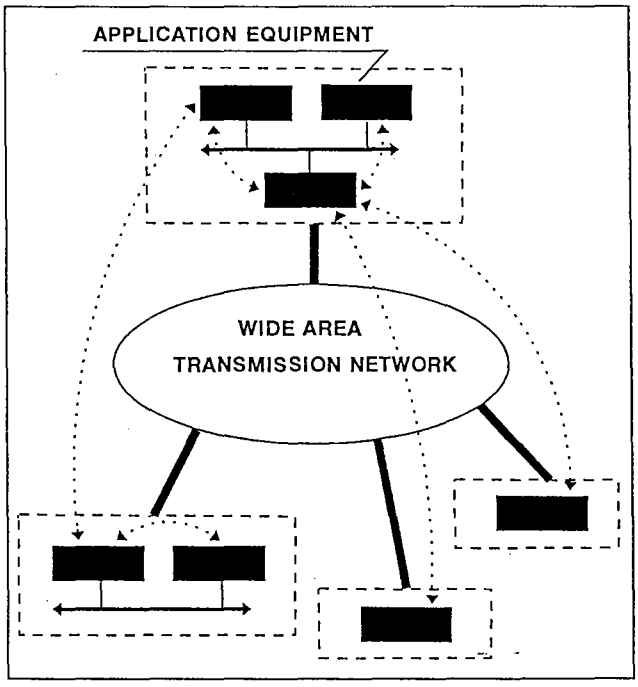

FIGURE VIII. TYPICAL COMMUNICATION NEEDS BETWEEN TELECONTROL EQUIPMENTS.

This relaying function can be performed either :

- on the application level, in which case the equipment is called a gateway and implements application and transmission functions, or on a lower level (typically the Network layer), in which case the equipment is called relay and is specialized in transmission alone.

The gateway scheme usually is preferred where an applicative control must be performed on certain communications, especially sensitive ones.

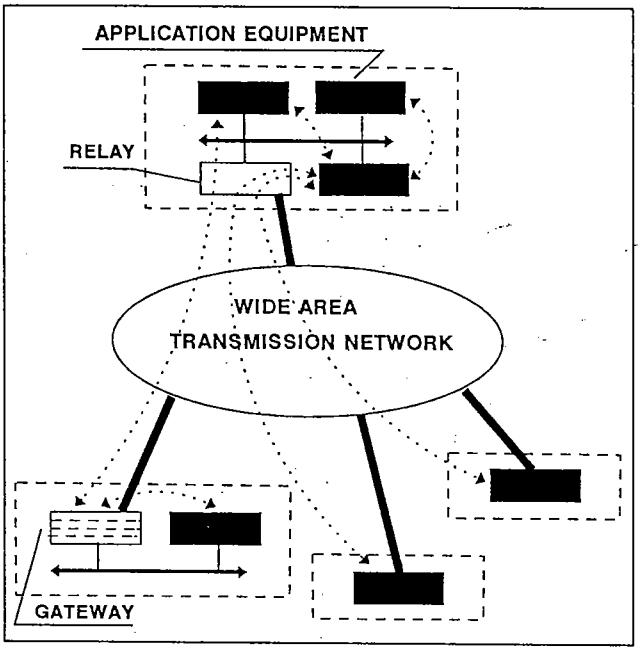

FIGURE IX. EXAMPLE OF CONFIGURATION USING GATEWAYS AND RELAYS.

Limiting entry points in a site and placing gateways at those points is a powerful solution to enforce access control (as an example, the latest version of ACSE standards incorporate authentication mechanisms). However, when such controls are not necessary, it is better not to use a gateway since it encourages a mix-up of application and transmission functions within the same software, sometimes creating difficulties when only one of the two has to be replaced.

A relay is a pure transmission equipment (except for what regards network management) and therefore is transparent to any pair of end systems involved in a communication through it. Basically, it looks like all the local area networks, in the sites where a relay has been installed, and the telecontrol wide area network had been merged into one single network. In this solution, creating a new communication between any pair of end systems merely amounts to the creation of new associations at the application level, irrespective of which geographical site these end systems are located in.

11.3.THE STANDARDIZED APPROACH : INTERNET(ISO 8473)

The OSI Reference Model (ISO 7498) stipulates that Transport connections shall be end-to-end, which means that Application Protocol Data Units(APDU) exchanged between two end systems may pass through any number of Network entities as they go through intermediate systems, but only through two Transport entities (one in each end system). Thus, at the Transport level and above, the nature of the subnetworks that are used in an instance of communication should be transparent.

A way to achieve this is to structure the Network entity of an intermediate system in such a way that part of it does not depend on the subnetwork. This is done in ISO 8648 ("Internal Organization of the Network layer"). The result is a kind of "sub-layering"of the Network layer, in which:

- a "lower" protocol is used in each subnetwork (e.g. X25 on a WAN and Internet on a LAN)

- a "higher" protocol, identical for all subnetworks, encapsulates the "lower" one : it is called the Subnetwork Independent Convergence Protocol (SNICP).

Today, the only standardized SNICP is Internet (ISO 8473). Since it is a Connectionless-mode protocol, it follows that the ways to achieve end-to-end connection at Transport level in a network with both LAN(s) and WAN(s) are:

- to use the CONP (X.25) all the way, even on the LAN(s): it is possible (as defined in ISO8881) but very rarely implemented and such products for LANs are not easily found on the marketplace;

- to use the CLNP (Internet) in LAN(s) and WAN(s) either directly or (in WAN(s)) above X.25: in such a case the amount of overhead data on WAN(s) increases dramatically.

- to use the CLNP in LAN(s) and to interconnect them by the use of direct links between CLNP routers. More details of these types of interconnection are given in chapter 11.7.

- Another possibility, which is dealt with in chapter 11.6.is the interconnection of LANs by the use of bridges.

11.4 THE TRANSPORT LAYER RELAY

In order to interconnect a CONP and a CLNP without using the CLNP as a convergence protocol, an alternative solution has been designed using the Transport layer Originally presented in a position paper (16-/11/87) from the MAP/TOP Users Group under the name "MSDSG" (Multi-System Distributed System Gateway), it has recently been incorporated into the body of ISO specifications as a Transport Layer Relay, by means of a Technical Report (TR 10172).

A Transport Layer Relay is an intermediate system with the following properties:

- it is transparent to any pair of end systems communicating through it, even if these end systems operate different Network protocols and/or different Transport classes;

- it behaves like a Network Layer Relay with regard to Network addressing (it "mirrors" the source address of incoming NPDUs into the corresponding outgoing NPDUs and vice versa):

- Transport Layer Relays can be operated in series and/or in parallel, just like Network Layer Relays.

Two different kinds of Transport Layer Relays have been defined, to allow for the varying degree of compatibility between the Transport protocols operated

by each end system:

- the Active Transport Layer Relay (ATLR) is the most complex one since it involves two Transport entities, each one managing a Transport connection with one end system, and a Transport Relaying

Function used to bridge the connections together .

- the Passive Transport Layer Relay (PTLR) is a simplified version with only a Transport Relaying Function passing TPDUs back and forth between the two Network entities.

The basic difference between a PTLR and a ATLR lies in that the former merely maps TPDUs with minimal change between the two Network entities, without intervening in the detailed operation of the Transport protocol; whereas the latter actually builds TSDUs from the incoming TPDUs and creates new TPDUs to be sent forward. Thus, only an ATLR can perform Transport protocol class conversion

As a result, if Transport class 0 or 2 is used over in a WAN (hence over a CONP), only an ATLR can be used to relay communications into a LAN where Transport class 4 is operated over a CLNP (the usual case). To put it differently, besides providing error detection and recovery as well as reachability monitoring. the choice of Transport class 4 over X.25 in a Wide Area Network allows the use of the much simpler and efficient Passive Transport Layer Relay for relaying into LANs using Internet, thus favouring the use of TP4 everywhere. Nevertheless, the use of Class 2 is unavoidable since according to ISO it should be implemented when using Class 4.

11.5 ADDITIONAL REMARKS ON TR 10172

Technical Report 10172 specifies the use of Internet as SNICP or the use of an active or passive Transport Layer Relay. Since the TLR solution is a violation of the OSI Reference Model, it is clearly stated in TR 10172 that this document will not be converted into an International Standard . However, since the TLR is a more efficient solution than the generalized use of Internet, especially in the field of industrial data transmission, it is expected that, this report having stabilized the TLR specification, vendors will soon offer corresponding products.

Many specific features of transmission are addressed in TR 10172 like Network addressing, Network routing and QOS processing, the latter being of particular significance in the field of telecontrol. When using Transport Layer Relays, satisfactory solutions can be found to achieve transparency with regard to these features provided that some prior agreements are made (e.g. an absolute order of preference between TLRs with regard to routing, or a global scale for priority values). These global agreements seem reasonable in a telecontrol environment where much of the data flows along predefined paths.

Some tricky situations can occur when using several TLRs in parallel (e.g. for the sake of redundancy) or when an alternate path exists through Network Layer Relays only. Once again, these pitfalls can be avoided by agreeing on preferred routes and a rational network topology.

11.6 CONNECTING LANs BY BRIDGES

For companies with geographically spread activities like power companies the benefits of company wide computer networks are obvious.

Local Area Networks (LANs) connected together to a Wide Area Network (WAN) offer a flexible highway for information transmission increasing the productivity of information systems.

One of the problems in forming WANs has been the high cost of telecommunication channels with adequate throughput. Long distance data transmission service is in most countries a privilege of PTT-companies resulting in overdimensioned costs.

On the other hand, power companies usually have the right to establish private telecommunication channels for their own usage. Due to today's high investment costs these channels offer moderate transmission speeds, for example 2 Mbit/s,which must be shared with several users.

Practical experiences have shown, that even a relatively slow connection channel between two or more LAN's can offer adequate fast response times for typical power company usage.

Figure X presents one example of LAN- WAN configuration in operation, where connections between LAN's are build with direct n*64 kbit/s channels, and for redundancy reasons X.25 - network is used as well. Low cost bridges isolate LAN-traffic and form necessary buffering capacity.

Even a capacity of 2*64 kbit/s allows normal programming and data terminal working over network. Of course big file transfers and similar actions show longer response times. Through priority settings important functions can be guaranteed faster service. Bridges offer also flexible transmisisson speed adjustment, when situation changes.

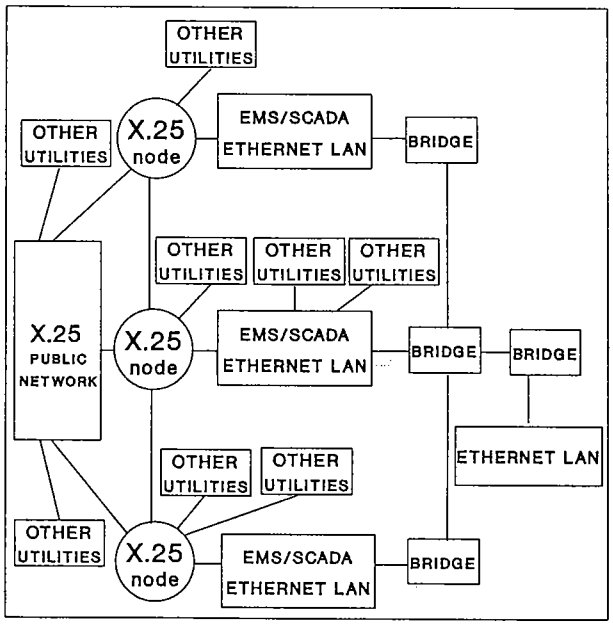

FIGURE X. A SPECIFIC ARCHITECTURE USING BRIDGES.

A ring connection of LANs offers automatic rerouting capacity. Another benefit is achieved by using private and commercial X.25 -services as stand-by channels. Automatic overflow and rerouting facilities on the level corresponding to OSI-level 4 (DECNET -service) takes effective use of low basic cost of these commercial services, but keeps the traffic dependent costs in minimum.

11.7 PROTOCOL STACKS AND NETWORK CONFIGURATIONS USING ISO CLASS 4 TRANSPORT PROTOCOL

To exemplify the networking possibilities allowed by the use of ISO protocols and the corresponding stacks of protocols, figure XI represents them and the corresponding stacks of protocols.

Some of the most interesting terminal protocol stacks for Telecontrol are:

A) TP4 over CLNP/LAN

B) TP4 over X.25

C) TP4 over CLNP/X.25

D) TP4 over INLP/LAN (ethernet or token ring)

Another possibility is TP4 over CLNP and HDLC. Nevertheless this possibility is usually supplied through the use of stack A) and of directly connected CLNP routers.

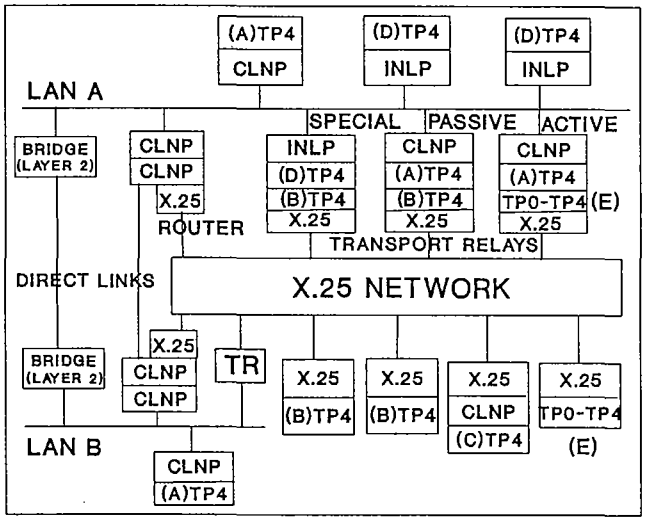

FIGURE XI. NETWORK CONFIGURATION WITH ALL THE DIFFERENT ISO PROFILES.

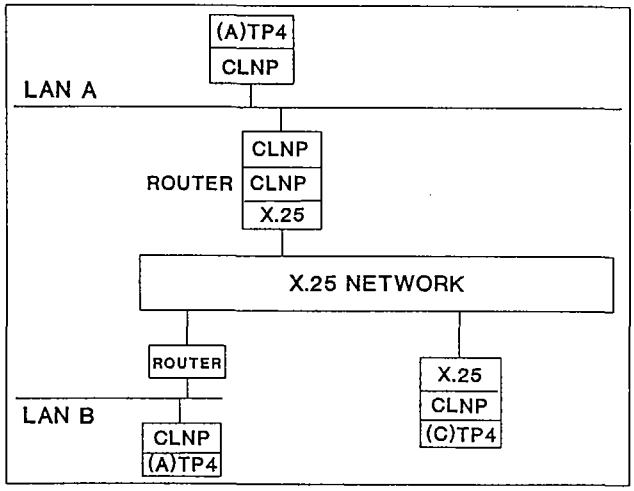

FIGURE XI-I. NETWORK CONFIGURATION WITH ALL THE DIFFERENT ISO PROFILES USING X.25 ROUTERS.

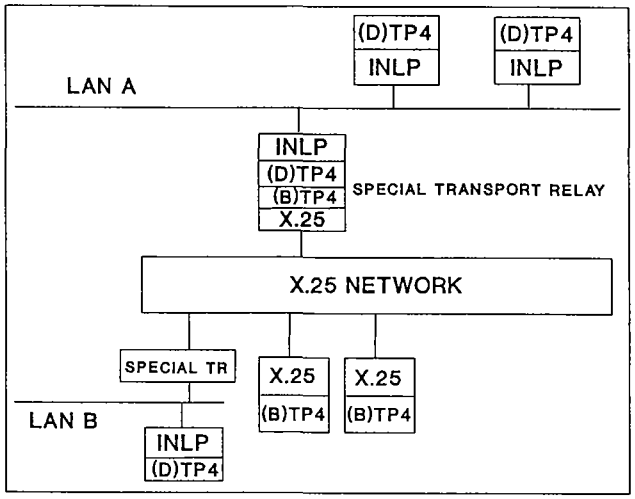

FIGURE XI-II. NETWORK CONFIGURATION WITH ALL THE DIFFERENT ISO PROFILES USING THE SPECIAL TRANSPORT RELAY.

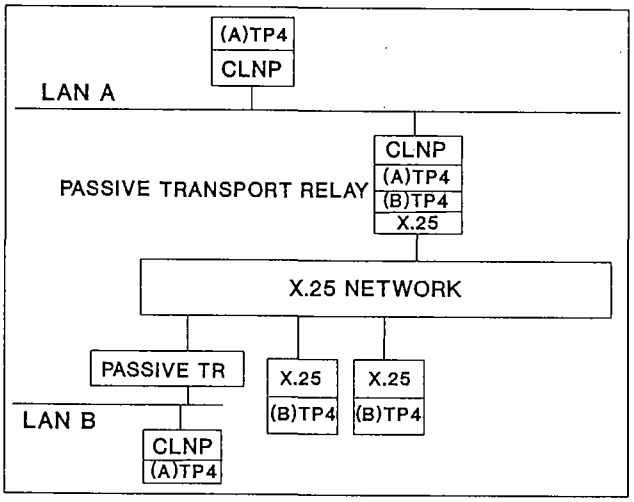

FIGURE XI-III. NETWORK CONFIGURATION WITH ALL THE DIFFERENT ISO PROFILES USING PASSIVE TRANSPORT RELAYS.

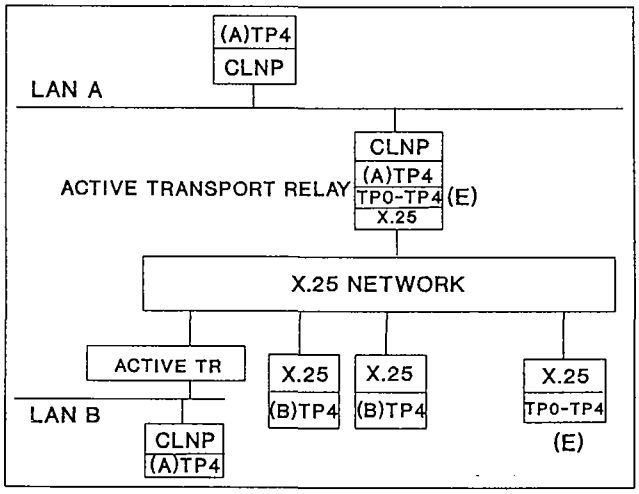

FIGURE XI-IV. NETWORK CONFIGURATION WITH ALL THE DIFFERENT ISO PROFILES USING ACTIVE TRANSPORT RELAYS.

Figure XII shows this protocol combinations when using ISO transport protocols, together with the options allowed by TCP/IP.

The interconnection of LANs can be done in three ways. One is by the use of an X.25 WAN (stacks B and C), another is by the use of direct links connecting CLNP routers (See figure XI-V). The third way is the interconnection by the use of bridges presented in chapter 11.6. In the second case the ISO line protocol to be used is HDLC as is indicated in figure XII.

A fourth possibility, the use of X.25 over both LANs and WANs, is not normally used.

The C) combination uses TP4 over CLNP/X.25 to access a Packet Switching Network. The operation of CLNP over X.25 PLP is standardized in ISO8473. In clause 8.4.3. of this standard the necessary convergence functions are defined.

The D) combination uses TP4 over an ethernet link layer, and the network layer is empty.(INLP = Inactive Network Layer Protocol).

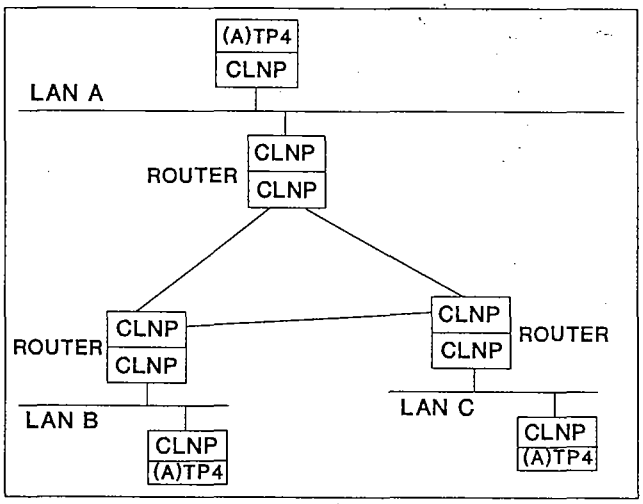

FIGURE XI-V. INTERCONNECTION OF ROUTERS VIA DIRECT LINKS

CLNP must be used to span several networks.

It is not possible for all the computers in figure XI to communicate with all the others in the configuration shown. The following comments to figure XI explain with are the possible communications.

- The computers labelled with the same letter can communicate among them.
- Type A and C computers can communicate over diffe rent networks by the use of X.25 routers.
- Type B computers can communicate directly with other B computers only over the X.25 network. They can also communicate with type A computers by the use of the active or passive Transport Relays specified by TR10172.
- B and C computer cannot interoperate.
- C computers are less efficient in transmitting data than B computers.
- CLNP may be null, in this case it is called Inactive Network Layer Protocol (INLP) and it has a header of only one byte set to zero. The computers using the INLP cannot communicate outside of their LAN (Computers type D) except by the use of a transport relay assuming that CLNP can be negotiated down to INLP.
- Type A and type D can communicate on the same LAN if CLNP can be negotiated down to INLP.
- Both ELCOM and IDEC support the configurations A,B,C and D in figure XI

Besides ELCOM-90 allows other combinations using TP2.

For better understanding figure XI has been split into five figures (XI-I, XI-II, XI-III, XI-IV and XI-V) one for each type of interconnection system, representing in each of them only the types of computers and stacks that interoperate by the use of the represented interconnection system.

Another interconnection possibility is by the use of GATEWAYS including the complete ISO stack up to the 7th layer.

When using gateways really each constituent network is really an independent ISO domain. The relay application running on top of the seven layer stack may perform any desired functions. This makes this type of interconnections attractive when special security tasks are to be performed. The inconvenient is the use of a machine with more software and protocols that may imply reduced performance, specially throughput.

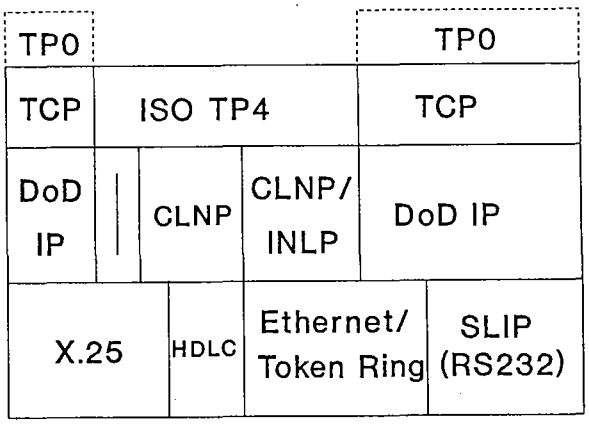

FIGURE XII. PROTOCOL COMBINATIONS WHEN THE OSI TRANSPORT PROTOCOL AND TCP/IP ARE USED.

11.8 PROTOCOL STACKS AND NETWORK CONFIGURATIONS USING TCP/IP TRANSPORT PROTOCOL

TCP/IP is very attractive because many LANs use TCP/IP today. This means there are many TCP/IP products available, and it is possible to interconnect TCP/IP based LANs with X.25 and leased lines.

The most interesting protocol stacks when using TCP/IP are:

A) TCP/IP over LANs

B) TCP/IP over X.25

C) TCP/IP over SLIP

SLIP is the Serial Line Internet Protocol, a packet framing protocol which defines a method of sending Internet datagrams over a serial line (RS-232).

Fig.XII shows the different protocol combinations.

Fig.XIII shows a network with all the possible configurations.

In this configuration most of the computers can communicate. However, the type C computers may have difficulties to communicate with the other computers. This depends on the function of the hybrid computer with the profiles A and C. It is possible to use the same technique as for the ISO Transport Protocol and use a gateway function on top of the application layer. However, if the computer supports IP routing functionality for SLIP lines, the type C computer can communicate with all the other computers.

An alternative is an IP router with SLIP functionality. In this way the type C computer could either use dial-up lines to the IP router or leased lines and access all the other computers.

The ELCOM protocol supports TCP/IP and the configurations in figure XIII, whereas WSCC and IDEC do not.

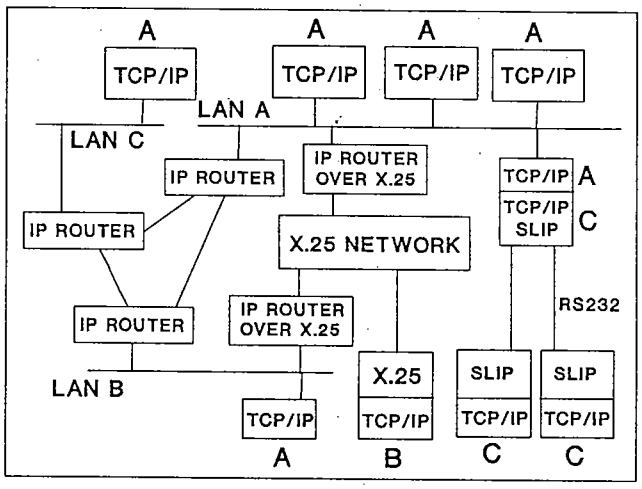

FIGURE XIII. NETWORK CONFIGURATIONS WITH ALL THE DIFFERENT TCP/IP PROFILES.

12.TELECONTROL AND THE TRANSPORT LAYER

12.1 TELECONTROL REQUIREMENTS FOR TRANSPORT PROTOCOLS

The Telecontrol requirements for transport protocols are complete interoperability (ability to communicate between any two end systems even over concatenated networks of different nature), performance (interoperability must be achieved in an economic/efficient manner), integrity (the communication must be robust against errors), and availability (the communication should be robust against network failures).

The figures that apply for integrity and availability are the end-to-end requirements defined by IEC[9) and CIGRE [10] for Telecontrol services.

The most relevant integrity figure is the undetected error probability of 10E-10 for integrity class IEC-12, specific for event initiated transmissions and a bit error rate of 10E-4.

Performance with respect to delay is basically a matter of the Network Layer. The common agreement is that data transfer one-way delay should be under one second [11]. In general the TL has little influence on delay.

ISO introduces another concept, resilience, that can defined as the probability of a TS provider initiated TC release (i.e. issuance of a T-DISCONNECT indication with no prior T-DISCONNECT request) during a specified time interval.

The TP4 tries to minimize resilience and this has consequences that are dealt with in the following chapters. This is the same to maximize the probability of not being released due to underlying errors.

To our best knowledge there is no requirement for this concept yet set for Telecontrol.

12.2 THE TRANSPORT LAYER IN TELECONTROL STANDARDS/RECOMMENDATIONS

The standards for Electric Power System Messaging (EPSM) being developed by IEC in the series of documents 870-6 (Telecontrol protocols compatible with ISO and CCITT standards) will define Functional Profiles for EPSM completely complying with ISO standards up through layer 6 and at least ACSE in Layer 7.

The Functional Profile for Electric Power System Messaging (FP-EPSM) will take decision about the options, parameters and classes to be used to fulfil the needs specific to telecontrol.

One of the aims of this report is to serve as a basis for the work in IEC.

More than one Functional Profile for Electric Power System Messaging (FP-EPSM) may be developed to account for different requirements and/or evolving technology.

Development of a standard FP-EPSM incorporating ELCOM-TASE (Telecontrol Application Service Element) will be started at once.

Potentially applicable on-going developments, including WSCC (Western System Coordinating Council) and MMS (Manufacturing Messaging Specification), will be closely followed and evaluated for possible standardization.

A Functional Profile includes an Application Profile, a Transport Profile and the description of the contents of the PICS (Protocol Implementation Conformance Statements) documents.

The Application Profile defines :

for the Session layer : the ISO standards, choice of functional units, parameters of Quality of Service,options and SPDUs and SPDU parameters.

- for the Presentation layer: the ISO standards, choice of functional units, services corresponding to Session functional units, parameters of Quality of Service, options, PPDUs and PPDU parameters, and abstract and transfer syntaxes (for the definition of data structures and their coding for transmission, respectively).

- for ACSE in the Application layer: the ISO standards, choice of services and APDUs, parameters of Quality of Service, options, and parameters of the APDUs.

- for TASE in the Application layer: choices of options, Quality of Service,....

The Transport Profile defines :

- for the Transport layer: the ISO standards (COTS, Protocol Class 4 for example), parameters (maximum TPDU length, time-out,....).

- for the 3 lower layers : the ISO standards (for CONS or CLNS over different subnetworks PSDN, CSTN, leased line...), the values of the parameters,.....;

The Transport Profile can be completed by Relay Profiles for the relaying between subnetworks.

Next,three stacks of protocols used in Telecontrol are commented.

12.2.1. ELCOM

The recent upgrading of ELCOM-83, a joint definition of the whole stack of protocols for Communication between control centers pushed up by several vendors and leadered by the Norwegian Electric Power Research Institute, to ELCOM-90 introduces the transport layer which was non existent in the first release.

Due to the de facto situation ELCOM-90 accepts both TCP/IP and ISO transport protocols and looks to a migration to the latter in the future. ELCOM-90 is not only for communication between control centers but also for communication between RTUs and control centers.

When using ISO transport protocols ELCOM allows two possibilities, TP2 and TP4, running over X.25 and IP (ISO 8473), thus supporting both, wide and local area networks. The recommended standard for LANs is Ethernet (ISO 8802/IEEE 802.3). Token ring is an option.

The ISO T-EXPEDITED DATA primitive option is not used.

ELCOM supports TCP/IP as an option, but IEC only favours the other option, the ISO transport protocol.

12.2.2. WSCC

The WSCC (Western Systems Coordinating Council) stack of protocols in its 1984 version [12], introduces a non ISO transport protocol running over an X.25 network layer (exactly the GTE Telenet version of X.25).

The WSCC transport protocol assumes the X.25 network layer to deliver good enough quality of service and,thus, the transport protocol do not try to improve it, being similar to ISO TP2 for the services it provides. The transport primitives are basically ISO, so allowing an easy migration to ISO transport protocols. The ISO T-EXPEDITED DATA primitive option is not used. Besides there are The following special WSCC transport primitives: RESET (request, indication, response, confirm), STATUS indication and RESTART (request, indication).

12.2.3. IDEC

The IDEC (Interutility Data Exchange Consortium) stack of protocols in its release A.1 (1990) [13], introduces only the ISO Class 4 Transport layer running over both X.25 (ISO 8208) and IP (ISO 8473) network layer, supporting, thus, both wide area networks and local area networks. For LAN connections, the recommended standard is ETHERNET (ISO 8802/IEEE 802.3). The use of Token ring (IEEE 802.5), is an option).

Table II indicates several characteristics of ELCOM, WSCC and IDEC protocols with regard to the TL.
Table II.Differences and similarities among ELCOM, WSCC, and IDEC transport layer approaches.

PROTOCOL	TYPE OF TRANSPORT PROTOCOL	UPPER LAYERS (>4)	LOWER LAYERS (<4)	TYPE OF TRANSPORT PRIMITIVES
ELCOM (1990 version	ISO:TP2/TP4 NON ISO: TCP/IP	Session: empty Present/ Applic.: ELCOM specific	X.25 LANs: Ethernet (Option: Token Ring)	ISO TCP/IP
WSCC (1984 version) [12]	NON ISO	Connec-tionless NON ISO	X.25	ISO plus additions
IDEC (1990 version) [13]	ISO:TP4	Session: ISO8327 Present/ Applic.: IDEC Message Service Option:ISO	X.25 LANs: Ethernet (Option: Token Ring)	ISO

TABLE II. DIFFERENCES AND SIMILARITIES AMONG ELCOM, WSCC AND IDEC TRANSPORT LAYER APPROACHES.

12.3 THE IMPORTANCE OF TP4 FOR TELECONTROL

Since the five ISO Transport Protocol classes do not interoperate, the requirement of complete interoperability implies that each end system must run at least one common class of transport protocol.

LANs are normally considered to be of type C because of their connectionless nature even for administrative purposes and thus the applications running on them will have to use ISO TP4.

It was argumented that for Telecontrol, X.25 networks should be considered of type C and thus requiring also the use of TP4.

Thus most of the Transport Protocols in the case of Telecontrol will need to be of Class 4. This favours the uniforms use of TP4 for Telecontrol. But there are still more points favouring this position:

- The state machine description of class 3 is more complicated than that of class 4 and provides less functions. Thus Class 3 should not be a serious contender regarding any criterion.

- Comparisons of performance between TP4 and TP2 show that the differences are small. Class 2 has the same efficiency in overhead and is only slightly worse in processing time compared to Class 4 with no checksumming. Nevertheless according to ISO8073 if the system implements class 4, it shall also implement class 2.

- The choice of TP4 over X.25 in a Wide Area Network allows the use of the much simpler and efficient Passive Transport Layer Relay suggested in ISOs TR

10172 for relaying into LANs using Internet.

- Also the choice of only one class of TP is a simplification in the operation of the network and a guarantee of uniform quality.

- TP4 implementations show throughputs of hundreds of Kbit/s and even a few Mbit/s that present no limitation for Telecontrol.

- The model introduced in chapter 14.5 shows that the use of a stack of protocols using ISO TP4 in layer 4 over HDLC or X.25 in lower layers comply with IEC integrity classes I1 and I2. Thus, it should be concluded that this stack is adequate for the telecontrol application.

And finally there are the functions not provided by the other TP classes and listed in chapter 4.

All these reasons allows to consider very convenient the uniform use of TP4 for Telecontrol with the exception of TP2 that according to ISO standards should be supported if TP4 is. This use of TP2 may be interesting for connecting industrial systems to administrative ones.

12.4. QUALITY OF SERVICE ASPECTS

Transmission media are not perfect and are subject to errors and disconnections. To combat this the link layer is necessary, but it protects only up to certain extend that is related to link protocol complexity and efficiency. The network layer is also unreliable, being able to lose, change the contents of packets or their sequence.

As a result of it, the Network layer finally provides a quality of service to the Transport layer that may be not enough for the application. The gap is to be bridged by the Transport layer, being this adaptation between the quality of service requirements of the application and the quality of service provided by the Network layer, the most relevant function of the Transport layer from the point of view of a demanding application such is Telecontrol.

Some impairments suffered by packet networks are the following:

- Average Delay
- Variation of Delay
- Throughput limitation
- Undetected Error Rate
- Lost NPDUs
- Missequenced NPDUs
- Duplicated NPDUs
- Disconnections/resets of Network Con nections
- Misdelivery of NPDUs.

The transport layer, within its function of bridging the gap between the quality of service delivered by the network layer and the quality of service required by the application, has to overcome all these impairments up to the necessary extend.

The previous network impairments can be classified in two classes. The first class is formed by the impairments that can be corrected at the Transport layer and the second class is formed by those that can only be to a limited extend. When severe,the impairments of this second class should be corrected in the lower layers.

12.4.1.NETWORK IMPAIRMENTS CORRECTABLE ONLY TO A LIMITED EXTEND AT THE TRANSPORT LAYER.

The main impairment not correctable by the Transport layer is Delay.

It is obvious that the delays incurred by packets in the lower layers cannot be recuperated at the Transport Layer. This means that the requirements of delay sensitive application should be fulfilled by the three lower layers. So the network must be designed with installed capacities, routing features, call set-up facilities, etc, designed to cope with the strongest delay requirements.

Some of these requirements may be:

A limit on round-trip delay for interactive applications (commands, etc).

A limit on call set-up times.
A limit on transit delays.

And these limits may be expressed in averages or in thresholds only exceeded by some small percentage of the cases or both requirements for each type of data.

Nevertheless delay can be influenced by the TL window, by priorities and by splitting over multiple connections.

Some special aspects of classical telecontrol systems may be difficult to handle by some networks because of their delay sensitivity, namely:

- The freezing command.
- The snap-shot command.
- Clock synchronization.

But probably their characteristics may be relaxed a little or even some of them be suppressed or solved some other way in modern systems.

Another typical delay sensitive application in Telecontrol Telecommunications networks is the Teleprotection/Teletripping command. This Application is now handled by dedicated links because of its extremely low delay requirements in the range of 15-60 msec.

Another main impairment over which the TL has a limited impact is Throughput limitation.

Throughput limitation can be mitigated by the Transport layer by splitting over multiple connections or data paths.

12.4.2.NETWORK IMPAIRMENTS CORRECTABLE AT THE TRANS PORT LAYER. DATA INTEGRITY.

The rest of impairments, the ones that impact the concept of data integrity, are correctable up to the necessary extend at the TL but only at the expense of adding delay, with techniques such as the following:

To recover from lost NPDUs: A sender retransmission upon time-out-mechanism based on the expiration of a timer and a possible request from the receiver to the sender.

To recover missequencing: Numbering at the source and reordering at the receiver.

To recover from duplications: Also by numbering and discarding already received numbers.

To recover from errors:By the use of error detecting/correcting codes usually combined with an automatic request mechanism.

The techniques mentioned are used by ISO Class 4 TP and allow to obtain a very high data integrity.

Error Correcting Codes are not used at the Transport layer neither by ISO nor by TCP/IP. Their use would only be justified in networks with a very high error rate.

It is interesting to note that the added delay is essential to the recuperation tasks.

12.5 ACHIEVING HIGHER DATA INTEGRITY IN THE TRANSPORT LAYER VERSUS ACHIEVING IT AT THE LOWER LAYERS

12.5.1.GENERAL SITUATION

There are two points of view for error recovery in data networks.

One is that the function of the network layer is to provide an error free packet pipe from source to destination site and that error recovery should be done at the network layer. One of the advantages of this approach is that the error recovery mechanisms can take advantage of the mechanisms used in the network layer for routing and flow control. Also recovery can take place in the communications network where typically implementation is simpler, because of the homogeneous nature of the nodes.

The other point of view is that the communication network can be designed with a lower quality of service requirements on data integrity and adapt to the desired level of quality of service at the transport layer.

This is consistent with the todays trend to simplify lower level protocols to achieve higher transmission speed typically over media with low error rates such are fibber optics and digital radio links.

The second point of view is supported also by the fact that sometimes messages travel through several networks to reach their destination. (This is particularly common where local area networks are used to access wide area networks). The different kinds of communication networks traversed may not then be able to assure end-to-end recovery, making it necessary to provide a solution at the transport layer within the external sites. Also, in the case taken into consideration, packet sizes may change on passing from one network to another.

In this case it becomes natural to provide an end-to--end acknowledgment on a message rather than a packet basis, again making error recovery more appropriate at the transport layer.

Also some sessions require a much higher degree of protection against errors than others. Error recovery at the transport layer can provide different degrees of added protection to different sessions.

Finally the standardization bodies have provided with five Transport protocol classes that allow to adapt to a wide range of situations between the two previous points of view, including them.

12.5.2.THE CASE OF X.25 BASED DATA NETWORKS

Since Telecontrol is a demanding application requiring high data integrity figures it turns out that networks that can be considered type A or B for other applications may be considered of type C from the point of view of Telecontrol.

For instance, X.25 networks which are normally considered type A from the point of view of administrative data networks, may be considered type C from the point of view of Telecontrol.

In this case the choice protocol for the TL in Telecontrol systems operating over X.25 networks would be again TP4.

As said in paragraph 12.1., the most relevant integrity requirement for Telecontrol is the undetected error probability of 10E-10 for a bit error rate of 10E-4.

This figure cannot be achieved by X.25 packet switching networks [14,15,16] and therefore the gap in integrity should be fulfilled by the Transport Layer.

Because of the previous arguments we submit that for Telecontrol, X.25 networks should be considered of type C and thus requiring the use of TP4. This situation would make it advisable to use TP4 in all Telecontrol systems.

The integrity model given in chapter 14.5 shows that TP4 over X.25 achieves an integrity level that is well within IEC integrity class I2. This shows that the combination is adequate for telecontrol.

Also, when using public networks (always based on X.25 access), it is difficult to know the internal network implementation and its effect on the residual error rate, thus again it is advisable to use TP4 over public networks.

In general if the application quality of service requirements are very stringent, it is probably desirable to use Class 4 Transport Protocol even over allegedly reliable networks.

The routing procedure within packet networks as well as the network internal operation are not standardized and in fact there are many routing procedures in operation in different networks. What has been standardized is the access to packet networks. This standard is known as X.25 and was first developed by the CCITT in 1978 with later successive updatings [6].

The X.25 protocol includes definitions of the three lower layers for accessing packet networks.

Nevertheless X.25 includes at least one feature belonging to the Transport Layer. It is the D or Delivery t included in the header of X.25 packets that indicates whether the acknowledgment has end-to-end significance or not.

If the D-bit is set to 1 then the reception of an acknowledgment with the number RN signifies that the destination site has received all packets for the session previous to RN, that RN is awaited, and that the source is free to send a window of packets from RN on.

If D=0, RN signifies only that the local packet switching node to where the terminal is connected has received packets previous to RN, that RN is a awaited, and that the terminal is free to send a window of packets from RN on.

It is possible for some sessions to use end-to-end significance and for others only access significance.

X.25 protocol is such that it must receive packets in correct sequence, otherwise the connection is restarted again. This means that the Transport layer will receive, in this case, packets in sequence and without lost or duplicated packets. Nevertheless there may still be a too low undetected packet error rate and too many disconnections, resets or restarts reported to the Transport layer, and so the network connections can still be considered of class C and need a class 4 TP no matter whether the D-bit is set to one or to zero.

12.5.3 THE CASE OF NETWORK CONNECTIONLESS TRANSMISSION

Network connectionless service is available by following the ISO network access standard CLNS (Connectionless Network Service).

LANs are usually connectionless and if OSI is adopted, the choice should be based on CLNS.

When using a Network connectionless access protocol, provision has to be made at the Transport layer to recover from lost, missequenced and duplicated NPDUs specially over concatenated network. So, clearly, a Class 4 protocol is needed in that situation.

Recognising this fact ISO 8073/ADD2 standardizes that the only class that can be used to provide COTS over the CLNS is Class 4.

So, LANs are considered, even for administrative data networks, as type C networks.

The ISO Standards 8072 and 8073 focus exclusively into connection-oriented communications in which a Transport connection must be set-up and then terminated.

Transport connectionless transmission is available as an option an is described in detail in two ISO standards documents ISO 8072/addendum 1 and ISO 8602.

Network connectionless service on WAN is only possible when using non standardized/recommended network layer protocols, since neither ISO nor CCITT have defined the corresponding protocol.

One feature similar to connectionless transmission available in X.25 is the Fast Select service, where user data is appended to the Call Request packet. The only difference with connectionless transmission is that in that case the packet is acknowledged at the network layer.

12.6 THE CONNECTIONLESS TRANSPORT PROTOCOL (CLTP) AND TELECONTROL

The Connectionless Transport Protocol is a simple protocol that may include as an option a checksum. This means that the CLTP may achieve the same data integrity as TP4 with respect to the protection against errors.

Thus the integrity model given in chapter 14.5 also applies to CLTP and so it should be concluded that the use of CLTP in layer 4 over HDLC or X.25 in lower layers complies with IEC integrity classes I1 and I2. This allows to conclude that, from the point of view of data integrity, this stack of protocols is also adequate for telecontrol.

The CLTP also allows priorities at the TPDU level, and interesting feature deserving more attention since it may be useful for Telecontrol, specially because it is a characteristic that does not exist in the other options such as the measurement of the throughput achieved in previous network connections or the sending of a round trip fictitious data TPDU to estimate the delay.

CLTP may be of interest for Telecontrol for instance to transmit cyclical telmetering data in a connectionless-mode.

CLTP is clearly not adequate for providing transport service for any telecontrol application.

Nevertheless its convenience for some telecontrol applications suggest to use it in combination with TP4 in order to allow the application to choose the most adequate service for telecontrol.

13 DISCUSSION OF SPECIFIC TOPICS OF INTEREST FOR TELECONTROL IN RELATION TO TP4.

In this paragraph a series of different topics of interest or possible concern for Telecontrol in relation to ISO TP4 are discussed with the aim of clarifying or giving an opinion on each of them. Some of them are an extension/compilation of comments in previous chapters.

Topic 1.Lack of continuous QOS monitoring at the application layer.

QOS parameters are transmitted only in the request primitive and not in the data primitives. This means that there is no QOS monitoring at the application layer during the data transfer phase.

This is a possible matter of concern for Telecontrol where connections may be permanent or very long and where there is the habit of controlling the QOS at the application layer.

In general the ISO solution for the problem of QOS monitoring is that the TL should be responsible for maintaining the agreed QOS, thus it has to monitor the connection and to disconnect in case of not being able to provide the desired QOS.

Acting like this the application knows that the QOS is the required one if the TC is maintained. In case of disconnection it can try to reconnect and be again informed about the new QOS in the corresponding service primitives.

The real concern is that there are not yet procedures defined to monitor QOS at the Transport Layer during data transfer and that, even during the negotiation phase, the only thing that can be done is to assume that sufficient a priori knowledge exists to derive a correct QOS.

Work on the subject is under way in ISO.

One procedure to inform the application layer could be to reconnect periodically at the TL. In this way the application would have a periodic refreshment of the QOS.

Topic 2.Lack of Priority at the Data Unit level

In the case of using the connectionless TP, the priority does apply to each individual TSDU.

But the service definition of the connection oriented TL contains only the idea of relative priority of a connection with respect to other connections but not the relative importance of different data units of one connection.

Specifically, the associated parameters, included in the QOS parameters, specify the relative priority of the connection with respect to :

- The order in which connections are broken to recover resources,if necessary.

- The notion of the relative priority of different messages sent over a given connection is not included in TP4

A possible solution is the establishment of several transport connections with different priorities for conveying different types of data (for instance, periodic measurements (low priority) and changes of status, alarms and commands (high priority).

But the main concern lies in that the way priority is managed is not clearly defined.

Priority may affect to the TL operation, but the main issue is the ability to pass the priority parameter down to the network layer and even more to have a subnetwork capable of managing priorities. Currently few subnetworks can offer this.

Topic 3 : Accumulation of different events in the Residual Error probability.

The probabilities of lost, duplicated or corrupted TPDUs are accumulated in only one figure termed Residual Error Probability.

In our opinion this accumulation may be confusing. To this respect one practical situation happens when using ISO Class 4 TP. This protocol Reorders and recovers from lost and duplicated TPDUs and thus these two probabilities are of no importance in this case. Nevertheless the probability of errored TPDUs is still of importance since it allows to decide whether to use the checksum or not.

The accumulation of figures may imply always using the TP checksum.

When using only TP4, as may be common in future Telecontrol systems, the Residual Error Probability would better refer only to the rate of corrupted TPDUs.

Topic 4. Abrupt disconnection

The disconnection process as specified by ISO does not guarantee that user data already on fly will be delivered once the disconnection process has started.

The NBS version of TP4 includes a function called "Graceful Close Down" that solves the problem at the Transport Layer.

ISO provides this function in the ISO session layer (Negotiated Release) and thus it is no longer a problem when using the whole ISO stack of protocols.

Anyway, since many connections in Telecontrol are permanent the abrupt close of ISO TPs may be probably considered irrelevant and it is always possible to wait some reasonable period of time after sending the last octet of data before closing a connection.

Topic 5.Overhead

In Telecontrol most of the TCs are permanently connected. Thus the overhead comes primarily from the Data TPDUs that include a Transport header of between 8 and 11 bytes, and the corresponding acknowledgments (AK TPDUs) which have a length between 6 and 12 octets or even more.

The problem with overhead is more important for systems with short user data messages as is typically the application of Telecontrol. This means that in layered Telecontrol systems the application should favour the generation of longer data messages by waiting for more data within the constraints imposed by the Telecontrol application.

We suggest to study the limits in waiting imposed by the Telecontrol application.

Overhead also affects delay, This side-effect of overhead may be important when using low speed channels.

Topic 6.Reachability or broken network connections control

An important functions in Telecontrol is to decide whether a RTU is connected to the network or not.

This is called the reachability function.

This function is provided by TP4 by sending acknowledgment (AK) TPDUs periodically over inactive but alive connections. The receiving transport entity disconnects if the inactive time is too long. The mechanism involves two timers, inactivity timer and window timer. The window timer ensures that there is a bound on the maximum interval between AK TPDUs and thus upper limits the time without activity in alive connections.

In this way TP4 protects the transport user against unsignalled breaks in the network connection or failures of the peer transport entity, a necessary and interesting function for Telecontrol.

Topic 7. Broken network detection duration

TP4 provides improved resilience against network disconnections by allowing multiple simultaneous network connections (splitting). Thus there may be no delay associated with the breaking of a NC provided that there are at least two.

This is an interesting feature but, unfortunately, when only one connection exists and after receiving a network disconnect, TP4 tries by all means to use other NCs and if none is available it waits for a new NC to appear.

Finally the issuing of a T-DISCONNECT is only decided upon the expiration of the Inactivity or Retransmission timers or when a disconnect or error TPDU is received from the other end.

This two timers may have typical values of at least a few minutes.

This delay between the reception of a N-DISC and the issuing of the corresponding T-DISC may be too long for Telecontrol and probably it would be better to inform the transport user as soon as possible by issuing a T DISC.

In any case this is a subject suggested for further study.

This is not only the case of TP4. We think that this is a problem also in TP classes 1 and 3. These classes also try to reassign the TC to another NC and, although they do no rely on timers to finally issue a transport disconnect, they do it after the use of complex algorithms that may involve delays also in the order of minutes.

Topic 8. Use of the Expedited Data option

The concept of EXPEDITED-DATA provides a mechanism for expediting the delivery of occasional urgent data. This mechanism is, however, subject to stringent and limiting rules concerning its use. It is not intended as a steady state data transfer mechanism.

The ISO expedited data mechanism specifically precludes sending any new normal data after transmitting an expedited data message until the expedited data acknowledgment is received.

This has an undesirable throttling effect which occurs because the ED TPDU is transmitted ahead of any

pending normal data and all normal data transmissions are suspended until the expedited data message is acknowledged.

This standardized procedure ensures that the expedited data TPDU will be delivered to the transport user at the other end before any normal data TPDUs sent after it.

The T-EXPEDITED-DATA request primitive may carry a maximum of 16 octets of transport user data to its transport entity.

The NBS specification allows some normal data, the one received from the sending user before the expedited data and retransmission, to be transmitted while the expedited data acknowledgement is awaited, thus reducing the idle time incurred by the ISO scheme during expedited data transfer.

The EXPEDITED DATA is an option negotiated during the connection establishment phase.

Although expedited data may have some similarity to priority, it does not have to be confused with it or used instead of it.

It is our opinion that the expedited data transfer option is not necessary for Telecontrol and that probably it would be better not to use it in Telecontrol systems.

Topic 9. Protection

Protection refers to the extent to which the TS provider attempts to prevent unauthorized monitoring or manipulation of TS-user-data.

The protection feature can be requested during the negotiation of QOS. The concern lies in that the way to obtain such protection is not yet specified by ISO.

Another problem with protection is that, like priority, it requires the use of similar parameters at the network layer, specially within the subnetwork. Currently few networks can offer this.

In our opinion protection is an important function in Telecontrol but not indispensable.

Topic 10.Transmission over very unreliable networks.

None of the ISO Transport Protocols is very well engineered for transmission over networks with many errors (not corrected by the lower layers) or losses. The non existence of selective request produces great reductions in throughput efficiency when errored or lost TPDUs are over 1%. This possible point of concern is not normally a problem in common Telecommunications networks given their good enough quality.

The timer for retransmissions is also critical for performance over networks with errors. This may be a concern over networks with frequent errors and delay variation.

All this can be of concern when transmitting over radio mobile channels or other special channels. In some of these cases the problem can be solved by using link layer error correcting codes.

It can also be solved at the TL. The TL NBS standard includes a selective acknowledgment procedure option that allows TP implementations with this option to interoperate with those implementations which do not use the selective acknowledgment discipline. (This feature of NB is meant for allowing satellite links).

One practical situation may be when using TP4. This protocol reorders and recovers from lost TPDUs,thus these two probabilities are of no importance. Nevertheless the corrupted TPDUs or probability or Residual Error Rate is still of importance since it allows to decide whether to use the checksum or not.

14. ABOUT FLETCHERS'S CHECKSUM

14.1. GENERAL

It is an error detecting technique published in [8] that is specifically designed to be easily implemented in software rather than the typical hardware implementation common to cyclic redundancy checking (CRC) mechanisms used in line protocols.

Computers are word oriented, rather than bit oriented, while CRCs are oriented to performing calculations based on polynomials computations over a binary field.

This makes computers rather inefficient in calculating CRC's by software since they have to shift and test each bit of transmission iteratively or treat short blocks of bits by table look-up.

Nevertheless CRCs are efficiently implemented by hardware and have very desirable error detecting properties and a large theoretical body of results backing them.

This has lead to the implementation of CRC's by hardware in the lower layers but still remains the problem of implementing then by software, a desirable thing in upper layers and specially at the transport layer.

ISO Class-4 transport protocol uses a software oriented integer arithmetic checksum that was first published in the Transaction on Communications,January, 1982 by J.G. Fletcher and as such it is known as Fletcher's Checksum.

This checkum is a bit weaker at detection than CRCs but is more efficient at implementing it by software.

14.2. ERROR DETECTING PROPERTIES

Its error detecting properties are the following:

1 - Except for a higher order effect in the one's complement case, the checksum (like a CRC) detects all but a fraction $1/2^C$ of all errors in the limit of long transmissions, where C is the number of checkbits.

2 - The two's complement checksum (like a CRC) detects all burst errors of length C, where C is the number of checkbits.

3 - The one's complement checksum detects all but a fraction on the order of $C/(K.2^{(C+K-1.)}$ where K is the number of bits in a byte.

4 - The checksum (like a CRC) detects all single bit errors.

5 - The one's complement checksum with at least two check bytes detects all double-bit errors, provided that the erroneous bits are spaced by less than $K.(2^K-1)$ bits, where K is the number of bits in a byte. (This is a smaller spacing than that achieved by a suitable CRC).

Differences with CRC's in detecting capabilities:

- The double-bit error capability presents a smaller spacing than in CRCs. For K=8 and R=2 (16-bit checksum) the maximum spacing is 2040 bits for Fletcher's checksum while in CRC's of 16-bits of length it is of 65535 bits. Nevertheless this should not be a problem in Telecontrol where messages are typically very short (<1000 bits).

- The ability of Fletcher's checksum in detecting triple errors has not yet been investigated. The CRC $X^{16}+X^{12}+X^5+1$ (CCITTs CRC) detects all triple errors.

14.3 DESCRIPTION

A transmission is treated as a sequence of K-bit bytes. Each byte is treated as an integer, and arithmetic is performed on these integers modulo M. The only values of M considered in detail are $M=2^K$ (two's complement arithmetic) and $M=2^K-1$ (one's complement arithmetic). In the former case, if an addition overflows beyond K bits, the overflow is discarded. In the latter case the overflow is added back into the result as an "end-around" carry.

The last R bytes of a transmission are the check bytes.

The most practical values are: K=8 (8-bit bytes), R=2 (16-bit checksum).

The sender and the receiver each maintain a record consisting of R one-byte checksum's C(r), r=0,1, ... R-1, that are all initialized to zero at the beginning of a transmission. As each byte is sent or received it is incorporated into the cheksum as follows: (In the case R-2).

$$C(0) \leftarrow C(0) + B$$

$$C(1) \leftarrow C(1) + C(0) \qquad (1)$$

The 2 checksum bytes are chosen by the transmitter as follows:

$$B \leftarrow (C(0) + C(1)) \qquad (2)$$

Each byte is computed by using the then current values of C(r). The byte is then included into the checksum according to [1].

The receiver expects each C(r) to equal zero when a transmission is complete.

The iterations (1) are easily seen to produce the following final result:

$$C(0) = B_1 + B_2 + B_3 + \ldots + B_n$$

$$C(1) = n\,B_1 + (n-1)\,B_2 + \ldots (2)\; B_{(n-1)}\; B_n$$

Where the information to be transmitted is formed by n bytes B.

14.4 FLETCHER'S CHECKSUM AND HDLC

Flaws in the reliability of LAP-B HDLC are well known [14,15,16] and have caused reluctance in using X.25 for Telecontrol.

The detection capability of HDLC CRC ($X^{16}+X^{12}+X^5+1$) is broken by the Bit Insertion Mechanism of HDLC. This mechanism produce large burst of errors that are only detected by the CRC with probability 2^{-16} [14]

One of the goals of the Transport layer is to correct the lack of reliability of the network layer.
To this respect the question is whether Fletcher's Checksum correct the flaws of HDLC.

In principle the idea of using an arithmetic checksum, a mechanism different in nature to the polynomial CRC used in HDLC, seems very good and probably may allow to consider that the probability of undetected error is at least increased again by a factor 2^{-16} reaching 2^{-32} ($\approx 10^{-9}$), probability that could be considered enough for the Telecontrol application.

It may even happen that none of the bursts undetected by the HDLC could pass the filter of a Class-4 Transport protocol, but this is still to be proved.

This subject is important since it may allow the use of general purpose packet networks and protocols (X.25, HDLC) for Telecontrol. In any case to know up to what extent the probability of undetected error is improved is very interesting for the Telecontrol application.

14.5 INTEGRITY OF AN ISO STACK OF PROTOCOLS WITH HDLC IN LAYER 2 PLUS TP4 WITH THE CHECKSUM OPTION IN LAYER 4.

Here a model of the integrity of an ISO protocol stack using HDLC in layer 2 plus ISO TP4 with the checksum option in layer 4 is presented.

The model is developed in Annex I and it applies as well when the protocol used in layer 4 is the ISO Connectionless Transport Protocol with the checksum option and when X.25 is used in the three lower layers.

It is based on references [8] and [16]

The worst possibility of degradation of HDLC due to a flaw in the HDLC Bit Insertion Mechanism is the insertion or deletion of a bit.

Since TP4 operates in a byte environment where lengths should be multiple of a byte, it is assumed here that insertions or deletions that produce a TPDU with length not multiple of 8, are detected somewhere.

So, the curve labelled "HDLC" in figure XIV of Annex I, that corresponds to the integrity of HDLC when insertions or deletions of bits are not detected, is not applicable here.

In this situation, the worst case event that degrades HDLC is the compensation of an insertion and a deletion of a bit.

This event produces a TPDU of correct length (multiple of a byte). For this situation the applicable integrity curve can be found in reference [16] and is represented by the curve labelled "HDLC plus length detection" in figure XIV of Annex I.

One insertion plus one deletion produces a typically long burst of errors and so the Fletcher's Checksum works on a burst channel. This means that the rate of undetection of this burst will be 2E-16 (See point 1 of chapter 14.2).

Thus, curve "HDLC with length detection" in figure XIV

should be multiplied by 2E-16 to produce the curve represented in figure XV of Annex I, which corresponds to the combination of HDLC at layer 2 plus Fletcher's Checksum at layer 4 (TC4 or CLTP).

Figure XV shows that the data integrity achieved when using TP4 or CLTP in layer 4 over HDLC or X.25 in lower layers complies with IEC integrity classes I1 and I2. This means that, from the point of view of data integrity, these are suitable stacks of protocols for the Telecontrol application.

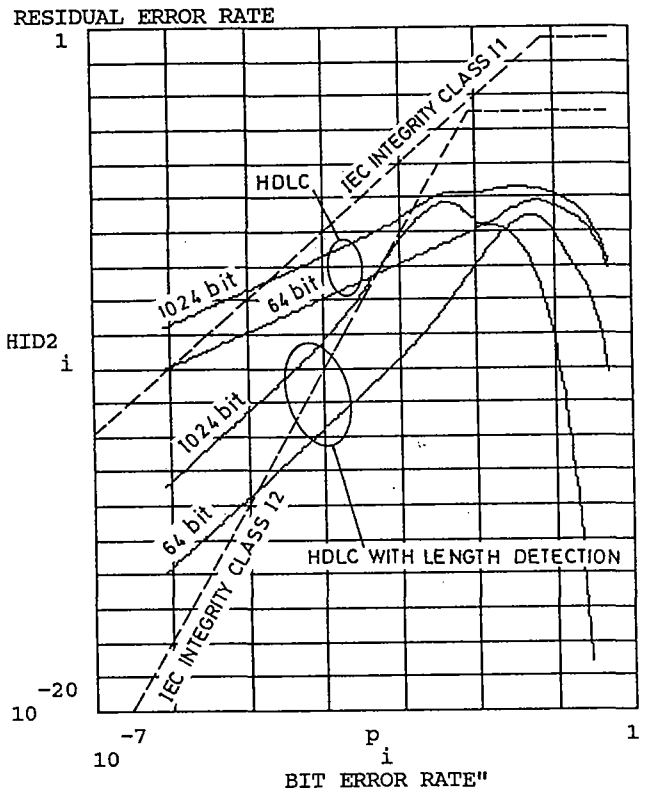

FIGURE XIV. INTEGRITY OF HDLC WITH AND WITHOUT LENGTH MODIFICATION DETECTION

15 CONCLUSIONS

The most important conclusion of this report is that ISO Class 4 Transport Protocol (TP4) basically satisfies Telecontrol requirements over most types of networks, although several undefined topics of possible concern for Telecontrol are identified.

It is also concluded that Class 4 should be preferred or even mandatory. Any other classes should be permitted to operate but none of them should be required except Class 2, that according to ISO standards should be implemented when using Class 4.

The CLTP may also be of interest for some Telecontrol services and we suggest a study of the possible convenience of using it in combination with TP4 so as to allow the application to choose the best transport service for each Telecontrol service.

Despite the convenience of using TP4, this protocol is open and allows many implementations, options and freedom in designing and it also has some unspecified possibilities. This raises many points of interest or possible concern for Telecontrol. Some of them have been identified and commented on.

The ones that produce more concern are those related to the indefinition of procedures for Quality of Service determination and monitoring, the use of priority and protection, the determination of the adequate values for timers and their effect on the time to decide transport disconnections, the overheads involved and others.

The model given in Annex I, for the use of TP4 or CLTP with the checksum option over HDLC or X.25 in lower layers shows that these stacks of protocols comply with IEC integrity classes I1 and I2 and, thus, it is concluded in the Brochure that, from the point of view of data integrity, they can be used safely in telecontrol applications.

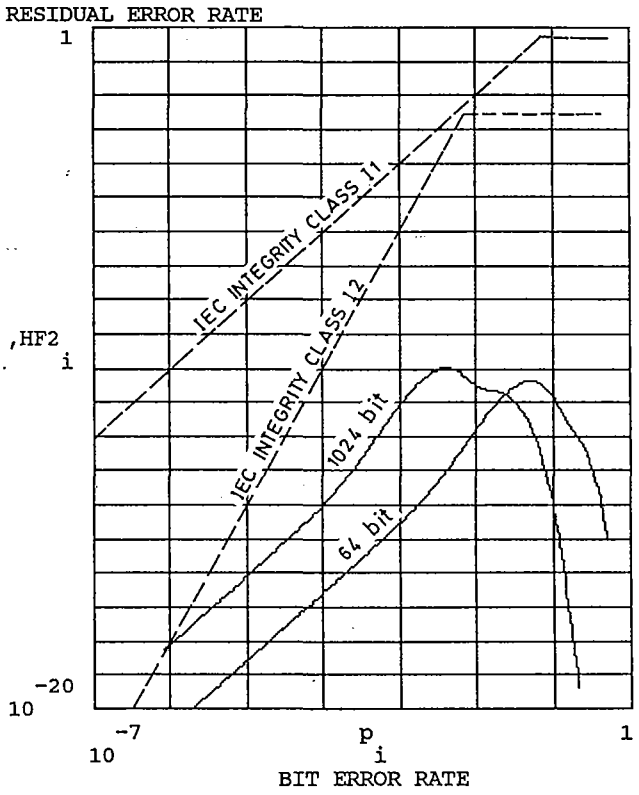

FIGURE XV. INTEGRITY OF AN ISO STACK CONTAINING TP4 OR CLTP IN LAYER 4 AND HDLC OR X.25 IN LOWER LAYERS.

16. REFERENCES

[1] IEC TC57 Draft "Telecontrol Equipment and systems. Part 6: Telecontrol protocols compatible with ISO and CCITT Standards. Section 2-Use of base standards (OSI Layer 1-4)". (May, 1991).

[2] ISO 7498:1984.
Information Processing Systems-Open Systems Interconnection-Basic Reference Model.

[3] K.G. Knightson
"The Transport Layer Standardization"
Proc. of the IEEE, Vol.71, No.12, December 1983.

[4] International Standards Organization (ISO)
International Standard ISO : 8072 : 1986
Information Processing Systems - Open Systems Interconnection - Transport Service Definition.

[5] International Standards Organization (ISO)
International Standard ISO : 8073 : 1986
Information Processing Systems - Open Systems Interconnection - Connection oriented transport protocol specification.

[6] National Bureau of Standards. 1983
Specification of a Transport Protocol for Computer Communications
Volume 1. Overview and Services.
Volume 2. Class 2 Protocol.
Volume 3. Class 4 Protocol
Volume 4. Service Specifications
Volume 5. Guidance for the Implementor
Volume 6. Guidance for Implementation Selection

[7] CITT Recommendation X.25 "Interface between data terminal equipment (DTE) and data circuit-terminating equipment (DCE) for terminals operating in the packet mode and connected to public data Networks by dedicated circuits; Fascicle VIII.3, 1984.

[8] J.G. Fletcher
"An Arithmetic Checksum for Serial Transmission" Transaction on Communications, Vol.COM-30, No.1, January, 1982.

[9] IEC TC57 "Telecontrol Equipment and Systems. Characteristics of Telecontrol Equipment : Transmission Frame Formats" Dec. 1985,part 5.1.

[10] CIGRE-SC35 "Guide for planning of Power Systems Telecommunication Networks".1986.

[11] Selga,J.M., Hegge,J. and Bisci, D. "Technical Report on Requirements and Performance of Packet Switching Networks with Special Reference to Telecontrol". (Proceedings of CIGRE, Paris,19-90).

[12] Western Systems Coordinating Council
"Energy management System inter-utility communication Guidelines"; June 1, 1984.

[13] Interutility Data Exchange Consortium (IDEC)
"IDEC Protocol/Guideline", Release A.1, February 12, 1990.

[14] G. Funk
"Message Error Detecting Properties of HDLC Protocols"
IEEE Transactions on Communications, Vol.COM-30, No.1, January, 1982.

[15] Ma, J.S."On the impact of HDLC Zero Insertion and Deletion on Link Utilization and Reliability".
(IEEE Trans. on Communications, Vol. COM-30, No.2, February, 1982)

[16] Selga, J.M."HDLC Reliability and the FRBS to improve it"
Proceedings of Seventh Data Communications Symposium, Mexico City, October 27-29, 1981.

ANNEX I. INTEGRITY OF HDLC, FLETCHER'S CHECKSUM AND THE COMBINATION

This annex is a program written in MathCAD. It calculates the integrity of HDLC CRC and Fletcher's Checksum. It also calculates the real integrity of HDLC taking into account the flaw in HDLC [14,16], and it finaly calculates the global integrity of an ISO stack including HDLC at layer 2 and Fletcher's Checksum at layer 4.

$i := 7 \ldots 140$

These are the sample points

$N := 64$

The calculation is done for a message length of N=64 bit. Later it is repeated for N=1024 bit.Normally Telecontrol messages have lengths in-between.

$$p_i := \frac{1}{\exp\left[\frac{i}{10}\right]}$$

This is to expand the points logarithmically to sample more often the low BER values. It is for representation reasons.
p is the bit error probability.

$$q_i := 1 - p_i$$

q is the bit probability of not having an error

DETECTION CAPABILITY OF HDLC CRC AND FLETCHER'S CHECKSUM

$$FC1_i := \frac{1}{2^{16}} \cdot \left[\left[1 - \left[q_i\right]^N - \left[(N) \cdot \left[p_i\right] \cdot \left[q_i\right]^{N-1}\right] - \left[\left[N \cdot \frac{N-1}{2}\right] \cdot \left[p_i\right]^2 \cdot \left[q_i\right]^{N-2}\right]\right]\right]$$

$$CRC1_i := \frac{1}{2^{15} - 3} \cdot \left[\frac{(N) \cdot (N-1) \cdot (N-2) \cdot (N-3)}{4!}\right] \cdot \left[p_i\right]^4 \cdot \left[q_i\right]^{N-4} + \left[\frac{2^{15} - 8}{\left[2^{15} - 3\right] \cdot \left[2^{15} \cdot 5\right]}\right] \cdot$$

$$\left[\frac{(N)\cdot(N-1)\cdot(N-2)\cdot(N-3)\cdot(N-4)\cdot(N-5)}{6!}\right]\cdot\left[p_i\right]^{6}\cdot\left[q_i\right]^{N-6}$$

PROBABILITIES OF VARIOUS EVENTS ACCORDING TO REF [16]

Probability of occurrence of a "Flag" in an HDLC message due to noise(PFN):

$$PFN_i := \left[1-\left[1-\left[\frac{1-2\cdot q_i^{5}+5\cdot q_i^{6}-4\cdot q_i^{7}}{252}\right]^{N-8}\right]\right]$$

Probability of having the trailing "Flag" of an HDLC message destroyed by noise:

$$PF_i := q_i^{2}\cdot\left[1-q_i^{6}\right]\cdot 2^{-16}$$

Probability of having at least one bit deletion in an HDLC message of N-bit length:

$$PDN_i := \left[1-\left[1-\left[\frac{1-q_i^{5}}{126}\right]\right]^{N-7}\right]$$

$$j := 1\ ..\ \mathrm{floor}\left[\frac{N+1}{5}\right]$$

$$INC := \sum_j \left[\left[\frac{N-(5\cdot j)+1}{2^{5\cdot j}}\right]-\left[\left[\frac{N-(5\cdot j)}{2^{5\cdot j+1}}\right]\right]\right]$$

INC = 0.981 N = 64

This is the average increment in length of an HDLC message of length N after passing the HDLC Bit Insertion Mechanism

Probability of having at least one bit insertion in an HDLC message of N-bit length:

$$PIN_i := \left[1-\left[1-\left[\left[1-q_i^{5}\right]\right]\right]^{INC}\right]$$

INTEGRITY REALLY DELIVERED BY HDLC

$$HDLC1_i := \left[PFN_i + PF_i + PIN_i + PDN_i\right]\cdot\left[2^{-16}\right]\cdot q_i^{8} + CRC1_i\cdot q_i^{8}$$

$k := 1\ ..\ \mathrm{ceil}(INC)$

$INCR := \mathrm{ceil}(INC)$

It is the INCrement rounded by excess

PROBABILITY OF HAVING THE SAME NUMBER OF INSERTIONS AND DELETIONS OF BITS IN A HDLC FRAME

$$PID_i := \sum_k \left[\frac{INCR!}{(k!)\cdot(INCR-k)!}\right]\cdot\left[1-q_i^{5}\right]^{k}\cdot\left[1-\left[1-q_i^{5}\right]\right]^{INC-k}\cdot\left[\frac{(N-7)!}{(k!)\cdot(N-7-k)!}\right]\cdot\left[\frac{1-q_i^{5}}{126}\right]^{k}\cdot\left[\left[1-\left[\frac{1-q_i^{5}}{126}\right]\right]^{N-7-k}\right]$$

GLOBAL INTEGRITY OF HDLC IN AN ENVIRONMENT DETECTING CHANGES IN MESSAGE LENGTH

$$HID1_i := \left[\left[PID_i\cdot 2^{-16} + CRC1_i\right]\cdot q_i^{16}\right]$$

GLOBAL INTEGRITY OF AN ISO STACK INCLUDING HDLC AT LAYER 2 AND TP4 WITH FLETCHER'S CHECKSUM AT LAYER 4

$$HF1_i := HID1_i\cdot 2^{-16}$$

NEXT, THE SAME CALCULATIONS COULD BE REPEATED FOR ANOTHER MESSAGE LENGTH (N)

The corresponding figures (XIV and XV) have been moved to chapters 14.5 and 15.

3-5 rue de Metz - F-75010 PARIS