

Data exchange for meter reading, tariff and load control — Local bus data exchange

The European Standard EN 61142:1993 has the status of a
British Standard

UDC 681.3.01:621.382:681.2

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW



Document Sharing Hub

Cooperating organizations

The European Committee for Electrotechnical Standardization (CENELEC), under whose supervision this European Standard was prepared, comprises the national committees of the following countries:

Austria	Italy
Belgium	Luxembourg
Denmark	Netherlands
Finland	Norway
France	Portugal
Germany	Spain
Greece	Sweden
Iceland	Switzerland
Ireland	United Kingdom

This British Standard, having been prepared under the direction of the Power Electrical Engineering Standards Policy Committee, was published under the authority of the Standards Board and comes into effect on 15 June 1993

© BSI 12-1999

The following BSI references relate to the work on this standard:
Committee reference PEL/14
Draft for comment 90/28063 DC

ISBN 0 580 22180 6

Amendments issued since publication

Amd. No.	Date	Comments

Contents

	Page
Cooperating organizations	Inside front cover
National foreword	ii
Foreword	2
Text of EN 61142	5
National annex NA (informative) Committees responsible	Inside back cover
National annex NB (informative) Cross-references	Inside back cover

National foreword

This British Standard has been prepared under the direction of the Power Electrical Engineering Standards Policy Committee and is the English language version of EN 61142:1993 *Data exchange for meter reading, tariff and load control — Local bus data exchange*, including corrigendum, March 1993, published by the European Committee for Electrotechnical Standardization (CENELEC). It is identical with IEC 1142:1993 published by the International Electrotechnical Commission (IEC).

Direct local data exchange is a means for reading a single meter whereas local bus has the ability to read multiple meters.

A British Standard does not purport to include all the necessary provisions of a contract. Users of British Standards are responsible for their correct application.

Compliance with a British Standard does not of itself confer immunity from legal obligations.

Summary of pages

This document comprises a front cover, an inside front cover, pages i and ii, the EN title page, pages 2 to 128, an inside back cover and a back cover.

This standard has been updated (see copyright date) and may have had amendments incorporated. This will be indicated in the amendment table on the inside front cover.

English version

Data exchange for meter reading, tariff and load control — Local bus data exchange

(IEC 1142:1993)

Echange des données pour la lecture des compteurs, contrôle des tarifs et de la charge —
Echange des données par bus en local
(CEI 1142:1993)

Zählerstandsübertragung, Tarif- und Laststeuerung Datenaustausch über örtlichen Bus
(IEC 1142:1993)

This European Standard was approved by CENELEC on 1992-06-16. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the Central Secretariat or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the Central Secretariat has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and United Kingdom.

CENELEC

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

Central Secretariat: rue de Stassart 35, B-1050 Brussels

Foreword

The text of document 13(CO)1016, as prepared by IEC Technical Committee No. 13: Equipment for electrical energy measurement and load control, was submitted to the IEC-CENELEC parallel vote in October 1991.

The reference document was approved by CENELEC as EN 61142 on 16 June 1992.

The following dates were fixed:

- latest date of publication
of an identical national
standard (dop) 1994-01-15
- latest date of withdrawal
of conflicting national
standards (dow) 1994-01-15

Contents

	Page		Page
Foreword	2	4.7 Functional specification of secondary station transmitter	110
1 General	5	4.8 Functional specifications of secondary station receiver	111
1.1 Scope and object	5	Annex A (informative) CRC 16	112
1.2 Normative references	5	Annex B (informative) DES encryption	112
1.3 Definitions	5	B.1 Introduction	112
1.4 List of abbreviations or acronyms used	7	B.2 Encryption and decryption algorithms	113
2 Local bus data exchange — secondary station (SLAVE)	11	B.3 DES operating modes	119
2.1 Specification	11	B.4 Choice of operating mode	122
2.2 General requirements	11	B.5 Development and tests	122
2.3 Basic principles	12	Annex C (normative) Random number generation (NAO) for response from forgotten unit	123
2.4 General organization of frames and exchanges	14	Annex D (normative) Random number generation for authentication	124
2.5 General organization of the protocol	22	Annex E (normative) Coding blocks in a frame	125
2.6 PHYSICAL layer	25	Annex F (normative) Possible cases for BERREUR (I,J) and BTIMOUT (I,J) fields	126
2.7 DATA LINK layer	39	Annex G (informative) HEX-ASCII correspondence	127
2.8 SESSION layer	46	Annex H (informative) Bibliography	127
2.9 APPLICATION layer	52	Annex ZA (informative) A-deviations	128
2.10 Summary and inter-layer relationships	59	Figure 1 — Signal envelope on the bus	105
3 Local bus data exchange — primary station (MASTER)	62	Figure 2 — Ferrite pot and bobbin	107
3.1 Introduction	62	Figure 3 — Associated components of the magnetic plug	108
3.2 General reminders	62	Figure — DES enciphering algorithm	113
3.3 Tables A received and B returned by the protocol	62	Figure — Key schedule calculation	117
3.4 Activation of protocol and concatenation of exchanges	70	Table — Initial permutation (IP)	114
3.5 PHYSICAL layer	73	Table — Final permutation IP^{-1}	114
3.6 DATA LINK layer	79	Table — Bit selection	115
3.7 SESSION layer	85	Table — Permutation P	116
3.8 APPLICATION layer	92	Table — Key permutation PC-1	117
3.9 Synopsis and inter-relationship between layers	102	Table — Key schedule of left shifts LS	118
4 Local bus data exchange — hardware	105	Table — Key permutation PC-2	118
4.1 General	105		
4.2 General characteristics	105		
4.3 Bus specification	106		
4.4 Magnetic plug	107		
4.5 Functional specifications of primary station transmitter	109		
4.6 Functional specifications of primary station receiver	110		

1 General

1.1 Scope and object

This International Standard describes a method for local bus data exchange, where a number of tariff devices in a given area are connected by a dedicated bus; all of these tariff devices may then be read by connection of a hand-held unit to a central magnetic plug.

This standard presents hardware and protocol specifications for local systems, while specifications for a remote system falls within the scope of another standard.

Considering the fact that several systems are in practical use already, particular care was taken to maintain compatibility with existing systems and/or system components and their relevant protocols.

This standard is specific for local bus systems. In these systems, a hand-held unit also known as primary station or MASTER is connected to several tariff devices also known as secondary stations or SLAVES through a dedicated bus having a flexible structure.

The master is connected to the bus by a magnetic (inductive) plug. The bus itself is passive and all the tariff units — the number of which is limited — are electrically isolated from it.

The protocol is also based on OSI and uses four layers: PHYSICAL, DATA LINK, SESSION and APPLICATION.

The protocol permits the reading and programming of tariff devices. It allows for the detection and identification of so-called “forgotten” units that are not registered in the portable terminal’s data base.

The protocol has been designed to be particularly suitable for the environment of electricity metering, especially as regards electrical isolation, and software security. While the protocol is well defined, its use and application are left to the user. The use of the local bus system for point to point communication is also left to the user.

1.2 Normative references

The following normative standards contain provisions which, through reference in this text, constitute provisions of this International Standard. At the time of publication, the editions indicated were valid. All normative standards are subject to revision, and parties to agreements based on this International Standard are encouraged to investigate the possibility of applying the most recent editions of the normative standards indicated below. Members of IEC and ISO maintain registers of currently valid International Standards.

ISO 7480:1984, *Information processing — Start/stop transmission — Signal quality at DTE/DCE interfaces*.

ISO 7498:1984, *Information processing systems — Open Systems Interconnection — Basic Reference Model*.

1.3 Definitions

address

sequence of binary digits indicating the destination of a communication or set of data

alternate

transmission on a data circuit in either (half duplex) direction

tariff device

fixed data collection unit, normally linked or combined with an electricity meter

call

process consisting of sending signals to set up a link between stations

baseband

transmission of a signal at its original frequency band without undergoing any modulation

baud

unit of speed of modulation

BCD

abbreviation for “Binary Coded Decimal”. Coding of a decimal figure between 0 and 9 using 4 bits

bit

acronym for binary digit

buffer

buffer memory

bus

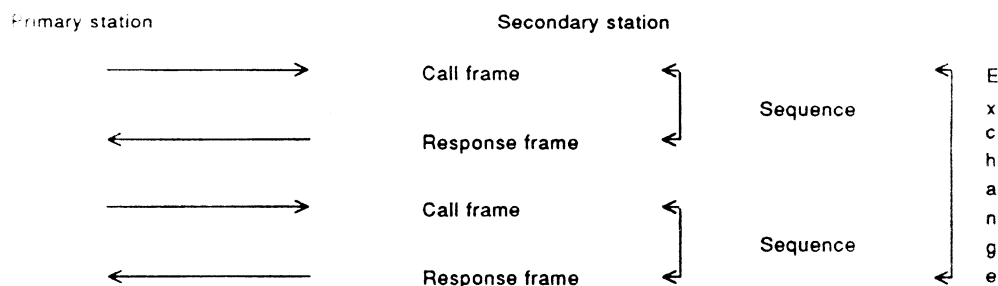
wired system of communication connecting stations and permitting a single communication at a time

flag

symbol used to indicate the particular status of a data item or unit

exchange

set of several frames constituting the whole of a remote reading or programming transaction



Organization of an exchange

remote data exchange

data exchange between one or a group of tariff devices and a data concentrator via a communications network

local data exchange

data exchange between one or a group of tariff devices and a hand-held unit

polling

process consisting of inviting data stations to transmit one after the other

selective calling

process consisting of inviting one or more stations to receive

polling list

list of data stations to be polled and the order in which they are to be polled

byte

set of 8 significant bits

startover

procedure by which a station attempts to solve conflict or error situations occurring during an exchange, by repeating the failed sequence

protocol

set of conventions required to make remote units co-operate in establishing and maintaining data exchanges

(data) sink

part of a terminal by which data is received from a data link

sequence

subset of an exchange, comprising call and response frames

different sequences

those not corresponding to a re-run procedure. The frames transmitted by the primary station are therefore different, either by way of their control field (as for remote programming), or by way of their TAB field (as in multiple remote readings)

identical sequences

those corresponding to a re-run procedure. In the event of a first call failing, the frame transmitted by the primary station at the time of these sequences is therefore absolutely identical

(data) source

part of a terminal by which data is fed into a data link

station

set of functional units comprising a terminal, an ETCD and their connections

primary station

station having complete control of a link

secondary station

station responding to commands in accordance with a link procedure

synchronization

function to enable processes to interact at a given moment in time

hand-held unit (HHU)

a portable equipment for transferring data to or from tariff devices, or electricity meters

time out

time lapse after which it is accepted that an expected event has not occurred

frame

transfer of a set of consecutive blocks forming a whole for the receiving station

field (block)

functional subset of n bytes in a frame

1.4 List of abbreviations or acronyms used

AADP	Primary station address (table A)
AADS	Secondary station address (table A)
ACLE	Key (table A)
ADG	General Address
ADON	Data (table A)
ADP	Primary station Address
ADS	Secondary station Address
ADTP	Remote programming data (table A)
AG	Wake up call
ALEA	Random variable
ANA	Number of bytes in ADON field (table A)
ANAP	Preceding random number (table A)
ANECHAU	Number of bytes in table A for a unit exchange
APREC	Previous call
APSES	Synchronization flag between APPLICATION and SESSION
AR	Out and return characterizing the different sequences

ARJ	Authentication reject
ASO	Coding of cases of reply to a forgotten station call
ATAB	Type of data (table A)
ATYPE	Type of operation
AUT	Authentication command
BDON	Data (table B)
BERREUR	Error (table B)
BFEx	Standby window number x (table B)
BNA	Random number (table B)
BNDEROU	Number of bytes in diagnostic field on exchange run (table B)
BNECHAU	Number of bytes in table B for a unit exchange
BNR	Number of bytes in BDON field (table B)
BNSEQI	Number of identical sequences (table B)
BTIMOUT	Error on TIME OUT (table B)
BTOB	Error flag on “chatterbox” time out (table B)
BTOCO	Error flag on communication time out (table B)
BTOE	Error flag on transmission time out (table B)
BTOL	Error flag on DATA LINK time out (table B)
CASO	Coding of cases of reply to a forgotten station call
CCITT	International Telegraph and Telephone Consultative Committee
COM	Command
CRC	Cyclic redundancy code
DASO	Forgotten station call flag
DAT	DATA command
DES	Data Encryption Standard
DIB	Drapeau d’Initialisation de Bus
DNA	Negative acknowledgment flag
DON	Data
DRJ	Data rejected
DSO	Forgotten station flag
DTP	Remote programming flag
DTR	Remote reading flag
ECH	ECHo command
EMP	Location
ENQ	ENQuiry
EOS	Last programming frame command
E/R	Transmission/reception
ER	Combination ERLI, ERSSES
ERAP	APPLICATION error
ERLI	DATA LINK error
ERREUR	Protocol error
ERSSES	SESSION error
ETCD	Data communication terminal equipment
ETTD	Data processing terminal equipment
FE	Transmission window
FINEMI	End of transmission
FINPHI	End of PHYSICAL

FR	Reception window
FROMEXT	Flag originating FROM EXternal process
HF	High frequency
HHU	Hand-held unit, also TSP
IASO	Standby window indicator for forgotten station calls
IB	Bus initialization command
ISO/OSI	Open Systems Interconnection
K	Key
LIPHI	Synchronization flag between DATA LINK and PHYSICAL
LISES	Synchronization flag between DATA LINK and SESSION
LON	Length
LSB	Least Significant Bit
LSUP	Number of bytes of data field
MSB	Most Significant Bit
N	Number
NAO	Random number for forgotten station response
NAx	Random number No. x
NAxK	Encrypted random number
NSEQD	Number of different sequences
NTR	Number of remote readings
PAG	Wake up call port
PAREP	Non-reply flag
PHILI	Synchronization flag between PHYSICAL and DATA LINK
REC	Remote programming command (RECORD)
RECNU	Non-reception
RSO	Reply from forgotten stations
RxD	Data reception
SESAP	Synchronization flag between SESSION and APPLICATION
SESLI	Synchronization flag between SESSION and DATA LINK
TAB	Type of data (Table)
TACEO	Cumulative time out between bytes
TACEOM	Maximum cumulative time out between bytes
TAG	Wake up call time
TAGM	Maximum wake up call time
TAO	No-byte time
TAOM	Maximum no-byte time
TA1O	Waiting time for first byte
TA1OM	Waiting time for first byte (maximum first byte time out)
TDP	Table of programming data
TE	Transmission time
TEMPO	Temporization
TFE	Time related to transmission window
TFR	Time related to reception window
TIMAX	MAXimum Time
TOB	“Chatterbox” time out
TOBM	Maximum “chatterbox” time out
TOCO	Communication time out

TOCOM	Maximum communication time out
TOE	Transmission time out
TOEM	Maximum transmission time out
TOL	DATA LINK time out
TOLM	Maximum DATA LINK time out
TP	Remote programming
TR	Remote reading
TRO	Forgotten station response time
TSP	Hand-held unit, also HHU
TxD	Data transmission
ZDT	Reading and programming data field

2 Local bus data exchange — secondary station (SLAVE)

2.1 Specification

The local bus reading protocol is designed to send data over a physical medium between one or more units called secondary stations to a data input unit called a primary station or more commonly a hand-held terminal (HHT) or hand-held unit (HHU). The latter name will be used from now on.

The transmission medium is a job-oriented medium; in other words it is only for use with the data transactions specified in the present standard. Under no circumstances will it be developed towards distribution line carrier (DLC) or telephone type communications without the general principles set out herein being substantially reworked. However, all the general conventions (transmission direction, data coding, etc.) conform to current standardization.

2.1.1 Functions of local bus reading

Local bus reading allows communication with isolated units or units located on a common bus.

The protocol shall support several types of transaction:

- Remote data reading

The HHU gathers data contained in the units.

- Remote programming

The HHU sends data to a unit to change all or part of its characteristics or to clear the data.

For security reasons and to avoid fraud, every remote programming transaction shall be accompanied by a two-way authentication by DES type encryption (see Annex B).

- Detection of forgotten units for deferred reading

Irrespective of the process used for remote reading of the stations on a bus, the protocol shall make provision for several units connected to a bus to be detected, even if they are unknown to the HHU and the higher levels (billing files prepared) so that data can be read from these units at a later stage. It is however specified that in a nominal case, the units on a bus are known to the HHU. Forgotten units are thus uncommon and shall not unduly complicate the simplicity of the principles employed under normal circumstances.

It is possible for a maximum of five units to be unknown to the HHU.

2.2 General requirements

2.2.1 Type of unit and addressing

The units connected to the bus may have different functions (e.g. electricity metering only, gas metering only or another function).

The detection of forgotten units shall be capable of being selective so as to address only certain types of units connected to a bus out of all the units connected to the same bus.

Each unit connected to the bus is given a specific address. Every HHU is also given a functional address to differentiate several possible levels of access.

2.2.2 Availability

The physical connection of an HHU to a bus for the purpose of any of the above-mentioned transactions is only momentary; the protocol selected shall therefore provide for immediate availability of the bus after connection and a non prohibitive transaction time in respect of each individual unit and all the units on a bus.

2.2.3 Compatibility

The number of units connected to a bus may vary between 1 and 100 independently distributed over the physical transmission medium.

There may be different types of remote reading or programming units; the protocol shall be transparent to the type of unit up to application level. Some units may, among other things, understand and accept only one type of transaction (e.g. remote reading only). The protocol of these units shall in all cases be compatible with the protocol specified below and shall not generate any malfunctions.

The protocol used shall be capable of easy installation in the various types of unit without the cost becoming prohibitive. The size of program memory and data required to install the protocol shall therefore be as small as possible.

The level of security and control brought into use is closely connected to the physical characteristics of the transmission medium. These characteristics are specified in clause 4.

According to knowledge as to current requirements in the field of local bus reading, the data to be transmitted is often not more than a few hundred bytes, it is transmitted in one block if possible, or in several blocks if the protocol requires so or if the length of the data exceeds the maximum permitted size for a block. In all cases, provision is made for a transaction which exceeds this nominal framework.

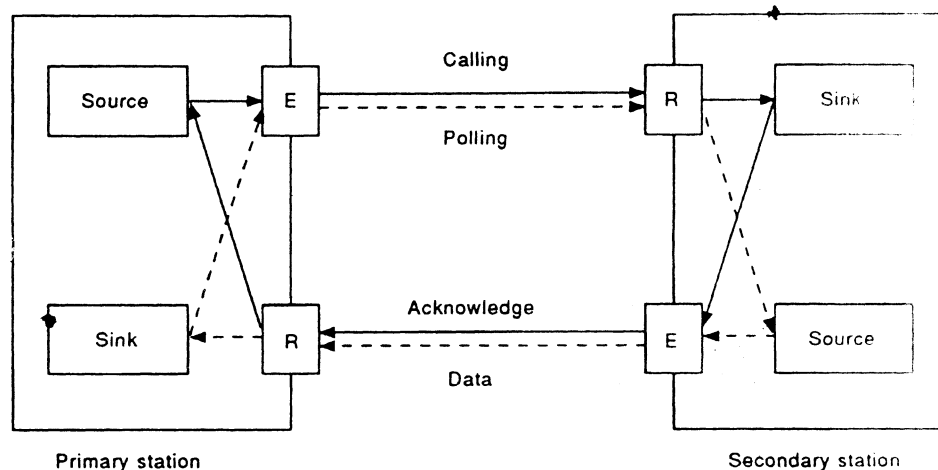
Transmission mode is asynchronous. The transmitter transmits data independently of the receiver. However, the start and end of a word are framed by two signals conventionally called “start” and “stop”. A word consists of an 8-bit byte framed by a start bit and a stop bit.



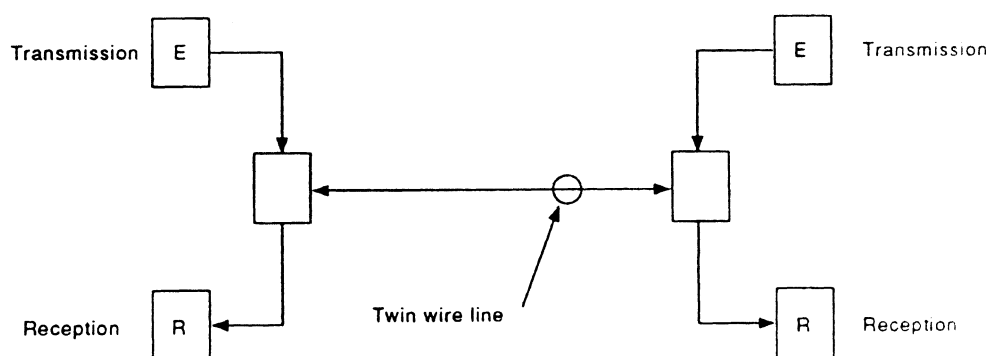
It should be stressed that this mode of transmission does not preclude the use of a more sophisticated higher level procedure (error detection, alternation management, etc.).

In order to comply with CCITT baud rate recommendations, tolerance will be $\pm 1\%$.

The same physical transmission line is used to transmit and receive, but not simultaneously: the data link is half-duplex (alternate).



Organization of the link



Physical organization of the link

The above diagrams only show a point to point link; a multipoint configuration can be obtained by connecting n secondary stations to the primary station shown.

2.3.4 Network access

The system consists of a multipoint bus at a physical level which becomes point to point at a higher level in the majority of cases.

Remote programming

With remote programming, the command function is given to the HHU which is then a data source; the primary station (HHU) invites the secondary station to receive the messages it has to send.

The link here is controlled by “selective” calling.

Remote reading

With remote reading, the command function is given to the HHU which is a data sink; the primary station (HHU) invites the secondary station to send a message.

The link here is controlled by “polling”.

The “polling/selective” function is combined with an addressing system which enables a single secondary station to be selected from the n stations standing by on the bus.

In this operating mode, the system does not have to manage collisions as the calls and responses are perfectly deterministic.

Special case

A special case is the detection of forgotten stations after remotely reading a whole bus. This is fairly unusual as the maximum number of forgotten units on a bus cannot exceed five. An oversight can only occur if there is an error in initializing the address list for the bus contained in the HHU or if there is an error after amending the address list (polling/selective list).

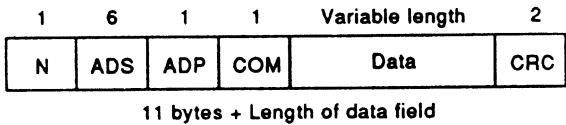
The method of access used is thus by broadcasting with a response from the forgotten stations in random time slots, implying collision handling.

The co-existence of this broadcasting option with the polling/selective method implies uniform acknowledgment handling for compatibility between these two principles.

It should be noted that the broadcast method (with random access) could not be applied to the whole bus without significantly increasing the complexity of the protocol or without significantly increasing the remote reading or programming time, to such an extent that it becomes null and void.

2.4 General organization of frames and exchanges

2.4.1 Format of a frame



A frame consists of six fields which can be grouped functionally.

2.4.1.1 Check field

- N: number using 1 byte (binary) set by the transmitter to show the number of bytes in the frame sent.
- CRC: Cyclic redundancy code using 2 bytes (binary) set by the transmitter and calculated for all (N – 2) preceding bytes (see characteristics of the CRC used in Annex A).

These control elements enable the receiver to verify that the frame has been transmitted error free.

2.4.1.2 Address field

ADS: Secondary station address using 6 bytes (coded in BCD – 2 digits per byte, see Annex E).

The value of this address in decimal is between
 $0 \leq ADS \leq 999999999999$ (12 digits)

In the HHU to secondary station direction, this field is completed by the HHU depending on the station(s) with which it wants to communicate.

In the secondary station to HHU direction, this field is completed via the system by the secondary station with its own internal address (placed in non-volatile memory when each unit is initialized).

NOTE ADS value 0 is reserved as a general address. It is then called ADG.

ADP: Primary station address using 1 byte (coded in BCD – 2 digits per byte).

The values taken by this variable are between (in decimal) $0 \leq ADP \leq 99$

In the HHU to secondary station direction, this field is completed by the calling HHU which inserts its specific address or the general address (ADP = 0). In the opposite direction, if the secondary station answers, it replies with the ADP address(es) to which it has been programmed.

NOTE The address ADP = 0 can be used to determine to which ADP the secondary station has been programmed to respond.

2.4.1.3 Command field

COM: command (coded in 1 byte) telling the receiver the type of action to be taken.

Commands which may be transmitted by the HHU

ENQ: Enquiry — remote reading

REC: Receive — remote programming

AUT: Authentication frame — remote programming

IB: Initialize bus — reset forgotten station flags (DSO) of units connected to the bus for the purpose of calling the forgotten stations.

ASO: Forgotten station call.

Commands which may be transmitted by a secondary station

DAT: Positive response to polling — remote reading (ENQ)

DRJ: Negative response to polling
— remote reading (ENQ) if TAB(i) is unknown
— remote programming (AUT) if programming data is not accepted.

ECH: Response to selection — remote programming (REC)

EOS: Final positive response after AUT command — remote programming.

ARJ: Final negative response after AUT command — remote programming.

RSO: Reply from forgotten station.

2.4.1.4 Data field

Variable length field depending on the frame in use and the type of data requested.

The data is partly application-unique and is therefore not covered by this standard. However, in remote reading, remote programming and calling forgotten stations, fixed fields (length and location in the frame) are used and all application shall take note of this so as to ensure system compatibility. The fields in question are an authentication field (ZA1, ZA2) for remote programming, a field to specify the type of data requested or transmitted (TAB) for remote reading and a field to give a list of the TAB(i) to sensitize the sought-after units in forgotten station calls.

2.4.1.5 Length of frame

In line with currently known and proposed future applications and bearing in mind the desired efficiency of the whole transmission, the maximum length of a frame is 128 bytes. Frames are of variable length. Only the data field can vary from 0 to 117 bytes (128 – 11).

However, the protocol provides for the transmission of several frames of data in succession if the maximum length cannot be adhered to.

2.4.2 Principle of wake up call — physical opening of communication

Before any exchange on the bus, the HHU at its own initiative sends a wake up call designed to alert the communications system of every unit connected to the bus. It should be noted that some of these multifunctional units may use all or part of the communications system for other applications and other links which have absolutely nothing to do with local bus reading.

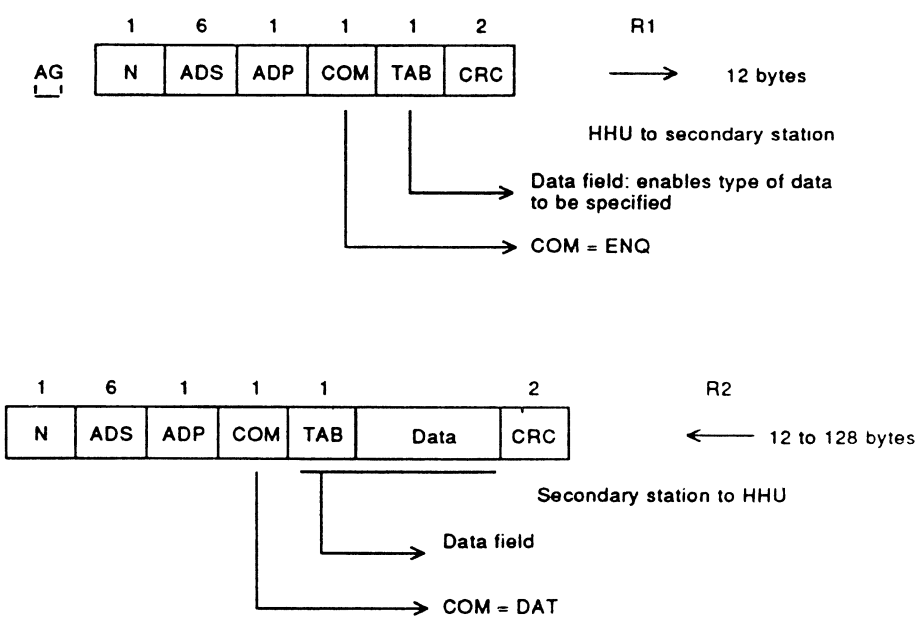
The wake up call consists of a specific sequence which is detailed in 2.6.2.

2.4.3 Principle of detection of an end of frame

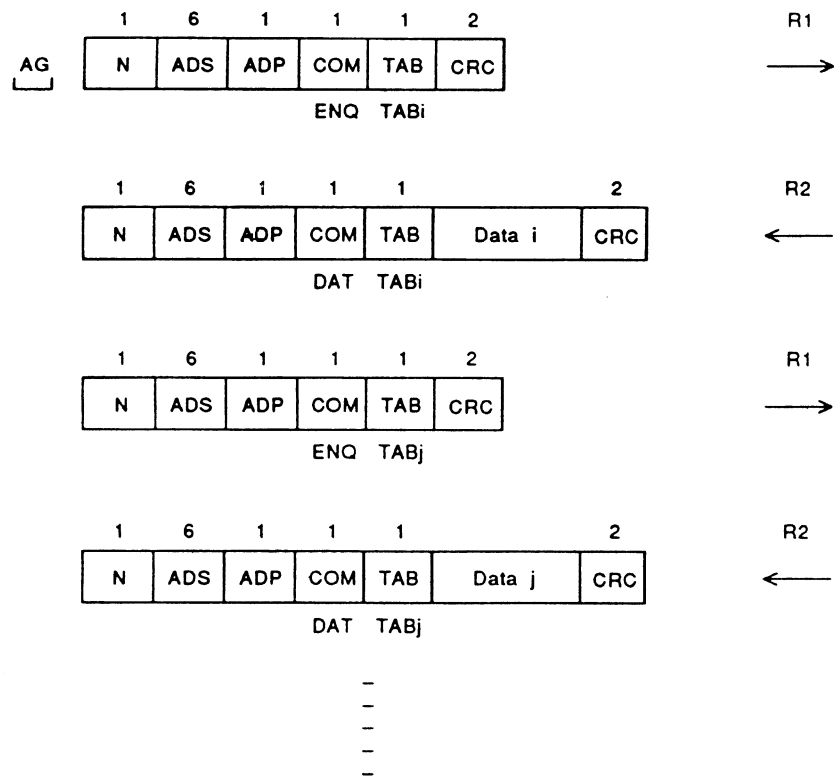
A receiver detects an end of frame when no bytes are detected in the PHYSICAL layer (TAOM) for a given period of time. It then switches from receive mode to standby while it analyzes the frame received and prepares the response frame. When the response frame is ready, the station switches to transmit mode.

2.4.4 Format of a remote reading exchange

2.4.4.1 Nominal example with error-free transmission



2.4.4.2 Example of data transmission spread over several frames

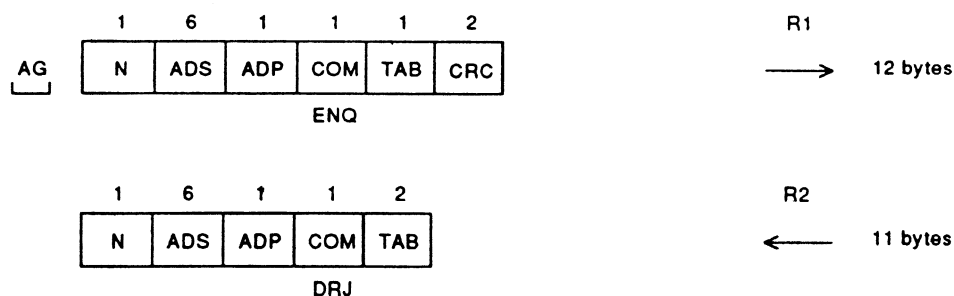


The HHU is able to read the data in succession according to the format of the exchange as specified above. A single wake up call is necessary at the beginning of the exchange.

The exchanges shall comply with the overall communication time and the frame and response time, details of which are given in 2.6.

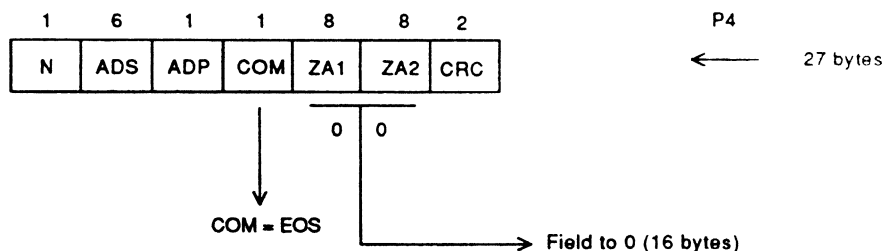
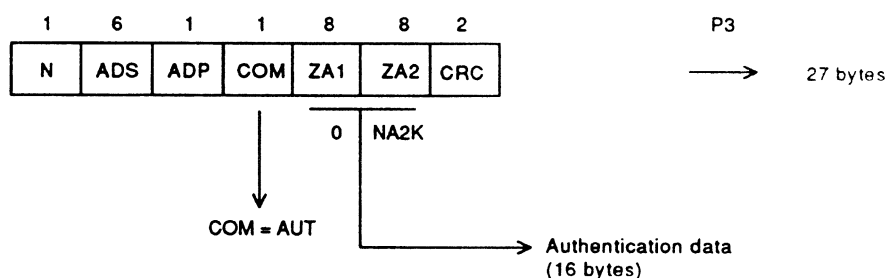
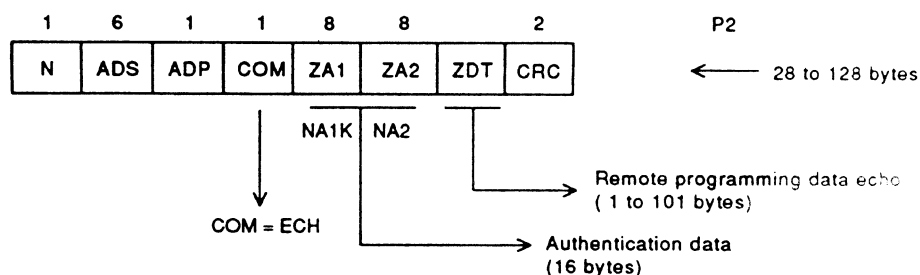
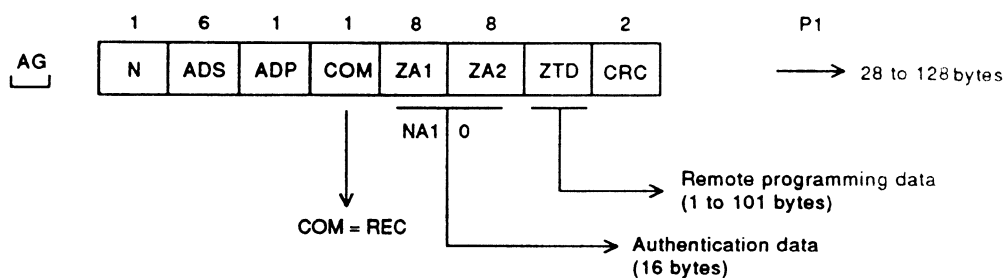
The maximum number of TAB(i) generated during an exchange is five.

2.4.4.3 Example of identifier TAB(i) unknown at the secondary station

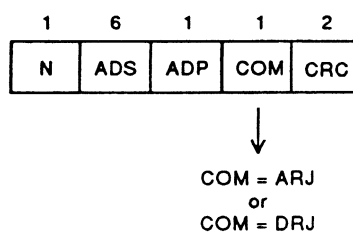


2.4.5 Format of a remote programming exchange

Example of error free transmission



OR



This exchange consists of four frames arranged in two successive return transmissions. In the data field, the first 16 bytes are reserved for authentication purposes. Details of authentication are given in 2.9.3.1. Henceforth, if the specification imposes two-directional authentication and the DES encryption system to be used, a minimum of three frames will be necessary to perform this function.

The first frame contains the remote programming data which is stored in the secondary station without being validated and echoed back on the following frame P2. Frame P3 is then transmitted to conclude two-directional authentication.

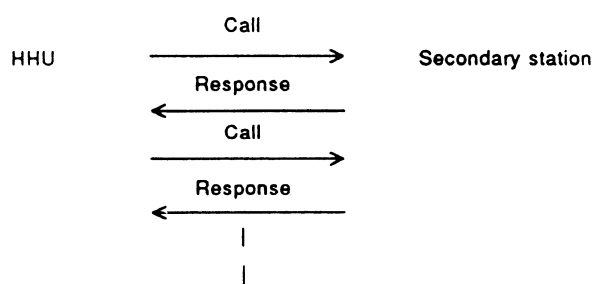
When the secondary station receives P3:

- if authentication is correct and if the remote programming data stored when P1 was sent is validated, a positive acknowledge (COM = EOS) frame P4 concluding the exchange is sent to the HHU;
- if authentication is incorrect or if the remote programming data is not validated, a negative acknowledge frame P4 is returned (COM = ARJ or COM = DRJ).

An ambiguity persists if P3 is received by the secondary station which then validates the data. If the frame P4 transmitted by this station is received in error, the HHU takes it that the data has not been accepted (even after several attempts to repeat P3 with no correct response). In this case, the remote programming exchange will be followed by a remote reading exchange to remove the ambiguity.

2.4.6 Uniformity of remote reading/remote programming exchanges — Example of startover after error

A properly conducted exchange consists of one or more call-response sequences with frames of identical format.



For the primary station (HHU), a remote reading or remote programming type call shall be followed by a response considered as a positive acknowledge or as notification of an error in the type of data transmitted (no startover is provided for in this case).

Detecting an error from a secondary station associated with a poor transmission is translated into a no response which constitutes a negative acknowledge for the HHU. A startover is then attempted at the initiative of the HHU by repeating the call of the defaulting sequence.

An error detected on the response frame received by the HHU initiates the same startover procedure on the incorrect sequence.

Startovers are generated by the HHU. The maximum number of startovers is two. If the exchange is unsuccessful despite these attempts, the HHU halts the exchange with that station and signals a fault.

2.4.7 End of exchange — physical disconnection

The end of an exchange is detected by the secondary station if no further frame is received after a response frame (R2 or P4 type) within a period of time specified at the PHYSICAL level by time TA1OM (see 2.6.2.2). The detection of an end of exchange switches the communication system to standby and it may be used for other applications. No further exchange can then be carried out unless preceded by a wake up call sequence.

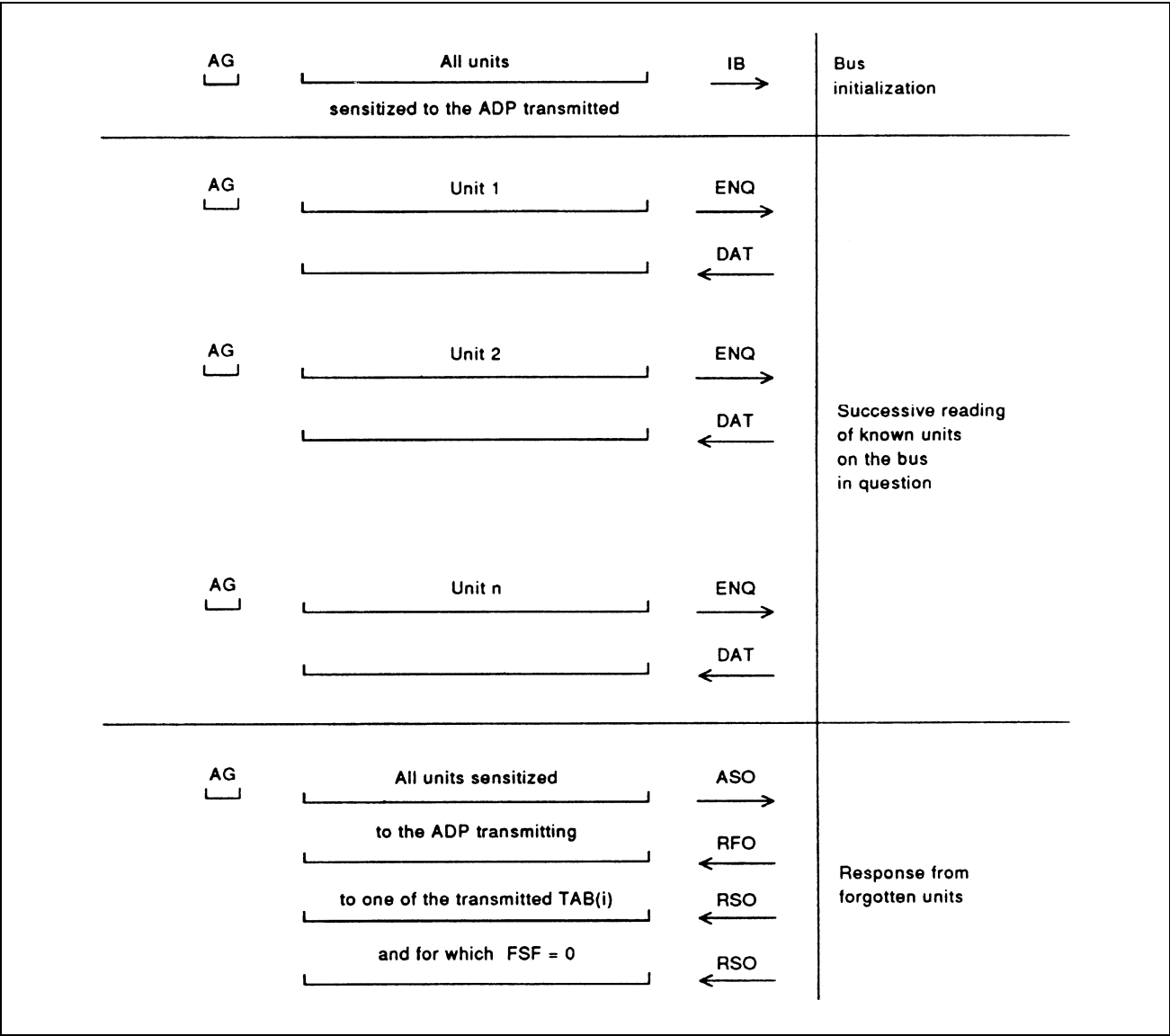
2.4.8 Initializing the bus and calls to forgotten stations

These two modes do not operate on a selective addressing with call-response principle, but on a broadcast with no response principle in the case of initializing the bus and possible responses in random time slots in the case of forgotten stations.

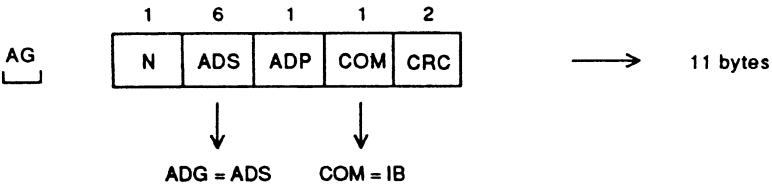
2.4.8.1 Principle of reading a complete bus

For the successive reading of a complete bus, the HHU can ascertain, after reading all the known units, that there are no more units which may have been forgotten and which do not appear in the HHU's files.

Schematic diagram of the sequence used



2.4.8.2 Format of a bus initialization frame



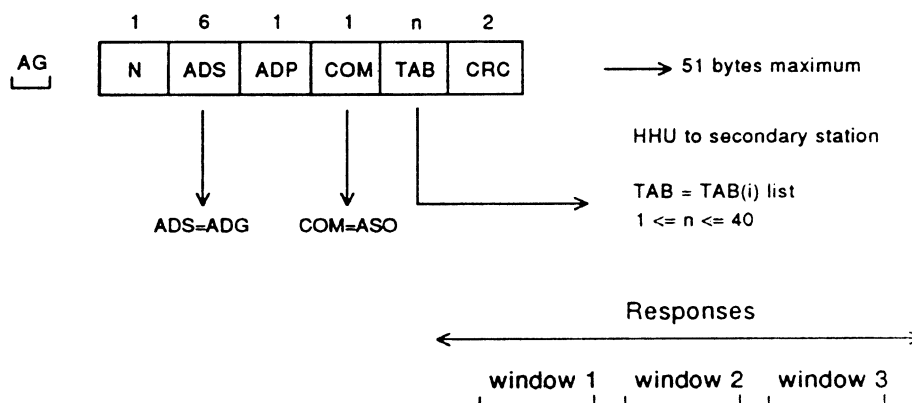
This frame has the same basic format as the others. The secondary station address field now serves to address all the units on the bus without exception and is called general address (value 0 over 12 digits). All units connected to the bus and acknowledging the ADP primary address are thus sensitized. The action of the bus initialization command is to reset a flag in these units to zero (DSO: forgotten station flag).

After the initialization frame, any read unit receiving an R1 frame relating to it (by the presence of its specific address in the ADS field) shows its DSO (DSO = 1) if TAB is known and will then no longer be considered as a forgotten station.

The bus initialization command is never followed by a response.

2.4.8.3 Format of a call to a forgotten station and the associated response

At the end of a remote reading sequence, the HHU can search for “forgotten” units (max 5 in 100). This can only be effective if the preceding “Initialisation and successive reads” sequence is respected.

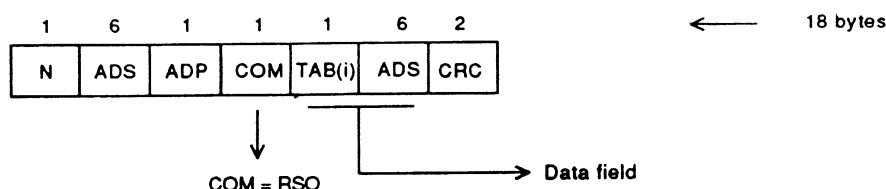


A forgotten station call, preceded by a wake up call, comprises the ADG general address in the secondary station address field. All the stations on the bus sensitized to the ADP of the received frame interpret the ASO command.

If the station's DSO flag is at zero and the ADP address is approved to authorize a response by the secondary station, the station is deemed to have been forgotten and responds to this call if it recognizes at least one of the TAB(i) in the list of its possible TAB(i).

If the station's DSO flag is activated (DSO = 1), the station does not respond and comes off standby for the bus.

This broadcast call implies that several responses may be sent to the HHU. In order to minimize collisions between response frames, each forgotten station has three time slots in which to respond. Each selects its slot at random; the random selection varies from one call to another, the length of the time slot is specified in accordance with the transmission time of a response.



The response frame complies with the general frame format given above; the 7-byte data field contains the first TAB(i) recognized from the list sent in the ASO frame and the 6 bytes of the address of the forgotten unit which is responding.

The HHU opening three monitoring time windows, may be confronted with any of the following situations:

- no response to the three monitoring windows, the HHU knows that no unit has been forgotten on this bus.
- at least one response (no collision) to one of the windows, the HHU records the address of the forgotten unit and proceeds to read it in a subsequent exchange in order to remove it from the group of forgotten units.
- collision response to a window, the HHU cannot act on the response but it knows that there are forgotten units on the bus. It therefore proceeds with another forgotten station call on the assumption that the change in the random selection procedure will enable the responses to be transmitted without collision.

This transmission continues until all the forgotten units are read.

2.4.9 Addressing — Opening and closing the link

On reception of an exchange initiating frame, all units on the bus are standing by to store and interpret the frame. After authentication, which we shall assume is error free, the address is analyzed in order to turn the link into:

Nominal example

- a point to point connection by acknowledging a specific address (selective addressing) in the case of remote reading or remote programming.

All units not recognizing their specific address are “cut off” immediately after this frame (protocol cancelled).

Other examples

- A random access multipoint connection by acknowledging the general address in the case of a forgotten station call (multipoint connection limited to a maximum of 5 units);
- A non response multipoint connection in the case of bus initialization.

2.5 General organization of the protocol

2.5.1 Overview

Protocols usually follow construction rules which give them a certain universality and allow them to be used in other systems. A reference model for Open Systems Interconnection (OSI) has been prepared; this architectural model opens up virtually unlimited possibilities and in particular an arbitrary number of layers.

Local bus reading does not require all the layers specified in this reference model, but the essence of four of them has been used to define an architecture in the application in question: PHYSICAL, DATA LINK, SESSION and APPLICATION layers.

The specification of this hierarchical, decentralized format shall:

- facilitate the design and construction of the protocol from existing basic elements, while minimizing installation costs;
- simplify its operation by offering formal rules;
- guarantee an acceptable system reliability, particularly through strict compartmentalization of the functions, thus avoiding error propagation;
- provide upgrade, expansion and maintenance facilities, thanks to its modular design;
- optimize performance.

The architecture thus presented specifies neither a hardware product nor a software product, but a hardware and software organizational concept with the advantage of a hierarchical structural.

2.5.2 PHYSICAL layer

This layer is intimately related to the hardware used; it specifies:

- the physical characteristics of the transmission medium;
- the characteristics of the connections between the DPTE (Processing Units) and the ETCD (Modems) as well as those of the interface connected to the bus;
- the way in which the physical making and breaking of the connection is performed;
- the half-duplex handling;
- the way in which the binary elements are represented (0, 1): link level, duration, code translation, etc.

2.5.3 DATA LINK layer

The purpose of this layer is to take the binary digits (grouped into bytes) supplied by the PHYSICAL layer and transform them into an error free link for the next layer.

It includes:

- checking the frame by CRC, credibility check on the frame length and the content of certain fields;
- transformation of a multipoint physical connection into a point to point link connection by selective addressing.

Link errors will cause a no-response which, after a TOLM (link time out), will be taken as a no-acknowledge and processed as such by the HHU or the secondary station depending on the sequencing of the original frames.

2.5.4 SESSION layer

The SESSION layer processes the command in successive frames and introduces the APPLICATION data. At this level, it is assumed that all the error detection problems associated with the DATA LINK layer have been resolved; the SESSION layer shall then interpret the action which is required of it (remote reading, remote meter programming, forgotten station call, bus initialization, etc.) introduce any data to be transmitted to the APPLICATION layer and initiate the response procedure by forwarding the field of data associated with the command to the lower layers.

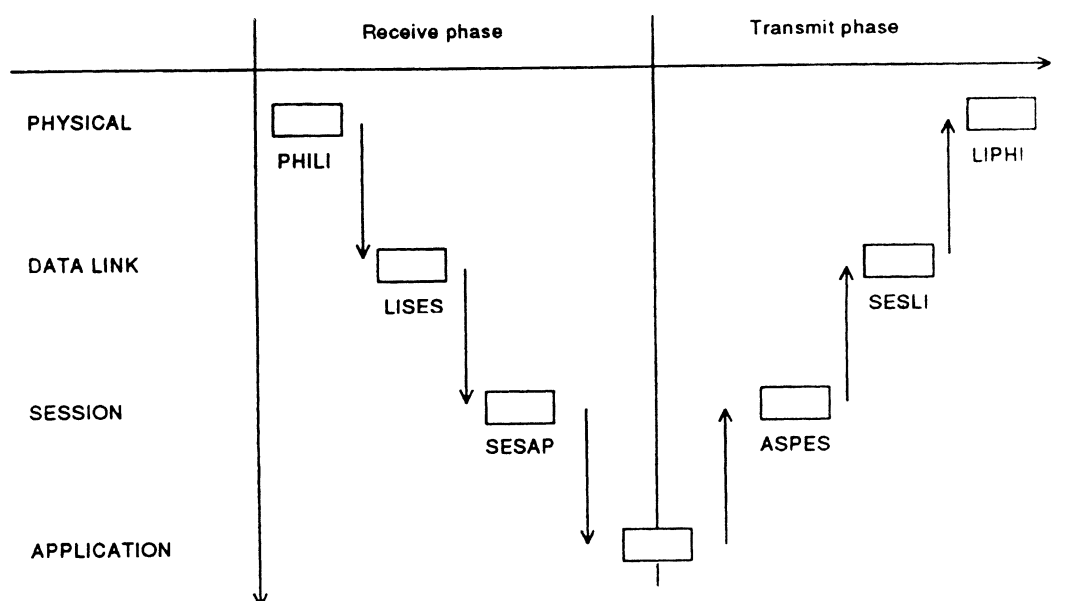
2.5.5 APPLICATION layer

This is the highest level layer. Its job is to forward three types of data:

- authentication data in some cases to ensure that certain transactions are secure and not open to fraud;
- data specifying the nature of the requested information or the type of data in the following fields;
- pure data regarding the remote reading of a unit or remote programming data.

2.5.6 Inter-layer interaction

The progress of the protocol brings each layer into play in succession using synchronization flags.



Nominal layer sequencing and synchronization over a "call-response" sequence

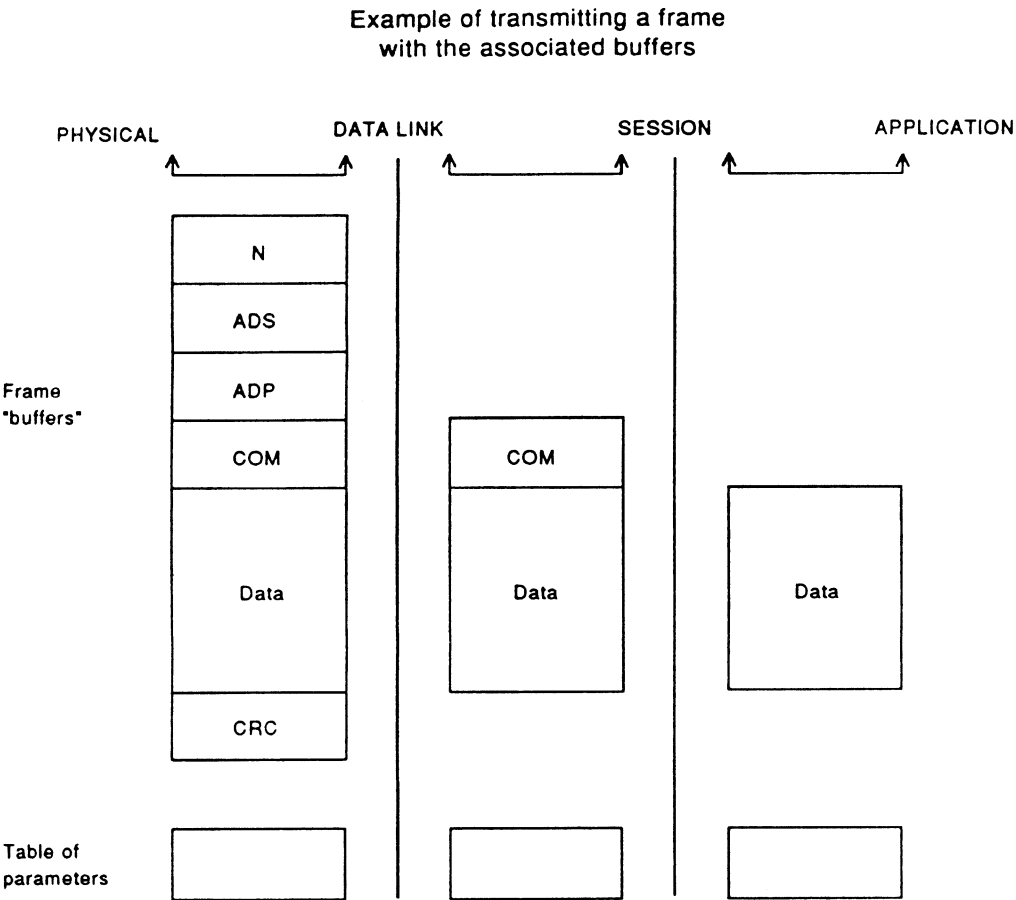
These "receive-transmit" stages follow one another depending on the exchange in progress.

A layer does not pass the synchronization flag to the next higher or lower layer until the task allotted to it has been completed.

Any error in the receive stage (on the secondary station side) is translated by signalling an error flag belonging to the layer in error (ERLI, ERSSES flags), stopping progress through the layers and retransmitting synchronization flags to the lower layers to signal the fault.

Timing is controlled by the PHYSICAL layer so that the inhibiting of one layer does not cause irreversible situations.

Moving from one layer to another may be accompanied by the transmission of parameters and “data buffers” known for example by their memory location (address) and length (number of bytes); such knowledge may be implicit or explicit.

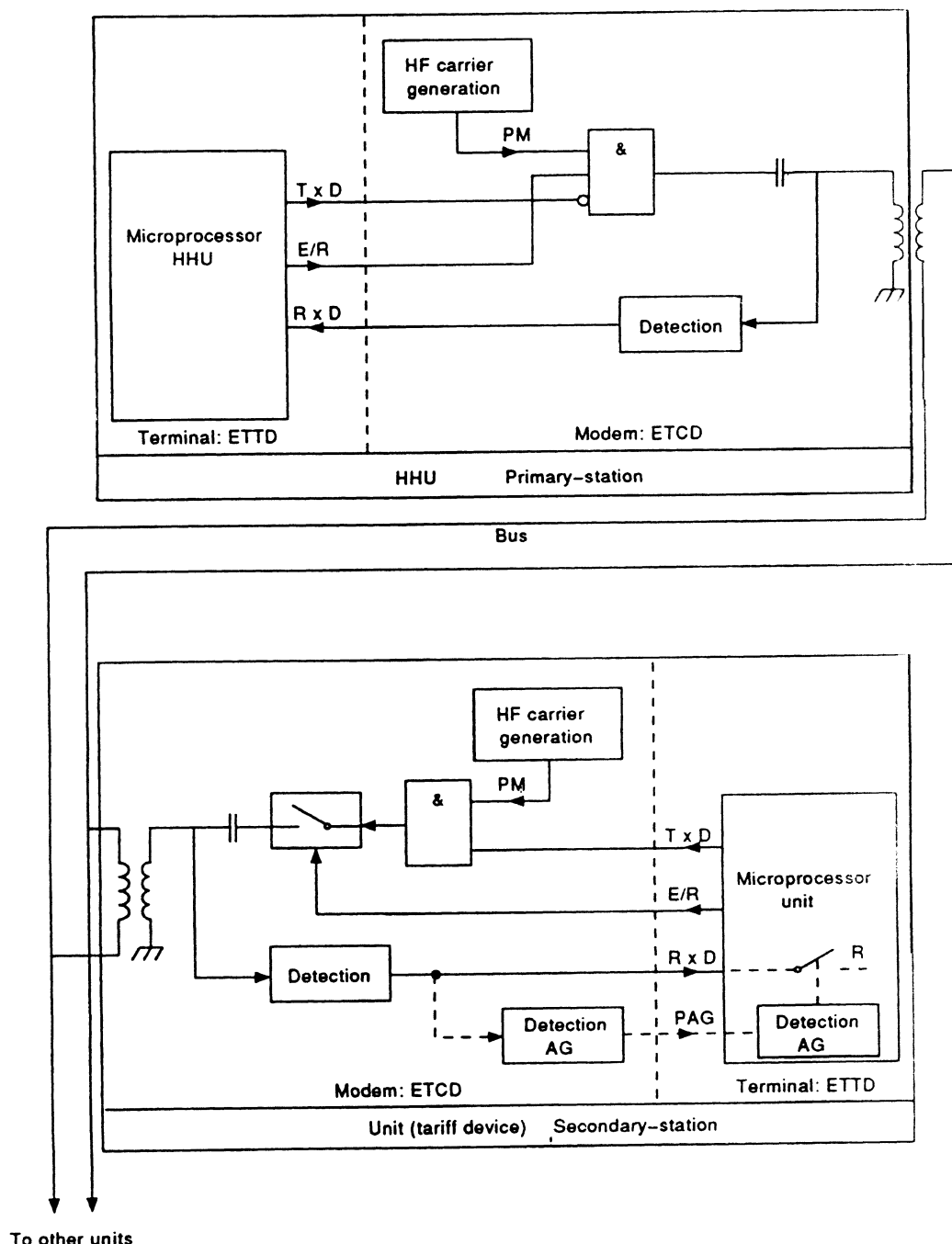


As stated above, these tables may be sent directly from layer to layer or more simply by defining the addresses and lengths of all the component sub-tables.

The parameters are therefore in a known location and always consist of the same number from one layer to another.

2.6 PHYSICAL layer

2.6.1 Hardware overview — Schematic diagram of transceivers



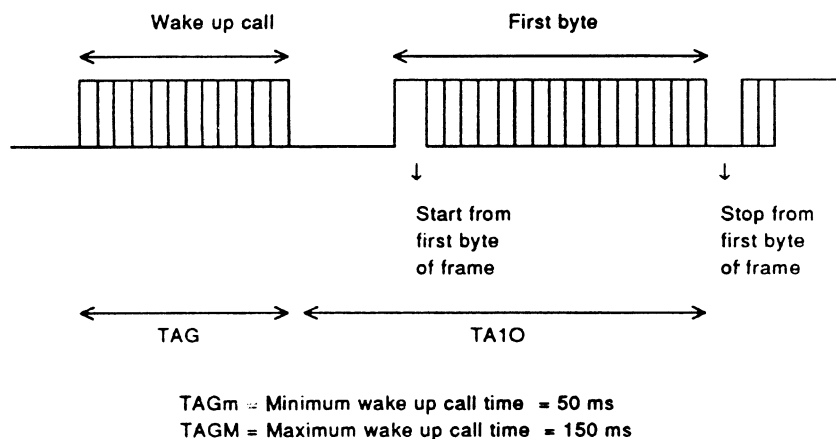
The HF carrier is generated continuously; the T×D serial transmission output modulates the carrier. An outlet port on the ETTD's microprocessor allows the ETCD modem to be switched to transmit or receive. On standby the modem is switched to receive (by E/R) the gate is non pass; the envelope of the signal moving on the bus is therefore permanently available at the microprocessor's serial receive input (R×D). On transmit, the ETTD transmitter is intrinsically monitoring for the bus (by R×D), software locking enables the ETTD's serial port not to be validated on receive (the serial port does not work on Full Duplex). On the primary station side, the system does not need to detect general calls. On the secondary station side, a software or hardware general call shall be detected.

A detailed description of the hardware components used in the modems and the characteristics of the communication medium is given in this standard (see clause 4).

2.6.2 Characteristics of a wake up call

A wake up call is a specific sequence whose job is to put the microprocessor's serial communication receive function on standby. This sequence consists of a continuous carrier for a nominal time of 100 ms (TAG).

2.6.2.1 Representation on the bus



2.6.2.2 Principle of detection — Immunity to interference

The end of a general call shall be followed by the first byte of the frame after a time out for the first byte, TA1O such that:

$$TA1Om \leq TA1O \leq TA1OM$$

where $TA1Om = 30 \text{ ms}$
 $TA1OM = 160 \text{ ms}$

NOTE From the end of the wake up call the secondary station has a maximum time of TA1Om to enter receive mode.

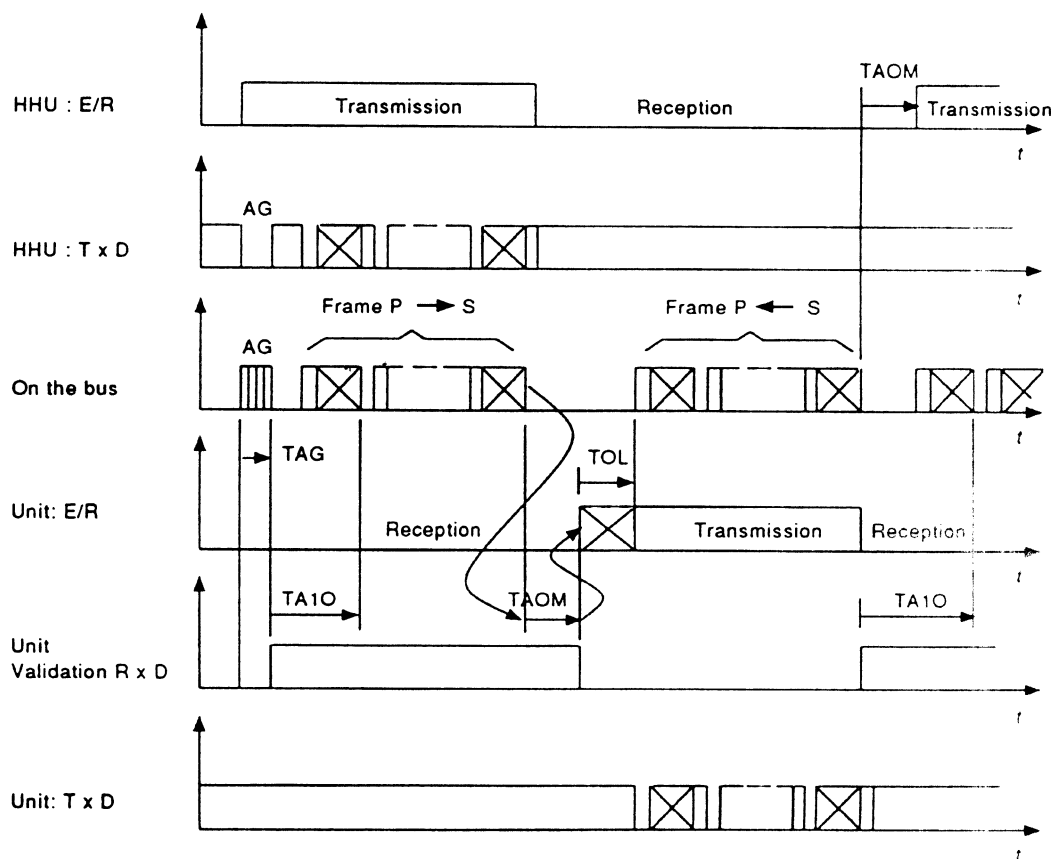
During the general call time, any interference interrupting the carrier for more than 100 μs reinitializes the general call detection parameters.

The presence of the carrier for between 50 and 150 ms without interference greater than 100 μs is therefore interpreted as a wake up call and “alerts” the secondary stations model to receive the bytes of the frame to follow.

2.6.3 Characteristics of transmission/reception sequences

In accordance with the schematic diagram given below, the characteristics of a transmit-receive sequence are as given below.

2.6.4 Timing chart (nominal)



2.6.4.1 Comments

The transceiving levels on the bus are given in this standard (see clause 4).

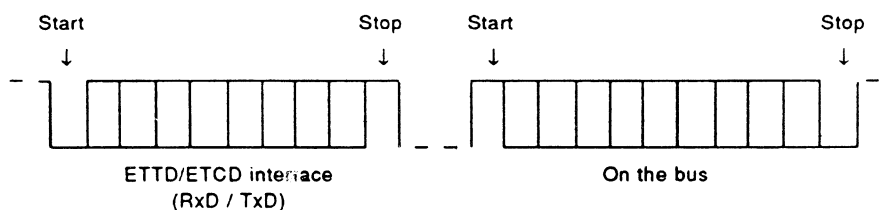
The first frame transmitted by the primary station is preceded by a general call nominally lasting 100 ms; this signal is generated by the serial transmission port used (T×D) and then modulates the frequency of the carrier.

The bytes in each frame, transmitted by the primary station or a secondary station, are transmitted in reverse logic:

level 1 logic from T×D or R×D = no carrier on the bus;

level 0 logic from T×D or R×D = carrier on the bus;

which translates into the following signals to transmit one byte:



After a frame and the stop of the last byte is transmitted, the bus will no longer contain a carrier; similarly, time outs between bytes will be translated by no carrier on the bus.

Receiving stops as soon as an end of frame is detected. The detection criterion is not receiving bytes for a given time $TAOM = 40$ ms (maximum absence of bytes time). Detection triggers the interpretation of the frame received and the associated actions handled at higher levels of the protocol. It disables serial reception logically. This detection criterion means that no similar sequence shall intervene in the transmission of a frame before it is completed. Furthermore, considerations as to the duration of exchanges mean that the maximum time for the sum of the time outs between the bytes in a frame shall be: TACEOM (maximum cumulative time out between bytes) = 30 ms. This parameter will be generated only by the transmitter and will not be checked on reception.

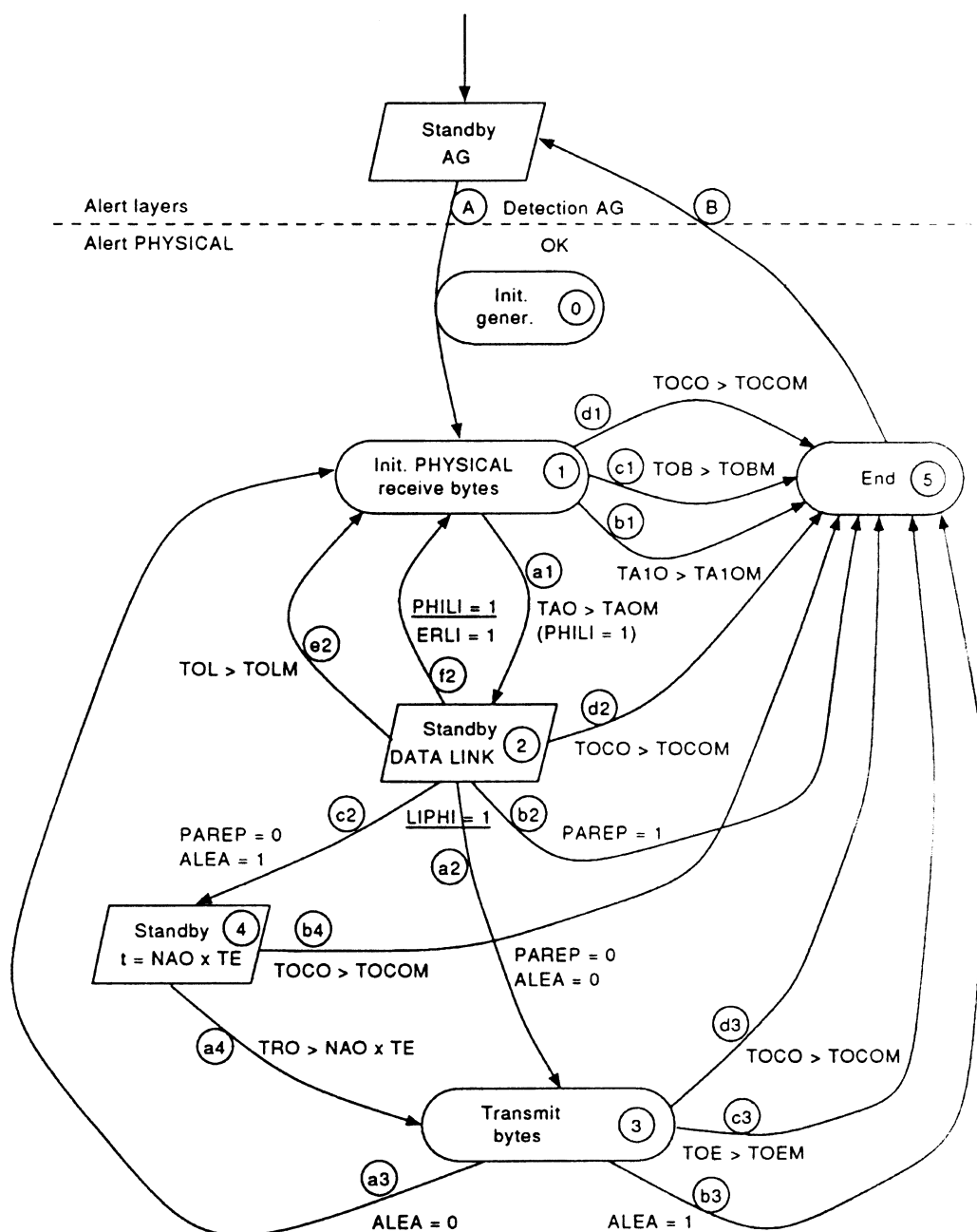
A modem may be switched to transmit as soon as an end of frame is detected (and reception stopped) or only when a frame starts to transmit. Both these facilities shall be possible and shall be totally transparent if the whole protocol is to work properly.

When an end of frame is detected in receive mode, the first byte of the frame shall be transmitted within the time required for the upper layers to process the information received and prepare the response frame. This time is called the "DATA LINK time out" (TOL) and its maximum value is $TOLM = 100$ ms. It does not include the transmission time for the first byte but only adds up the time until the start of the first byte transmitted.

The modem is switched from transmit to receive logically after the transmission of the stop of the last byte in the frame. This length is in fact known by the transmission software which determines the moment it is switched to receive.

2.6.5 States on the PHYSICAL layer

2.6.5.1 Diagram of states on the PHYSICAL layer



2.6.5.2 Description of states on PHYSICAL layer

* General principles

All states are controlled at execution time level by “time outs” labelled TOXXX. By definition, a “time out” occurs in parallel with the execution of the actions of the corresponding state. They are reset whenever the state in question is reached, except for the communication time out, TOCO which controls the overall duration of an exchange and operates in parallel with all states from the “Receive bytes” state achieved by a “general call detection” event.

Time outs labelled TAXXX run in series with the execution of the actions of the state in question. They are reset and validated as soon as the action is completed.

The various timers are incremented by a clock, the frequency of which will be selected to comply with the timing operations specified in the application. The clock increments in parallel to the action of the PHYSICAL layer.

The PHYSICAL layer is alerted and synchronized if a general call is detected logically or physically, provided that the validation criteria of a general call are met.

However, depending on the type of application developed, it is possible to leave the PHYSICAL layer on permanent standby; start up will be activated only on a general call; this option depends on the application which shall be managed outside the local bus reading protocol.

The diagram and related explanations assume the PHYSICAL layer is completely switched off outside a local bus reading communication.

** State 0*

General initialization of the protocol. All variables on all layers required for handling a complete exchange are initialized in this state. Start communications time out timer TOCO.

** State 1*

Reinitialization of PHILI.

Receive bytes: each byte received is stored in a buffer which will be sent to upper layers for processing.

** State 2*

LIPHI synchronization flag from DATA LINK put on standby.

** State 3*

Transmit bytes: the upper layer has prepared a buffer or a set of buffers to be transmitted; their location and length are transmitted to PHYSICAL for this transmit state.

** State 4*

Time lapse $TRO = NAO \times TE$, NAO is a random value between 0 and 2 coming from the upper layers. The time TE is fixed. In this state, the modem is in receive mode. TE is fixed at 500 ms.

** State 5*

Closure of the physical connection, the PHYSICAL layer switches off all upper layers and itself logs off. All the layers of the protocol are thus deactivated.

2.6.5.3 Description of PHYSICAL events

- A. The carrier has been detected for a time TAG between TAGm and TAGM; this information enables all the protocol layers to be put on standby and the PHYSICAL layer activated by coming to state 1 "receive bytes". This event is also associated with the overall initialization of the protocol and the initialization of time out TOCO.
- a1. Exceeding the no bytes time TAO means that the end of reception of a frame can be assumed. This event then causes the DATA LINK layer to execute by changing the synchronization flag PHILI = 1.
This event is the standard exit from state 1 when no time out overrun has been detected and the exchange is not finished.
- b1. Exceeding the time out for the first byte TA1O halts the protocol by moving to state 5. This event means that switching the modem to receive is not followed by the expected frame.
This is the event which indicates among other things that a restart has not occurred and the protocol can cut off (example of exist after transmission of the remote reading frame).
- c1. Exceeding the "chatterbox" time out (TOB) enables reception to be cut off if it lasts longer than the transmission time for the maximum number of bytes comprising a frame (128 bytes) plus the cumulative time out between bytes (TACOM) and a 10 % safety margin to cover inaccuracies in time measurement.

$$TOBM = \left(\frac{127 \times 10^4}{1\ 200} + TACEOM \right) \times 1,1^2 + TAOM$$

$$TOBM = 1\ 360\ ms$$

TOB monitors a "chatterbox" HHU.

NOTE This time check may be replaced by a check on the maximum number of bytes which can be transmitted on a frame, with equivalent effect.

- d1. If the overall communication timer TOCO overruns, this causes a change to state 5. This timer is initialized once only during the overall initialization of the protocol.

a2 – b2 – c2 – f2.

Returning the upper layers to synchronization by LIPHI = 1, indicating that their actions are terminated, causes a move to state 1, 3, 4 or 5.

These events are then differentiated depending on the state of the three parameters PAREP (no response), ALEA (random) and ERLI (DATA LINK error). PAREP tells the PHYSICAL layer to move to end of protocol state without transmitting a frame and without waiting for a startover.

PAREP is set by the upper layers when

- decoding an IB command (bus initialization);
- detecting an ADS address which is not that of the unit;
- an ASO command (forgotten station call) addresses a unit which has not been forgotten or is not concerned;
- detecting a primary address ADP unknown to the secondary station.

ALEA is located by the upper layers when an ASO command is detected, it tells the unit, whether it has been “forgotten” or not, that no startover is to be expected after the transmission of its response frame.

- a2. Event LIPHI = 1 associated with state (PAREP = 0 and ALEA = 0), this is when a response is to be transmitted and a startover is expected.
- b2. Event LIPHI = 1 associated with state (PAREP = 1) when no response is to be transmitted.
- c2. Event LIPHI = 1 associated with state (PAREP = 0 and ALEA = 1) when a response is to be transmitted with a delay (state 4).
- d2. Communication time out TOCO overrun.
- e2. DATA LINK time out TOL overrun, which in fact controls the execution time of all upper layers after an end of frame has been detected and the associated synchronization PHILI = 1 has moved to synchronization feedback LIPHI = 1. It is associated with the reinitialization of all upper layers: DATA LINK reset to state 0, SESSION reset to state 0 and APPLICATION reset to state 0.
- f2. Event LIPHI = 1 associated with ERLI = 1 (DATA LINK error) means that an error has been detected at an upper level. Under these states, the unit reverts to state 1 “receive bytes” to wait for a startover from the primary station.
- a4. time out TRO = NAO×TE is reached and allows a move to state 3 for the transmission of a forgotten station response frame into one of the authorized time windows.
- b4. Communication time out TOCO overrun.
- a3. Exit after end of frame transmission where ALEA = 0 (the frame which has just been transmitted is not a response to a forgotten station call). The PHYSICAL layer reverts to state 1 to receive any subsequent frame.
- b3. Exit after end of frame transmission where ALEA = 1 (the frame transmitted is a response to a forgotten station call). The PHYSICAL layer knows that no startover or frame is expected. It can therefore switch to state 5 to disconnect.

The unit shall not revert to state 1 so as not to receive frames transmitted by other stations.

- c3. The transmission time out (TOE) stops transmission if it lasts longer than TOEM.

$$\text{TOEM} = \left(\frac{128 \times 10^4}{1\,200} + \text{TACEOM} \right)$$

$$\text{TOEM} = 1\,100 \text{ ms}$$

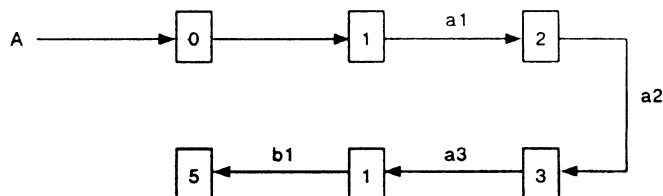
- d3. Communication time out TOCO overrun.

NOTE TOCO will be detected with a precision encompassing the maximum duration of a “call-response” sequence; it may therefore only be checked at the beginning of state 1.

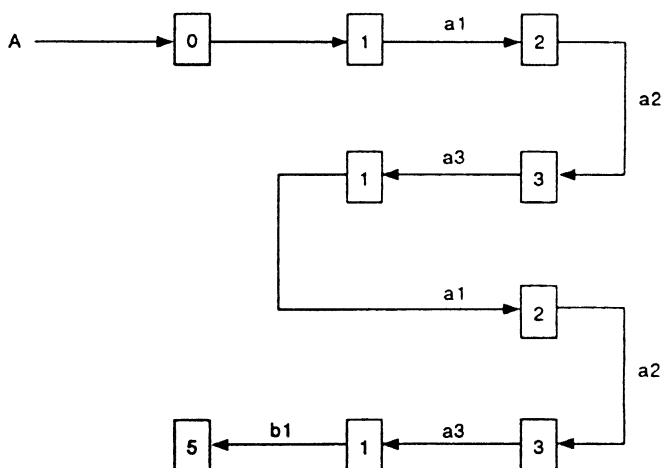
B. After switching off all the layers of the protocol, the PHYSICAL layer switches itself off.

2.6.5.4 Diagram of several examples of states

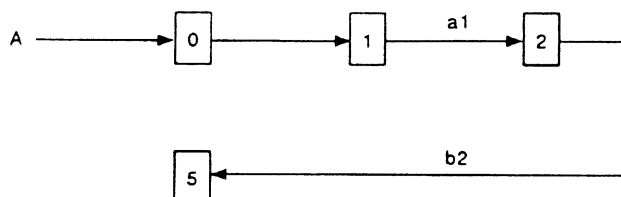
— Remote reading: nominal example



— Remote programming: nominal example

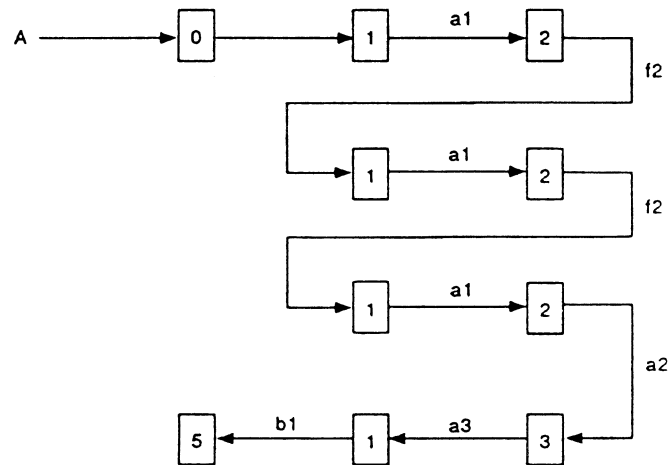


— Bus initialization: nominal example



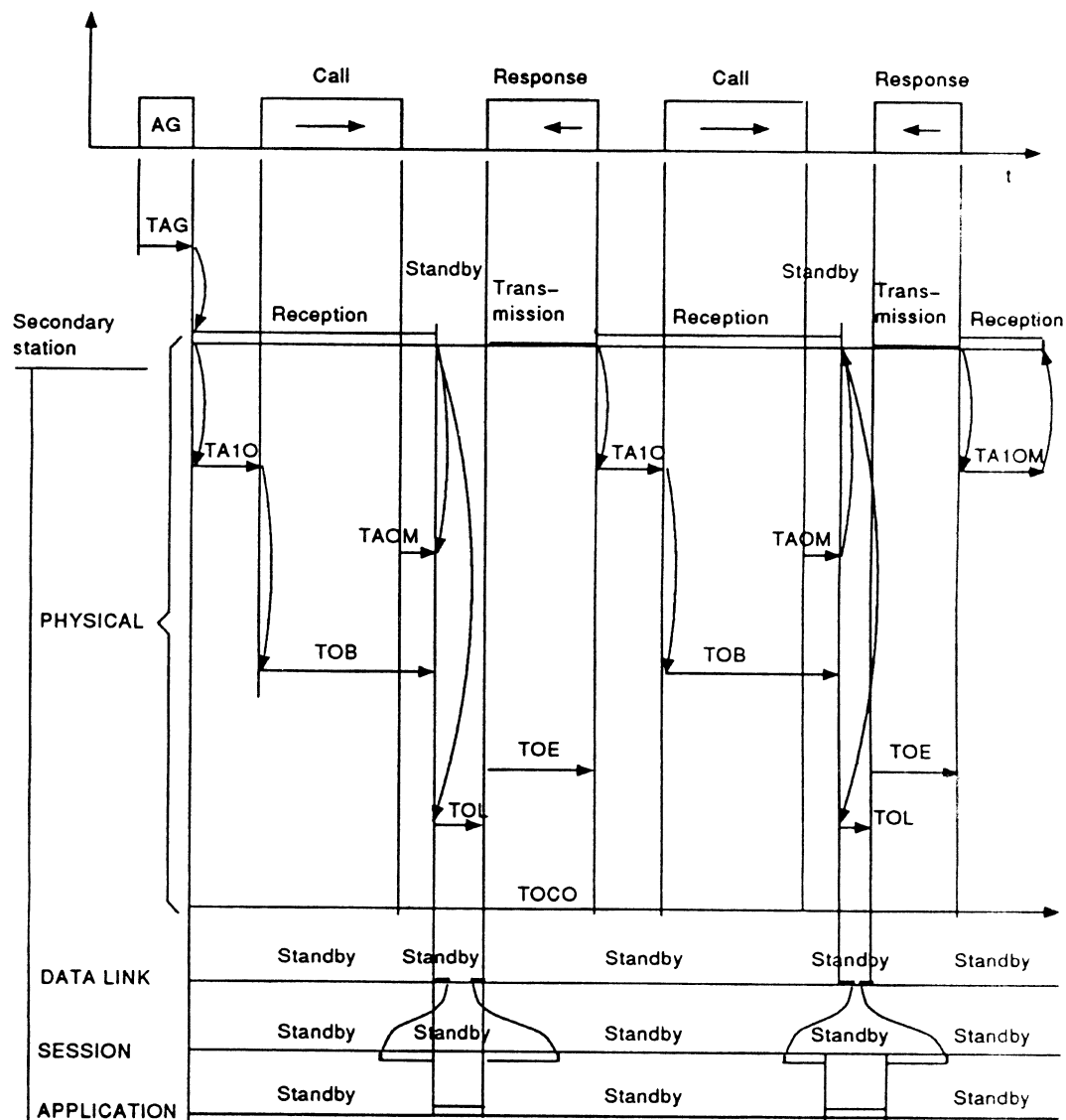
This diagram is also applicable in the case of a forgotten station call addressing a non forgotten unit and in the case of remote reading or remote programming arousing a station whose address is not that of the primary call address ADP.

— Example of startovers followed by correct remote reading on an error detected by the secondary station in the upper layers



2.6.6 Time division charts

2.6.6.1 Nominal example (as seen from secondary station)

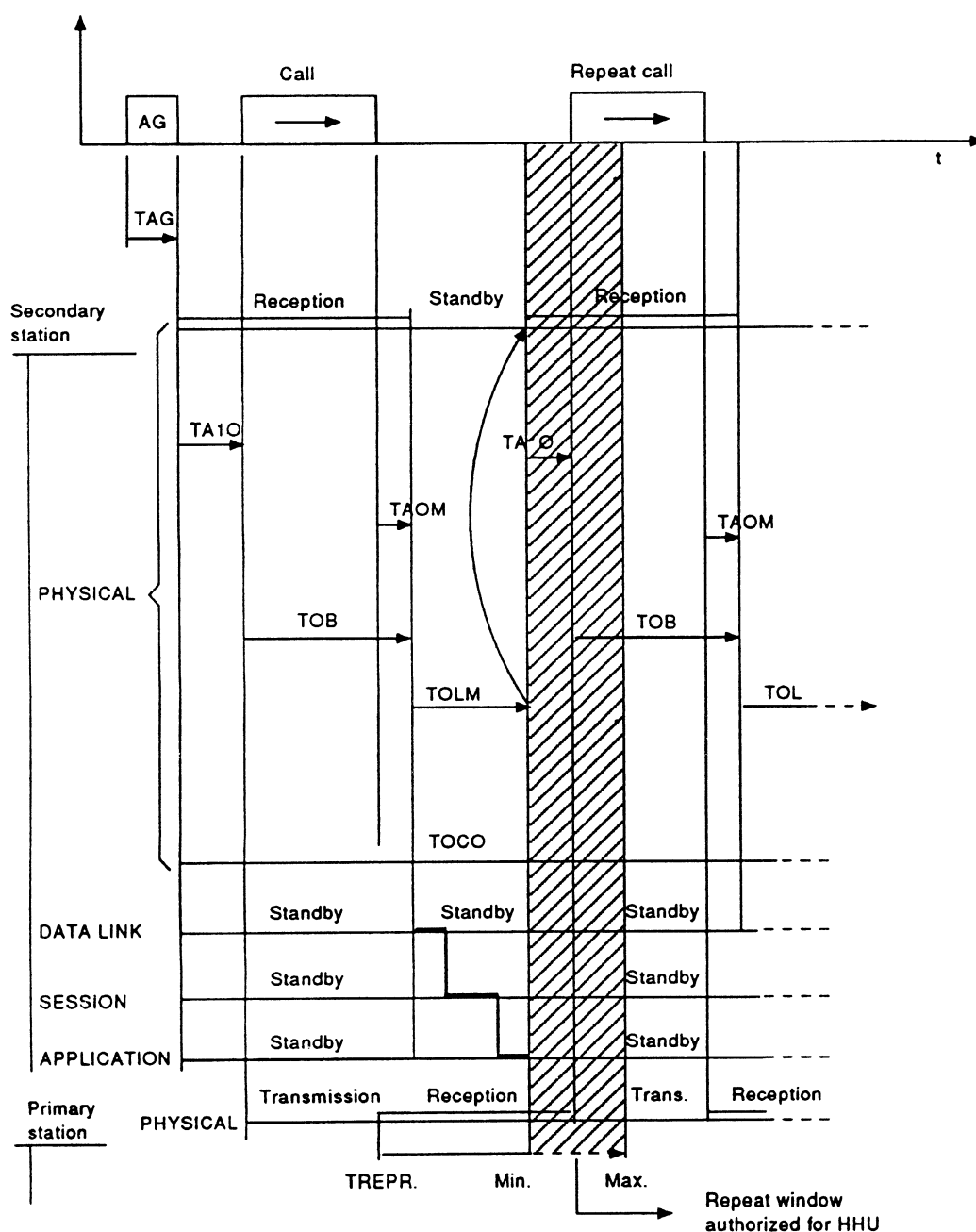


TAG	=	100 ms
TAOM	=	40 ms
TA1OM	=	160 ms
TOLM	=	100 ms
TACEOM	=	30 ms
TOCOM	=	15 s
TOEM	=	1 100 ms
TOBM	=	1 360 ms

2.6.6.2 Example of error on reception (as seen from secondary station)

Example corresponding to events e2 and f2 on the PHYSICAL layer diagram corresponding to an overrun of the DATA LINK time out or an error on the upper layers (ERLI = 1).

* Example of event e2 ($TOL > TOLM$)



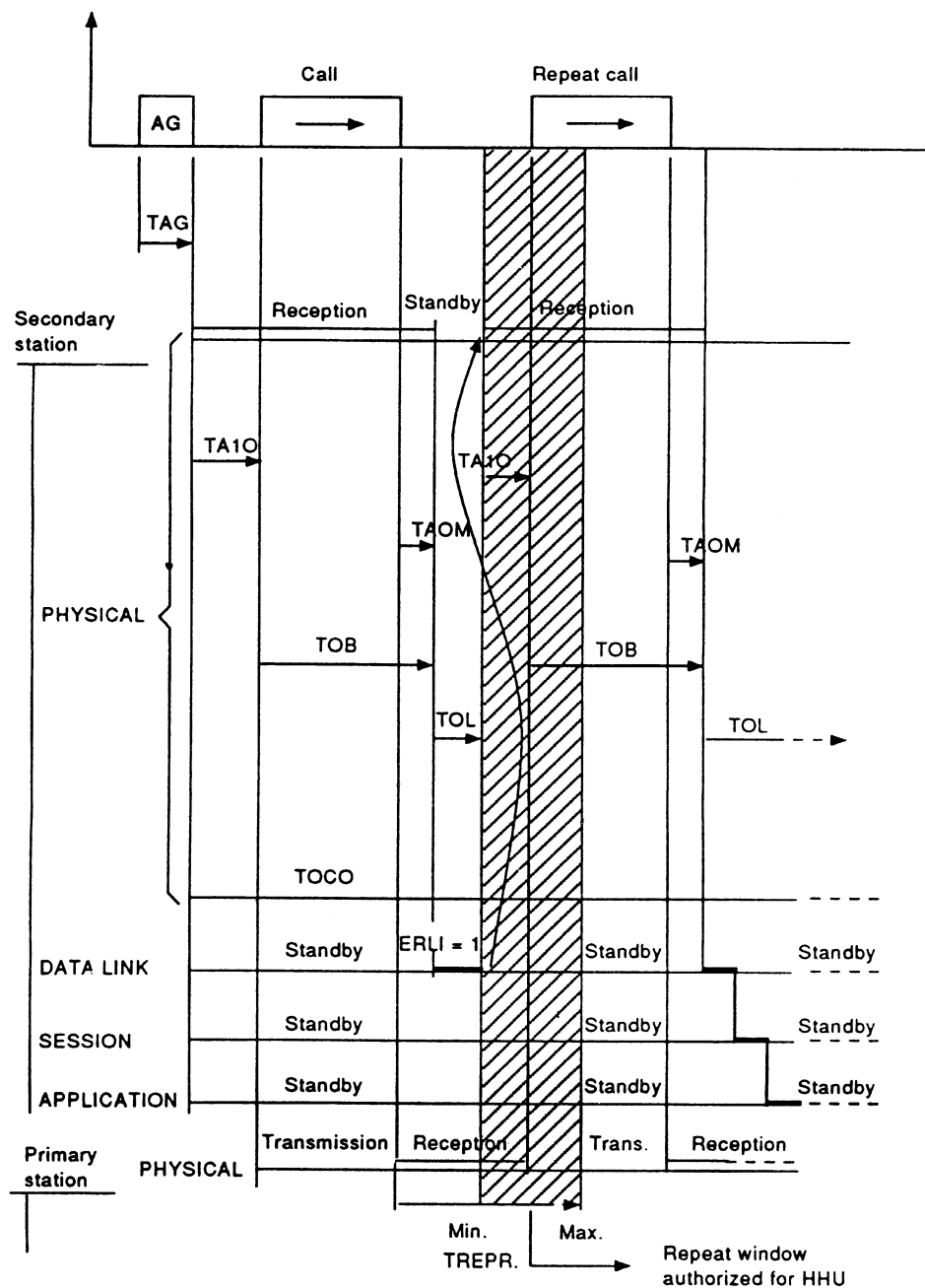
Repeat call time of HHU after transmission

$$TREPR_{min} = TAOM + TOLM$$

$$TREPR_{max} = TAOM + TOLM + (TA1OM - \text{duration of 1 byte})$$

Time seen from secondary station

— Example of event f_2 ($ERLI = 1$)



HHU startover time after transmission:

$TREPR_{min} = TAOM + TOL$ with min $TOL = 0$

$TREPR_{min} = TAOM$

$TREPR_{max} = TAOM + (TA1OM - \text{duration of 1 byte})$

— By combining the above two examples, the startover time shall be between
 $\text{MAX}(\text{TREPR}_{\text{min}}) \leq \text{TREPR} \leq \text{min}(\text{TREPR}_{\text{max}})$

$\text{TAOM} + \text{TOLM} \leq \text{TREPR} \leq \text{TAOM} + \text{TOL} + (\text{TA1OM} - \text{duration of 1 byte})$

$\text{TAOM} + \text{TOLM} \leq \text{TREPR} \leq \text{TAOM} + (\text{TA1Om} - \text{duration of 1 byte})$

$160 \text{ ms} \leq \text{TREPR} \leq 170 \text{ ms}$

It should be noted that according to the above inequation TA1OM cannot be less than TOLM.

If no expected response frame comes after a call frame is transmitted, the primary station shall carry out a startover in the time division window specified by TREPR_{min} and TREPR_{max}. The startover time (after having been reset to zero) is counted whenever the primary station switches to receive mode.

2.6.6.3 Example of forgotten station call

