

# Telecontrol equipment and systems —

## Part 5-104: Transmission protocols — Network access for IEC 60870-5-101 using standard transport profiles

The European Standard EN 60870-5-104:2001 has the status of a  
British Standard

ICS 33.200

# National foreword

This British Standard is the official English language version of EN 60870-5-104:2001. It is identical with IEC 60870-5-104:2000.

The UK participation in its preparation was entrusted to Technical Committee PEL/57, Power system control and associated communications, which has the responsibility to:

- aid enquirers to understand the text;
- present to the responsible European committee any enquiries on the interpretation, or proposals for change, and keep the UK interests informed;
- monitor related international and European developments and promulgate them in the UK.

A list of organizations represented on this committee can be obtained on request to its secretary.

From 1 January 1997, all IEC publications have the number 60000 added to the old number. For instance, IEC 27-1 has been renumbered as IEC 60027-1. For a period of time during the change over from one numbering system to the other, publications may contain identifiers from both systems.

### Cross-references

The British Standards which implement international or European publications referred to in this document may be found in the BSI Standards Catalogue under the section entitled “International Standards Correspondence Index”, or by using the “Find” facility of the BSI Standards Electronic Catalogue.

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.**

This British Standard, having been prepared under the direction of the Electrotechnical Sector Policy and Strategy Committee, was published under the authority of the Standards Policy and Strategy Committee on 19 March 2002

### Summary of pages

This document comprises a front cover, an inside front cover, the EN title page, pages 2 to 56, an inside back cover and a back cover.

The BSI copyright date displayed in this document indicates when the document was last issued.

### Amendments issued since publication

| Amd. No. | Date | Comments |
|----------|------|----------|
|          |      |          |
|          |      |          |
|          |      |          |
|          |      |          |
|          |      |          |

© BSI 19 March 2002

ISBN 0 580 39119 1

**Telecontrol equipment and systems**  
**Part 5-104: Transmission protocols -**  
**Network access for IEC 60870-5-101**  
**using standard transport profiles**  
(IEC 60870-5-104:2000)

Matériels et systèmes de téléconduite  
Partie 5-104: Protocoles de transmission -  
Accès aux réseaux utilisant des profils  
de transport normalisés  
pour la CEI 60870-5-101  
(CEI 60870-5-104:2000)

Fernwirkleinrichtungen und -systeme  
Teil 5-104: Übertragungsprotokolle -  
Zugriff für IEC 60870-5-101 auf Netze  
mit genormten Transportprofilen  
(IEC 60870-5-104:2000)

This European Standard was approved by CENELEC on 2001-03-01. 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, Czech Republic, 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 57/487/FDIS, future edition 1 of IEC 60870-5-104, prepared by IEC TC 57, Power system control and associated communications, was submitted to the IEC-CENELEC parallel vote and was approved by CENELEC as EN 60870-5-104 on 2001-03-01.

The following dates were fixed:

- latest date by which the EN has to be implemented  
at national level by publication of an identical  
national standard or by endorsement (dop) 2001-12-01
- latest date by which the national standards conflicting  
with the EN have to be withdrawn (dow) 2004-03-01

Annexes designated "normative" are part of the body of the standard.  
In this standard, annex ZA is normative.  
Annex ZA has been added by CENELEC.

---

## **Endorsement notice**

The text of the International Standard IEC 60870-5-104:2001 was approved by CENELEC as a European Standard without any modification.

---

## CONTENTS

|                                                                                                               | Page |
|---------------------------------------------------------------------------------------------------------------|------|
| INTRODUCTION .....                                                                                            | 5    |
| Clause                                                                                                        |      |
| 1 Scope and object .....                                                                                      | 6    |
| 2 Normative references .....                                                                                  | 6    |
| 3 General architecture .....                                                                                  | 7    |
| 4 Protocol structure .....                                                                                    | 9    |
| 5 Definition of Application Protocol Control Information (APCI) .....                                         | 11   |
| 5.1 Protection against loss and duplication of messages .....                                                 | 13   |
| 5.2 Test procedures .....                                                                                     | 15   |
| 5.3 Transmission Control using Start/Stop .....                                                               | 17   |
| 5.4 Portnumber .....                                                                                          | 18   |
| 5.5 Maximum number of outstanding I format APDUs ( <i>k</i> ) .....                                           | 19   |
| 6 Selection of ASDUs defined in IEC 60870-5-101 and additional ASDUs .....                                    | 20   |
| 7 Mapping of selected application data units and functions to the TCP services .....                          | 23   |
| 7.1 Station initialization (6.1.5 to 6.1.7 of IEC 60870-5-5) .....                                            | 23   |
| 7.2 Data acquisition by polling (6.2 of IEC 60870-5-5) .....                                                  | 28   |
| 7.3 Cyclic data transmission (6.3 of IEC 60870-5-5) .....                                                     | 28   |
| 7.4 Acquisition of events (6.4 of IEC 60870-5-5) .....                                                        | 28   |
| 7.5 General interrogation (6.6 of IEC 60870-5-5) .....                                                        | 28   |
| 7.6 Clock synchronization (6.7 of IEC 60870-5-5) .....                                                        | 29   |
| 7.7 Command transmission (6.8 of IEC 60870-5-5) .....                                                         | 30   |
| 7.8 Transmission of integrated totals (6.9 of IEC 60870-5-5) .....                                            | 31   |
| 7.9 Parameter loading (6.10 of IEC 60870-5-5) .....                                                           | 31   |
| 7.10 Test procedure (6.11 of IEC 60870-5-5) .....                                                             | 32   |
| 7.11 File transfer (6.12 of IEC 60870-5-5) Control and monitor direction .....                                | 32   |
| 8 ASDUs for process information in control direction with time tag .....                                      | 34   |
| 8.1 TYPE IDENT 58: C_SC_TA_1 Single command with time tag CP56Time2a .....                                    | 34   |
| 8.2 TYPE IDENT 59: C_DC_TA_1 Double command with time tag CP56Time2a .....                                    | 35   |
| 8.3 TYPE IDENT 60: C_RC_TA_1 Regulating step command with<br>time tag CP56Time2a .....                        | 36   |
| 8.4 TYPE IDENT 61: C_SE_TA_1 Set-point command with time tag CP56Time2a,<br>normalized value .....            | 37   |
| 8.5 TYPE IDENT 62: C_SE_TB_1 Set-point command with time tag CP56Time2a,<br>scaled value .....                | 38   |
| 8.6 TYPE IDENT 63: C_SE_TC_1 Set-point command with time tag CP56Time2a,<br>short floating point number ..... | 39   |
| 8.7 TYPE IDENT 64: C_BO_TA_1 Bitstring of 32 bit with time tag CP56Time2a .....                               | 40   |
| 8.8 TYPE IDENT 107: C_TS_TA_1 Test command with time tag CP56Time2a .....                                     | 41   |

| Clause                                                                                                                          | Page |
|---------------------------------------------------------------------------------------------------------------------------------|------|
| 9 Interoperability .....                                                                                                        | 42   |
| 9.1 System or device .....                                                                                                      | 42   |
| 9.2 Network configuration .....                                                                                                 | 42   |
| 9.3 Physical layer .....                                                                                                        | 43   |
| 9.4 Link layer .....                                                                                                            | 43   |
| 9.5 Application layer .....                                                                                                     | 44   |
| 9.6 Basic application functions .....                                                                                           | 50   |
| Annex ZA (normative) Normative references to international publications with their<br>corresponding European publications ..... | 55   |
| Figure 1 – General architecture (example) .....                                                                                 | 8    |
| Figure 2 – Selected standard provisions of the defined telecontrol companion standard .....                                     | 9    |
| Figure 3 – Selected standard provisions of the TCP/IP protocol suite RFC 2200 (example) ....                                    | 10   |
| Figure 4 – APDU of the defined telecontrol companion standard .....                                                             | 11   |
| Figure 5 – APCI of the defined telecontrol companion standard .....                                                             | 11   |
| Figure 6 – Control field of type Information transfer format (I format) .....                                                   | 12   |
| Figure 7 – Control field of type numbered supervisory functions (S format) .....                                                | 12   |
| Figure 8 – Control field of type unnumbered control functions (U format) .....                                                  | 13   |
| Figure 9 – Undisturbed sequences of numbered I format APDUs .....                                                               | 14   |
| Figure 10 – Undisturbed sequences of numbered I format APDUs acknowledged by<br>an S format APDU .....                          | 14   |
| Figure 11 – Disturbed sequence of numbered I format APDUs .....                                                                 | 15   |
| Figure 12 – Time-out in case of a not acknowledged last I format APDU .....                                                     | 15   |
| Figure 13 – Undisturbed test procedure .....                                                                                    | 16   |
| Figure 14 – Unconfirmed test procedure .....                                                                                    | 16   |
| Figure 15 – Start data transfer procedure .....                                                                                 | 17   |
| Figure 16 – Stop data transfer procedure .....                                                                                  | 18   |
| Figure 17 – TCP connection establishment and close .....                                                                        | 24   |
| Figure 18 – Initialization of the controlling station .....                                                                     | 25   |
| Figure 19 – Local initialization of the controlled station .....                                                                | 26   |
| Figure 20 – Remote initialization of the controlled station .....                                                               | 27   |
| Figure 21 – ASDU: C_SC_TA_1 Single command with time tag CP56Time2a .....                                                       | 34   |
| Figure 22 – ASDU: C_DC_TA_1 Double command with time tag CP56Time2a .....                                                       | 35   |
| Figure 23 – ASDU: C_RC_TA_1 Regulating step command with time tag CP56Time2a .....                                              | 36   |
| Figure 24 – ASDU: C_SE_TA_1 Set-point command with time tag CP56Time2a,<br>normalized value .....                               | 37   |
| Figure 25 – ASDU: C_SE_TB_1 Set-point command with time tag CP56Time2a,<br>scaled value .....                                   | 38   |
| Figure 26 – ASDU: C_SE_TC_1 Set-point command with time tag CP56Time2a,<br>short floating point number .....                    | 39   |
| Figure 27 – ASDU: C_BO_TA_1 Bitstring of 32 bit with time tag CP56Time2a .....                                                  | 40   |
| Figure 28 – ASDU: C_TS_TA_1 Test command with time tag CP56Time2a .....                                                         | 41   |
| Table 1 – Process information in monitor direction .....                                                                        | 20   |
| Table 2 – Process information in control direction .....                                                                        | 21   |
| Table 3 – System information in monitor direction .....                                                                         | 22   |
| Table 4 – System information in control direction .....                                                                         | 22   |
| Table 5 – Parameter in control direction .....                                                                                  | 22   |
| Table 6 – File transfer .....                                                                                                   | 22   |

## INTRODUCTION

IEC 60870-5-101 provides a communication profile for sending basic telecontrol messages between a central telecontrol station and telecontrol outstations, which uses permanent directly connected data circuits between the central station and individual outstations.

In some applications, it may be required to send the same types of application messages between telecontrol stations using a data network containing relay stations which store and forward the messages and provide only a virtual circuit between the telecontrol stations. This type of network delays messages by varying amounts of time depending on the network traffic load.

In general, the variable message delay times mean that it is not possible to use the link layer as defined in IEC 60870-5-101 between telecontrol stations. However, in some cases it is possible to connect telecontrol stations having all three layers of the companion standard IEC 60870-5-101 to suitable data networks using Packet Assembler Disassembler (PAD) type stations to provide access for balanced communication.

In all other cases this companion standard, which does not use the link functions of IEC 60870-5-101, may be used to provide balanced access via a suitable transport profile.

## TELECONTROL EQUIPMENT AND SYSTEMS –

### Part 5-104: Transmission protocols – Network access for IEC 60870-5-101 using standard transport profiles

#### 1 Scope and object

This part of IEC 60870 applies to telecontrol equipment and systems with coded bit serial data transmission for monitoring and controlling geographically widespread processes. It defines a telecontrol companion standard that enables interoperability among compatible telecontrol equipment. The defined telecontrol companion standard utilizes standards of the IEC 60870-5 series. The specifications of this part present a combination of the application layer of IEC 60870-5-101 and the transport functions provided by a TCP/IP (Transmission Control Protocol/Internet Protocol). Within TCP/IP, various network types can be utilized, including X.25, FR (Frame Relay), ATM (Asynchronous Transfer Mode) and ISDN (Integrated Service Data Network). Using the same definitions, alternative ASDUs (Application Service Data Unit) as specified in other IEC 60870-5 companion standards (for example, IEC 60870-5-102) may be combined with TCP/IP, but this is not described further in this part.

NOTE Security mechanisms are outside the scope of this standard.

#### 2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this part of IEC 60870. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this part of IEC 60870 are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies. Members of IEC and ISO maintain registers of currently valid International Standards.

IEC 60870-5-3:1992, *Telecontrol equipment and systems – Part 5: Transmission protocols – Section 3: General structure of application data*

IEC 60870-5-4:1993, *Telecontrol equipment and systems – Part 5: Transmission protocols – Section 4: Definition and coding of application information elements*

IEC 60870-5-5:1995, *Telecontrol equipment and systems – Part 5: Transmission protocols – Section 5: Basic application functions*

IEC 60870-5-101:1995, *Telecontrol equipment and systems – Part 5: Transmission protocols – Section 101: Companion standard for basic telecontrol tasks*  
Amendment 1 (2000)

IEC 60870-5-102:1996, *Telecontrol equipment and systems – Part 5: Transmission protocols – Section 102: Companion standard for the transmission of integrated totals in electric power systems*

ITU-T Recommendation X.25:1996, *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 circuit*

IEEE 802.3:1998, *Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications*

RFC 791, *Internet Protocol, Request for Comments 791 (MILSTD 1777) (September, 1981)*

RFC 793, *Transmission Control Protocol, Request for Comments 793 (MILSTD 1778) (September, 1981)*

RFC 894, *Internet Protocol on Ethernet Networks*

RFC 1661, *Point-to-Point Protocol (PPP)*

RFC 1662, *PPP in HDLC Framing*

RFC 1700, *Assigned Numbers, Request for Comments 1700 (STD 2) (October, 1994)*

RFC 2200, *Internet Official Protocol Standards, Request for Comments 2200 (June, 1997)*

### 3 General architecture

This standard defines the use of an open TCP/IP-interface to a network, containing for example a LAN for telecontrol equipment, which transports IEC 60870-5-101 ASDUs. Routers which include the different WAN-types (for example, X.25, Frame Relay, ISDN, etc.) may be connected via a common TCP/IP-LAN-interface (see figure 1). Figure 1 shows a redundant configuration in the central station in addition to a non-redundant system.

Motivations:

The use of separate routers offers the following advantages.

- There is no need for network-specific software in end systems.
- There is no need for routing functionality in end systems.
- There is no need for network management in end systems.
- It facilitates obtaining end systems from manufacturers that specialize in telecontrol equipment.
- It facilitates obtaining individual separate routers, to suit a variety of networks from manufacturers specializing in this non-telecontrol specific field.
- It is possible to change the network type by replacing only the router type, without affecting the end systems.
- It is particularly suitable for converting existing end systems that conform to IEC 60870-5-101.
- It is suitable for present and future implementations.

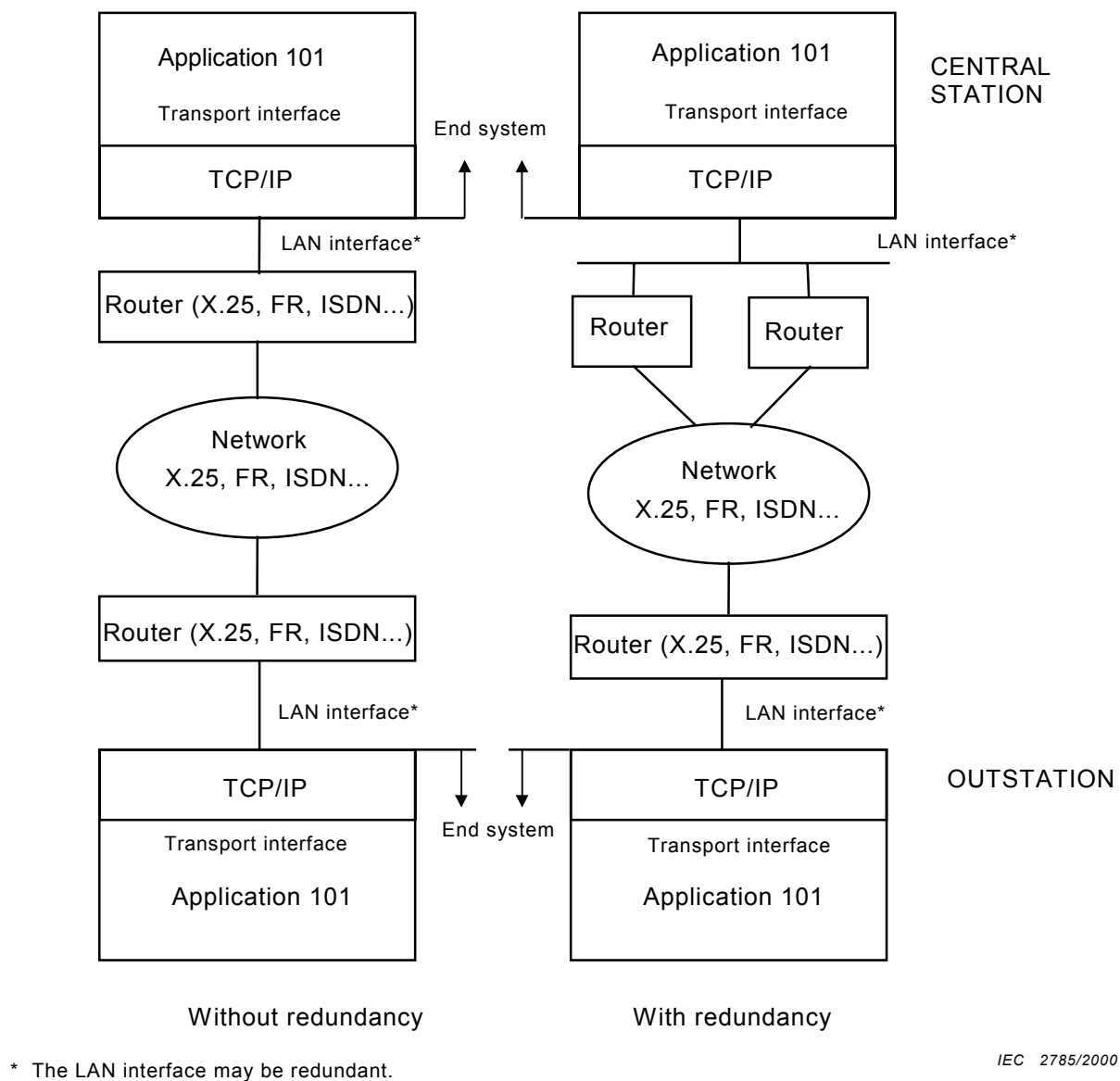


Figure 1 – General architecture (example)

## 4 Protocol structure

Figure 2 shows the protocol structure of the end system.

|                                                                                  |                                                                                                |                       |
|----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|-----------------------|
| Selection of application functions of IEC 60870-5-5 according to IEC 60870-5-101 | Initialization                                                                                 | User process          |
| Selection of ASDUs from IEC 60870-5-101 and IEC 60870-5-104                      | APCI (Application Protocol Control Information)<br>Transport Interface (user to TCP interface) | Application (layer 7) |
|                                                                                  |                                                                                                |                       |
| Selection of TCP/IP protocol suite (RFC 2200)                                    |                                                                                                | Transport (layer 4)   |
|                                                                                  |                                                                                                | Network (layer 3)     |
|                                                                                  |                                                                                                | Link (layer 2)        |
|                                                                                  |                                                                                                | Physical (layer 1)    |
| NOTE Layers 5 and 6 are not used.                                                |                                                                                                |                       |

**Figure 2 – Selected standard provisions of the defined telecontrol companion standard**

IEC 2786/2000

Figure 3 shows the recommended selection of the TCP/IP Protocol suite (RFC 2200) used in this standard. At the time of publication, the RFCs indicated were valid, but may have been replaced in the meantime by equivalent, relevant RFCs. The relevant RFCs are available at the Internet address <http://www.ietf.org>.

The Ethernet 802.3 stack shown may be used by a telecontrol station end system or DTE (Data Terminal Equipment) to drive a separate router as shown in the example in figure 1. If a redundant configuration is not required, a point-to-point interface (for example, X.21) to the separate router may be used instead of a LAN interface, thus retaining more of the original hardware when converting end systems originally conforming to IEC 60870-5-101.

Other compatible selections from RFC 2200 are also permitted.

This standard uses the TCP/IP transport profile as defined in other referenced standards, without alteration.

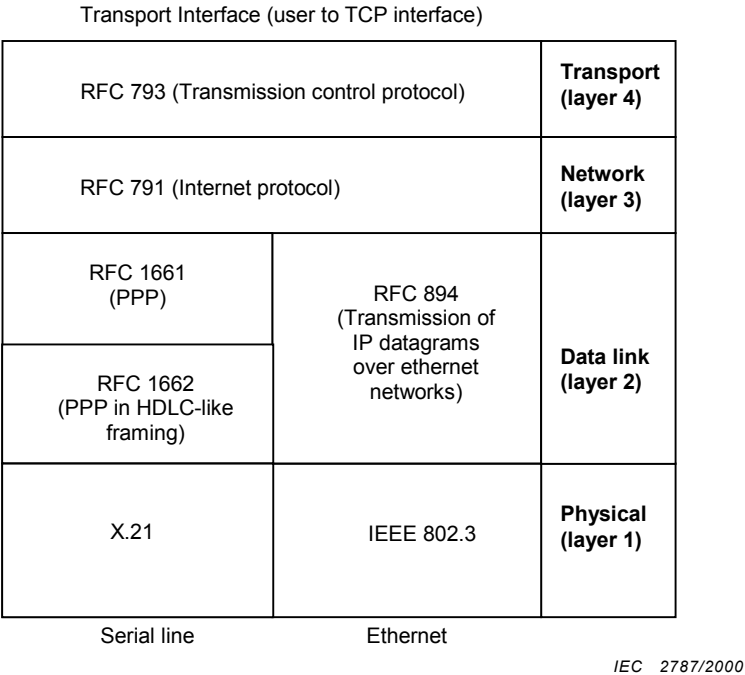


**Figure 3 – Selected standard provisions of the TCP/IP  
 protocol suite RFC 2200 (example)**

## 5 Definition of Application Protocol Control Information (APCI)

The transport interface (User to TCP interface) is a stream-oriented interface which does not define any start or stop mechanism for the ASDUs of IEC 60870-5-101. In order to detect the start and the end of the ASDUs, each APCI includes the following delimiting elements: a start character, the specification of the length of the ASDU, plus the control field (see figure 4). Either a complete APDU (or, for control purposes, only the APCI fields) may be transferred (see figure 5).

NOTE The abbreviations used above are taken from clause 5 of IEC 60870-5-3 as follows.

APCI Application Protocol Control Information

ASDU Application Service Data Unit

APDU Application Protocol Data Unit

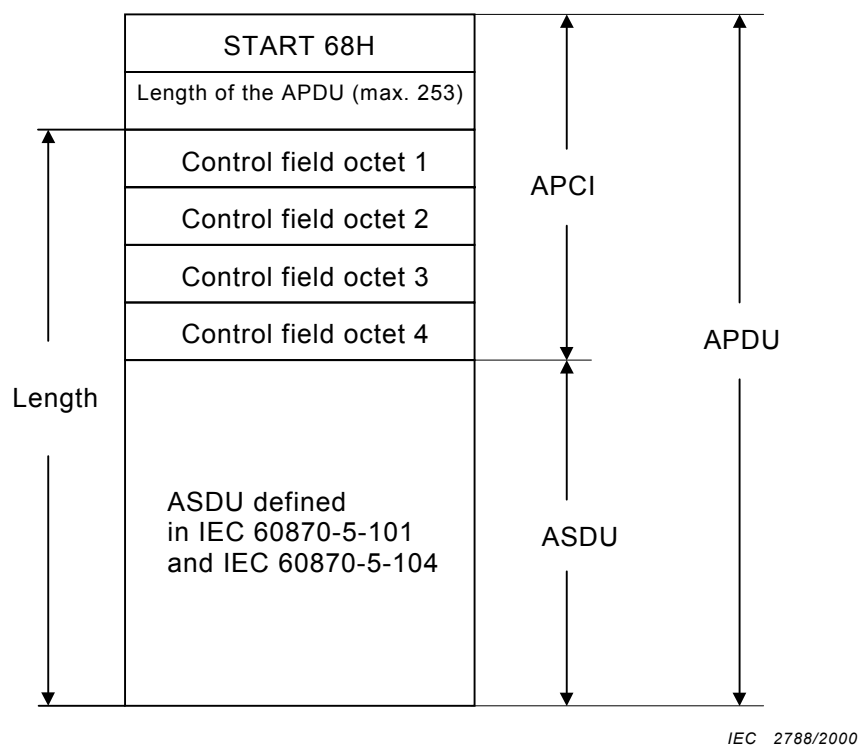


Figure 4 – APDU of the defined telecontrol companion standard

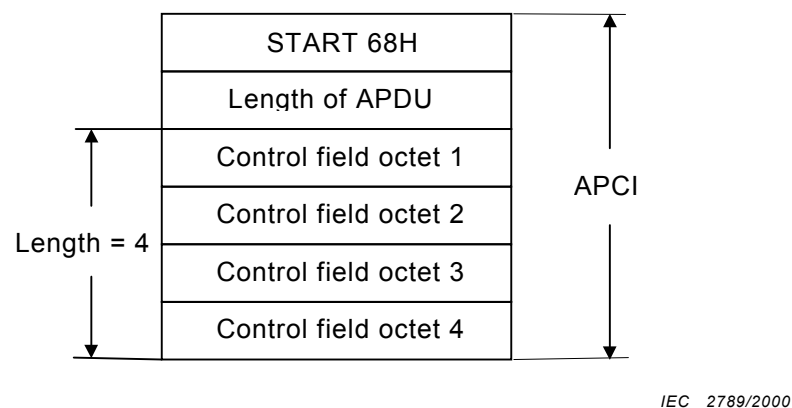


Figure 5 – APCI of the defined telecontrol companion standard

START 68H defines the point of start within the data stream.

The length of the APDU defines the length of the body of the APDU, which consists of the four control field octets of the APCI plus the ASDU. The first counted octet is the first octet of the control field, the last counted octet is the last octet of the ASDU. The maximum length of the ASDU is limited to 249 because the maximum value of the field length of APDU is 253 ( $APDU_{max} = 255$  minus start and length octet) and the length of the control field is 4 octets.

The control field defines control information for the protection against loss and duplication of messages, start and stop of message transfers and the supervision of transport connections. The counter mechanism of the control field is defined according to 2.3.2.2.1 to 2.3.2.2.5 of the ITU-T X.25 recommendation.

Figures 6, 7 and 8 show the definition of the control field.

Three types of control field formats are used to perform numbered information transfer (I format), numbered supervisory functions (S format) and unnumbered control functions (U format).

Control field octet 1 bit 1 = 0 defines the I format. I format APDUs always contain an ASDU. The control information of an I format is shown in figure 6.

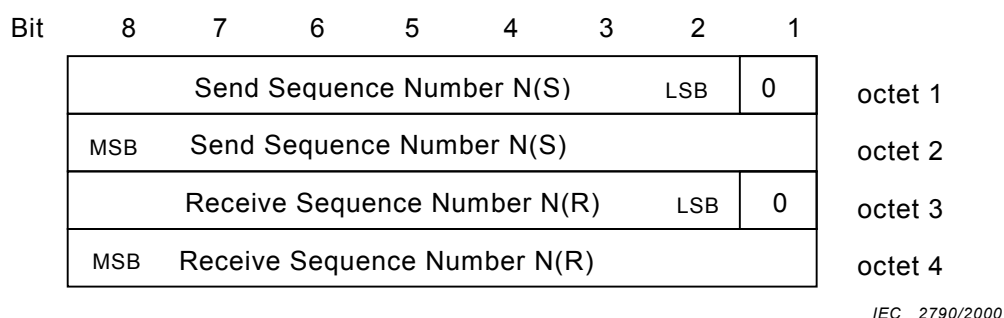


**Figure 6 – Control field of type Information transfer format (I format)**

Control field octet 1 bit 1 = 1 and bit 2 = 0 defines the S format. S format APDUs consist of the APCI only. The control information of an S format is shown in figure 7.

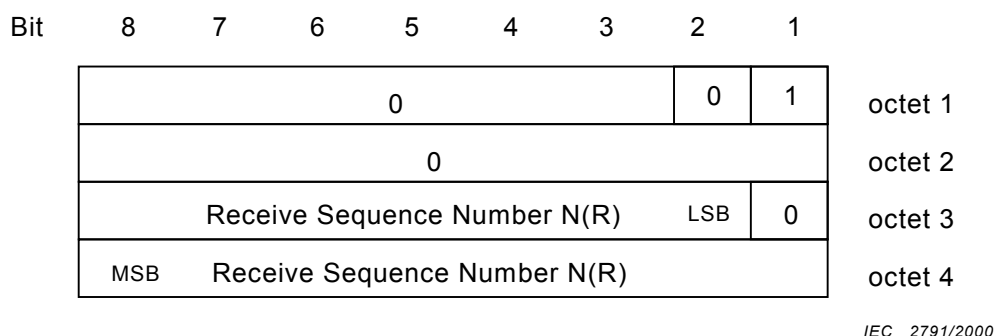


**Figure 7 – Control field of type numbered supervisory functions (S format)**

Control field octet 1 bit 1 = 1 and bit 2 = 1 defines the U format. U format APDUs consist of the APCI only. The control information of a U format is shown in figure 8. Only one function – TESTFR, STOPDT or STARTDT – may be active at the same time.

|        |     |        |     |         |     |   |   |         |         |
|--------|-----|--------|-----|---------|-----|---|---|---------|---------|
| Bit    | 8   | 7      | 6   | 5       | 4   | 3 | 2 | 1       |         |
| TESTFR |     | STOPDT |     | STARTDT |     | 1 | 1 | octet 1 |         |
| con    | act | con    | act | con     | act |   |   |         |         |
| 0      |     |        |     |         |     |   |   |         | octet 2 |
| 0      |     |        |     |         |     |   | 0 | octet 3 |         |
| 0      |     |        |     |         |     |   |   |         | octet 4 |

IEC 2792/2000

Figure 8 – Control field of type unnumbered control functions (U format)

### 5.1 Protection against loss and duplication of messages

The use of the Send Sequence Number N(S) and the Receive Sequence Number N(R) is identical to the method defined in ITU-T X.25. For simplification purposes, the additional sequences are defined in figures 9 to 12.

Both sequence numbers are sequentially increased by one for each APDU and each direction. The transmitter increases the Send Sequence Number N(S) and the receiver increases the Receive Sequence Number N(R). The receiving station acknowledges each APDU or a number of APDUs when it returns the Receive Sequence Number up to the number whose APDUs are properly received. The sending station holds the APDU or APDUs in a buffer until it receives back its own Send Sequence Number as a Receive Sequence Number which is a valid acknowledge for all numbers  $\leq$  the received number. Then it may delete the correctly transmitted APDUs from the buffer. In case of longer data transmission in one direction only, an S format has to be sent in the other direction to acknowledge the APDUs before buffer overflow or time out. This method should be used in both directions. After the establishment of a TCP connection, the send and receive sequence numbers are set to zero.

The following definitions are valid for figures 9 to 16:

V(S) = Send state variable (see ITU-T X.25);

V(R) = Receive state variable (see ITU-T X.25);

Ack = Indicates that the DTE has received correctly all I format APDUs numbered up to and including this number;

I(a,b) = Information format APDU with a = send sequence number and b = receive sequence number;

S(b) = Supervisory format APDU with b = receive sequence number;

U = Unnumbered control function APDU.

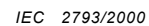


**Figure 9 – Undisturbed sequences of numbered I format APDUs**

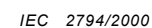
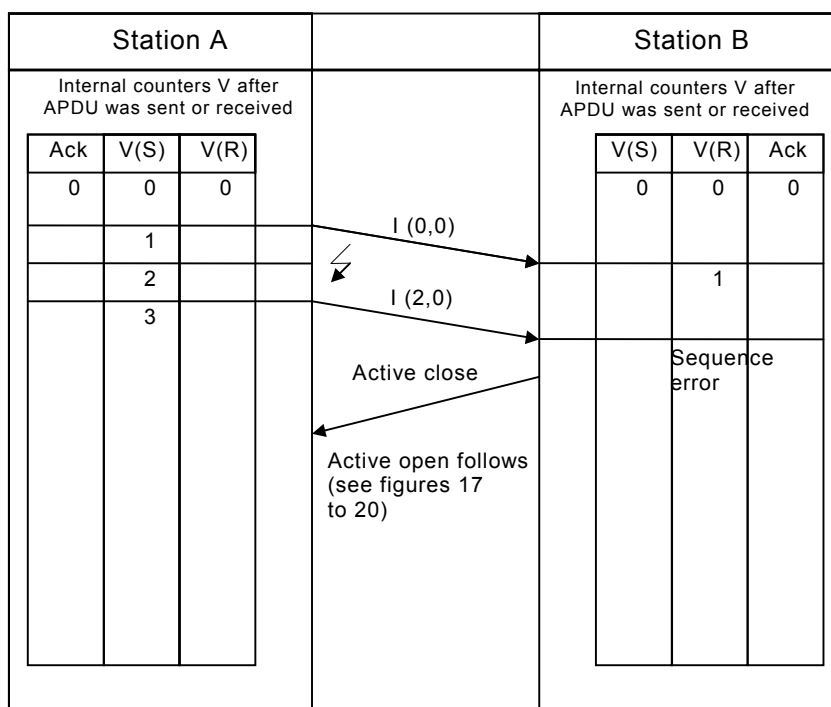
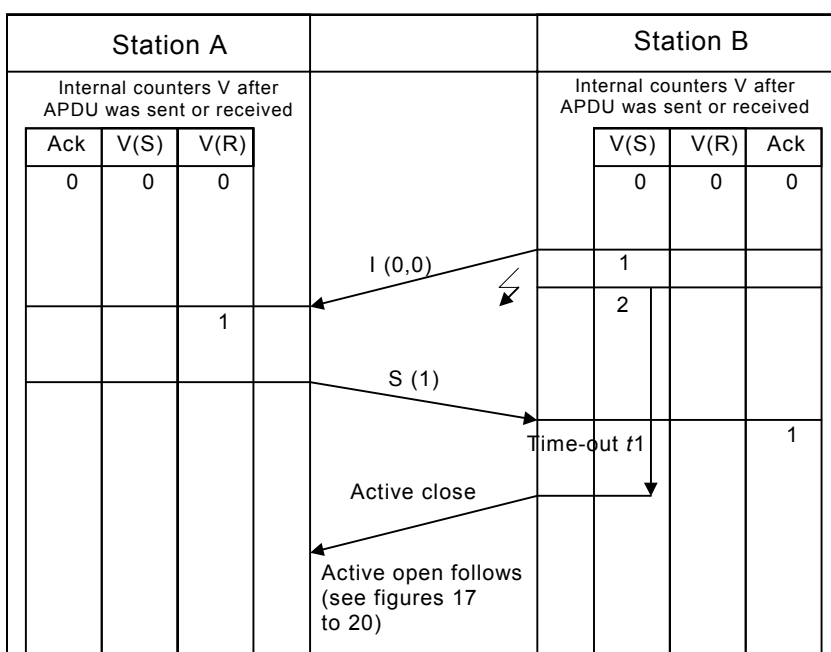


**Figure 10 – Undisturbed sequences of numbered I format APDUs acknowledged by an S format APDU**



IEC 2795/2000

Figure 11 – Disturbed sequence of numbered I format APDUs



IEC 2796/2000

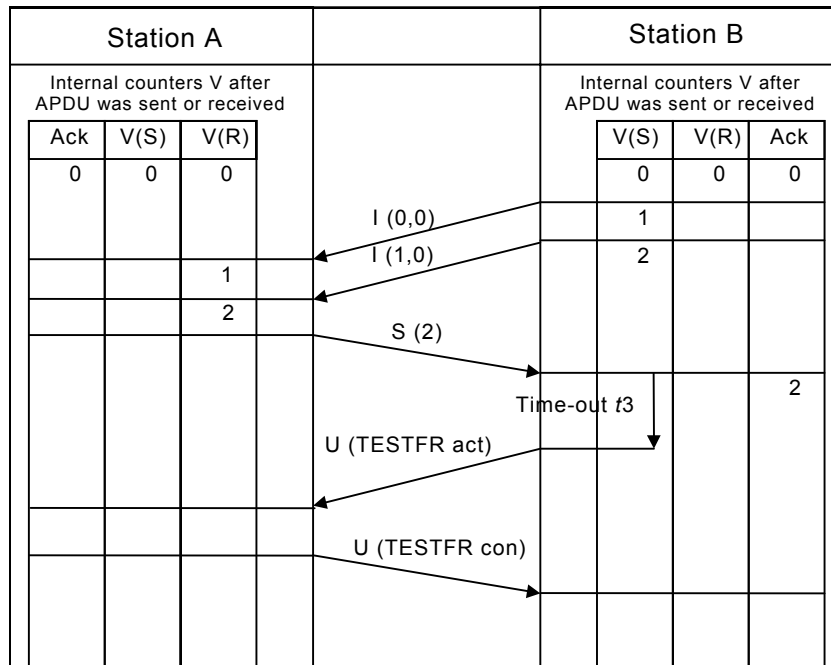
Figure 12 – Time-out in case of a not acknowledged last I format APDU

## 5.2 Test procedures

Unused, but open, connections may be periodically tested in both directions by sending test APDUs (TESTFR = act) which are confirmed by the receiving station sending TESTFR = con. Both stations may initiate the test procedure after a specified period of time in which no data transfers occur (time out). The reception of every frame – I frame, S frame or U frame – retriggers timer t3.

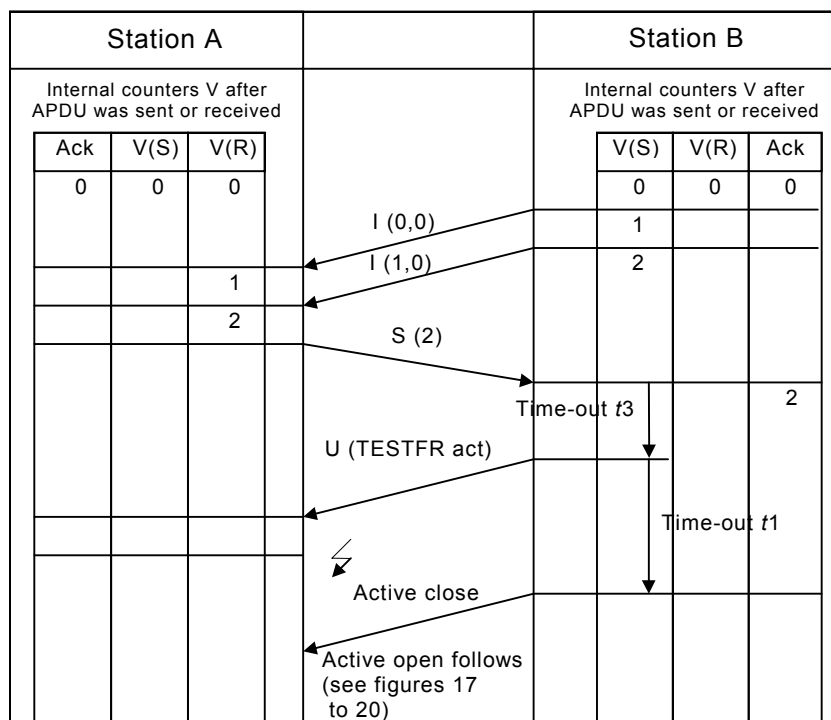
Station B has to supervise the connection independently. However, as long as it receives test frames from station A, it will not send test frames.

The test procedure can also be initiated on "active" connections where absence of activity is possible for extended times and connectivity needs to be assured.



IEC 2797/2000

Figure 13 – Undisturbed test procedure



IEC 2798/2000

Figure 14 – Unconfirmed test procedure