INTERNATIONAL STANDARD

IEC 60870-5-104

Second edition
2006-06

Telecontrol equipment and systems –

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

This ***English-language*** *version is derived from the original* ***bilingual*** *publication by leaving out all French-language pages. Missing page numbers correspond to the French-language pages.*

Reference number
IEC 60870-5-104:2006(E)

Publication numbering

As from 1 January 1997 all IEC publications are issued with a designation in the 60000 series. For example, IEC 34-1 is now referred to as IEC 60034-1.

Consolidated editions

The IEC is now publishing consolidated versions of its publications. For example, edition numbers 1.0, 1.1 and 1.2 refer, respectively, to the base publication, the base publication incorporating amendment 1 and the base publication incorporating amendments 1 and 2.

Further information on IEC publications

The technical content of IEC publications is kept under constant review by the IEC, thus ensuring that the content reflects current technology. Information relating to this publication, including its validity, is available in the IEC Catalogue of publications (see below) in addition to new editions, amendments and corrigenda. Information on the subjects under consideration and work in progress undertaken by the technical committee which has prepared this publication, as well as the list of publications issued, is also available from the following:

- **IEC Web Site (www.iec.ch)**

- **Catalogue of IEC publications**

  The on-line catalogue on the IEC web site (www.iec.ch/searchpub) enables you to search by a variety of criteria including text searches, technical committees and date of publication. On-line information is also available on recently issued publications, withdrawn and replaced publications, as well as corrigenda.

- **IEC Just Published**

  This summary of recently issued publications (www.iec.ch/online_news/ justpub) is also available by email. Please contact the Customer Service Centre (see below) for further information.

- **Customer Service Centre**

  If you have any questions regarding this publication or need further assistance, please contact the Customer Service Centre:

Email: custserv@iec.ch
Tel: +41 22 919 02 11
Fax: +41 22 919 03 00

INTERNATIONAL STANDARD

IEC 60870-5-104

Second edition
2006-06

Telecontrol equipment and systems –

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

International Electrotechnical Commission, 3, rue de Varembé, PO Box 131, CH-1211 Geneva 20, Switzerland
Telephone: +41 22 919 02 11 Telefax: +41 22 919 03 00 E-mail: inmail@iec.ch Web: www.iec.ch

Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

PRICE CODE XB

For price, see current catalogue

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

TELECONTROL EQUIPMENT AND SYSTEMS –

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

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 60870-5-104 Ed.2 has been prepared by IEC technical committee 57: Power systems management and associated information exchange.

This second edition cancels and replaces the first edition published in 2000 and constitutes a technical revision. The main changes of this second edition with respect to the previous edition are as follows: improvement of the sequences and interoperability of the protocol and addition of new functions for the handling of redundant connections.

The text of this standard is based on the following documents:

FDIS	Report on voting
57/812/FDIS	57/819/RVD

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC directives, Part 2.

IEC 60870-5 consists of the following parts, under the general title *Telecontrol equipment and systems – Part 5: Transmission protocols*

Part 5: Transmission protocols – Section One: Transmission frame formats

Part 5: Transmission protocols – Section 2: Link transmission procedures

Part 5: Transmission protocols – Section 3: General structure of application data

Part 5: Transmission protocols – Section 4: Definition and coding of application information elements

Part 5: Transmission protocols – Section 5: Basic application functions

Part 5-6: Guidelines for conformance testing for the IEC 60870-5 companion standards

Part 5-101: Transmission protocols – Companion standard for basic telecontrol tasks

Part 5: Transmission protocols – Section 102: Companion standard for the transmission of integrated totals in electric power systems

Part 5-103: Transmission protocols – Companion standard for the informative interface of protection equipment

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

Part 5-601: Conformance test cases for the IEC 60870-5-101 companion standard

The committee has decided that the contents of this publication will remain unchanged until the maintenance result date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- reconfirmed;
- withdrawn;
- replaced by a revised edition, or
- amended.

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 referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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 60870-5-101:2003, *Telecontrol equipment and systems – Part 5-101: Transmission protocols – Companion standard for basic telecontrol tasks*

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)*

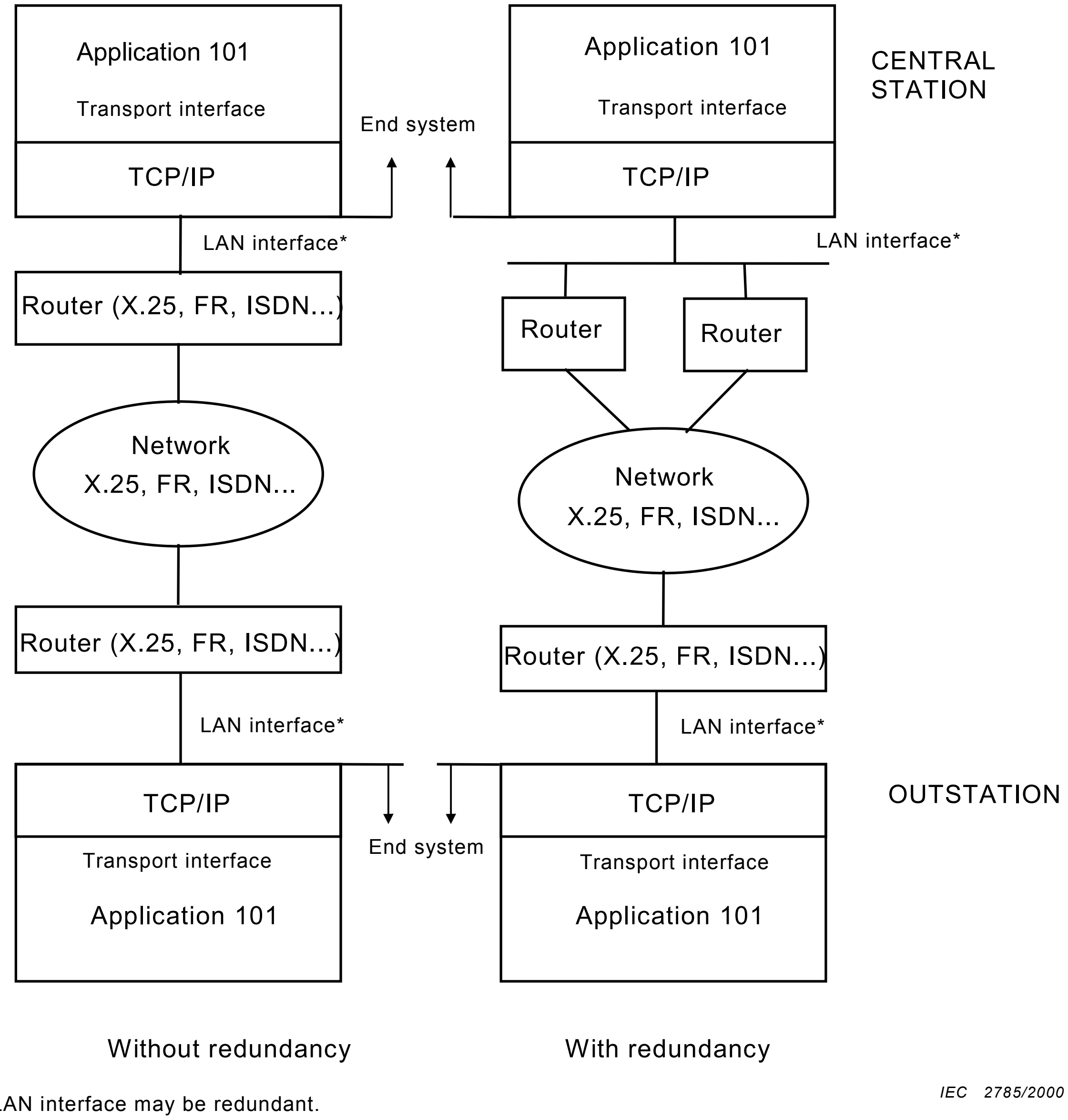
3 General architecture

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.



* The LAN interface may be redundant.

Figure 1 – General architecture (example)

4 Protocol structure

Figure 2 shows the protocol structure of the end system.

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

IEC 2786/2000

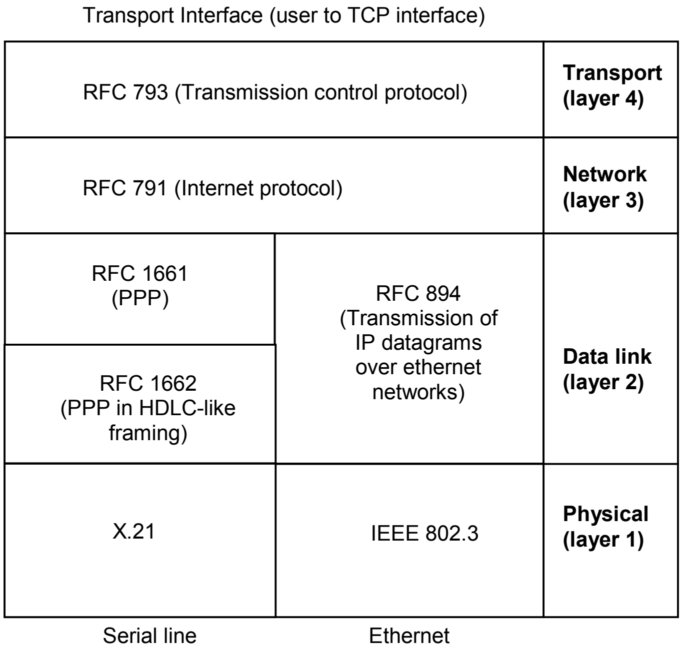
Figure 2 – Selected standard provisions of the defined telecontrol companion standard

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.



IEC 2787/2000

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

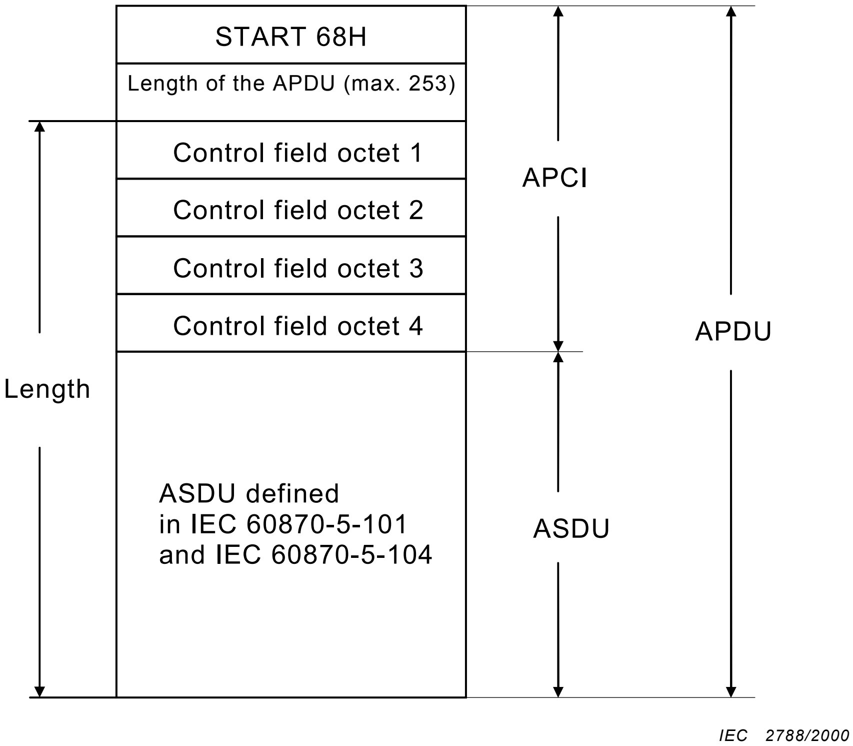


Figure 4 – APDU of the defined telecontrol companion standard

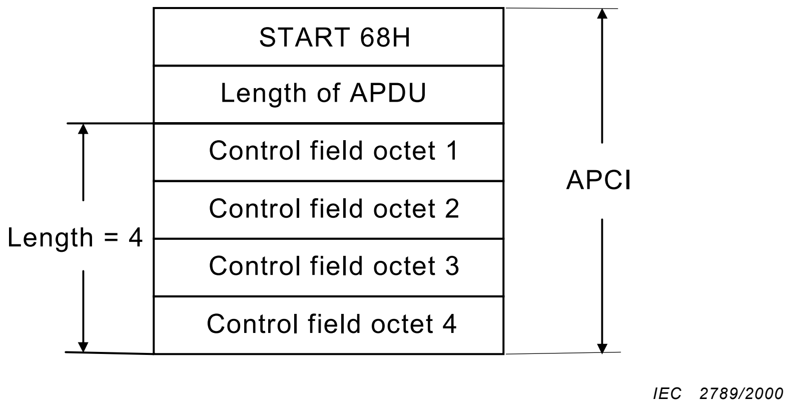


Figure 5 – APCI of the defined telecontrol companion standard

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.

Bit 8 – 2	Bit 1	
Send Sequence Number N(S) LSB	0	octet 1
MSB Send Sequence Number N(S)		octet 2
Receive Sequence Number N(R) LSB	0	octet 3
MSB Receive Sequence Number N(R)		octet 4

IEC 2790/2000

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.

Bit 8 – 3	Bit 2	Bit 1	
0	0	1	octet 1
0			octet 2
Receive Sequence Number N(R) LSB		0	octet 3
MSB Receive Sequence Number N(R)			octet 4

IEC 2791/2000

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 <= 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.

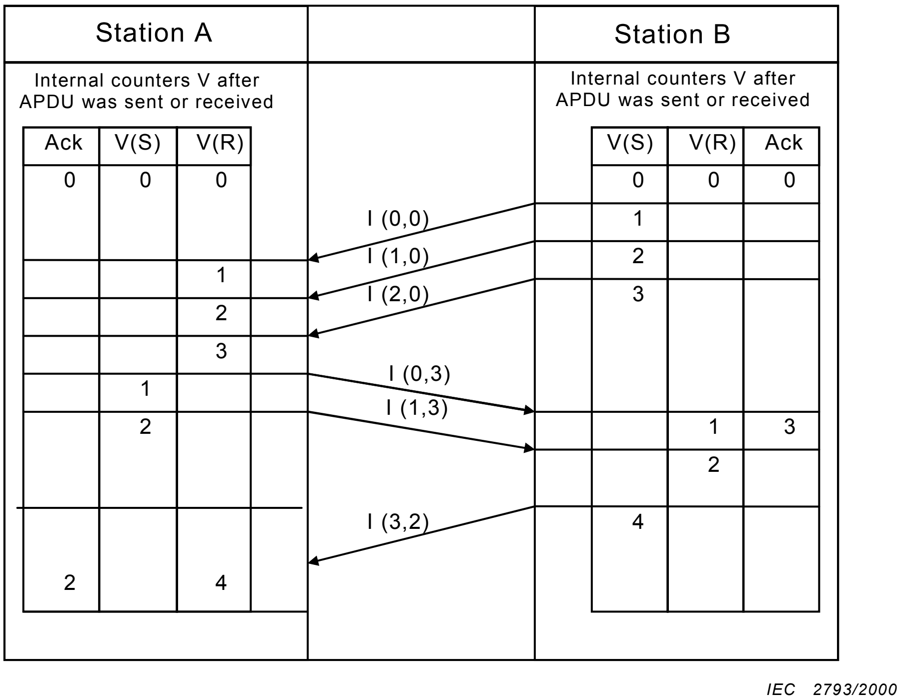


Figure 9 – Undisturbed sequences of numbered I format APDUs

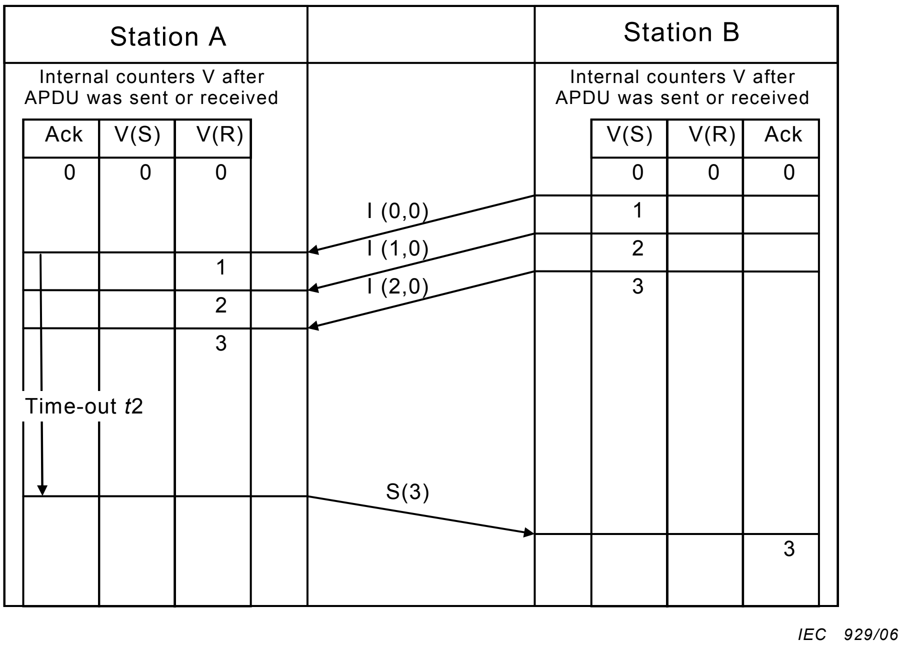
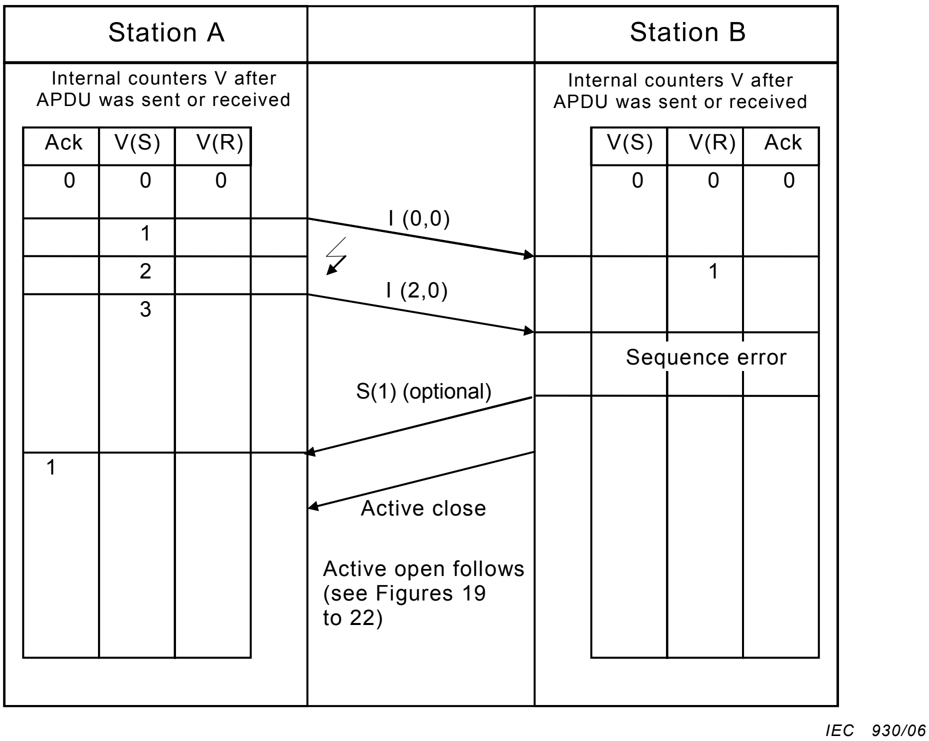


Figure 10 – Undisturbed sequences of numbered I format APDUs acknowledged by an S format APDU



NOTE To avoid retransmission of APDU's that have already been accepted, an S-frame should, if possible, be sent prior to the active close.

Figure 11 – Disturbed sequence of numbered I format APDUs

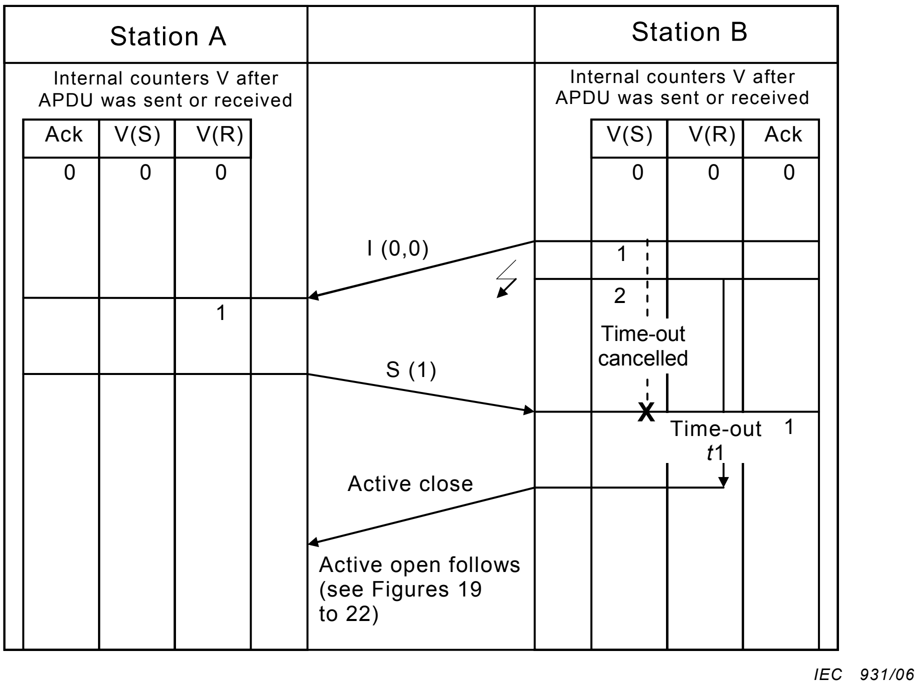


Figure 12 – Time-out in case of a not acknowledged last I format APDU

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.

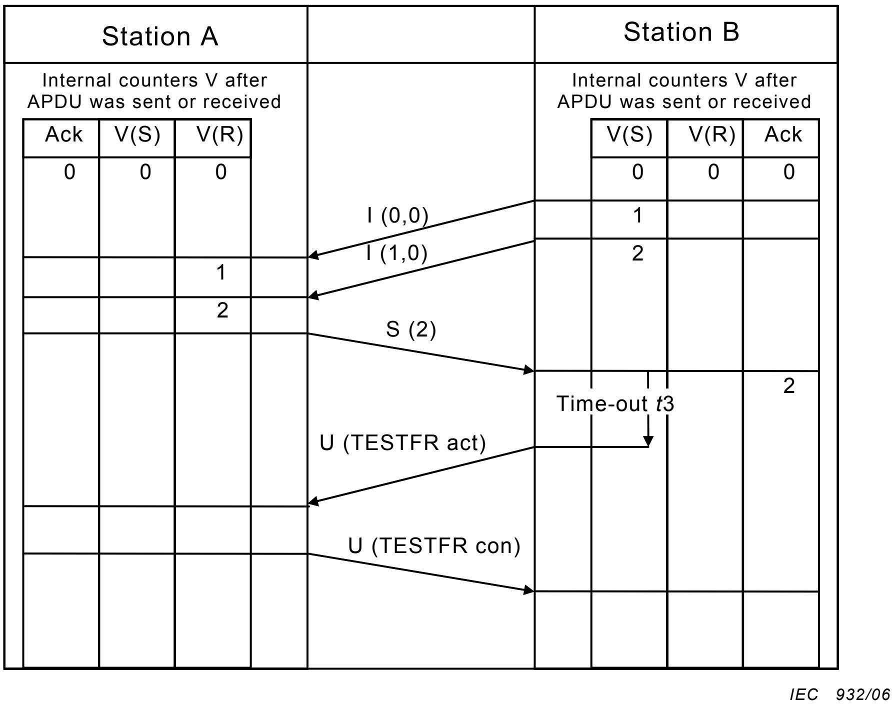


Figure 13 – Undisturbed test procedure

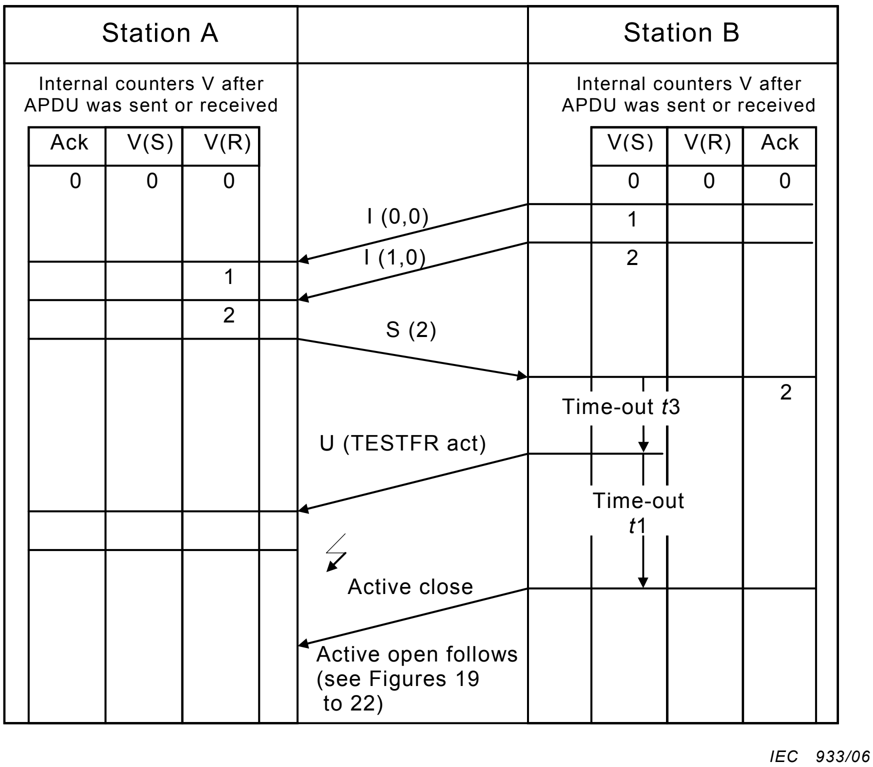


Figure 14 – Unconfirmed test procedure

5.3 Transmission control using Start/Stop

STARTDT (Start Data Transfer) and STOPDT (Stop Data Transfer) are used by the controlling station (for example, Station A), to control the data transfer from a controlled station (Station B). This is useful, for example, when more than one connection between the stations is open and therefore available, but only one connection at a time is used for the data transfer. The defined functionality for STARTDT and STOPDT avoids loss of data in the case of switchover from one connection to another. STARTDT and STOPDT are also used with single connections between the stations to control the traffic on the connection.

When the connection is established, user data transfer is not automatically enabled from the controlled station on that connection, i.e. STOPDT is the default state when a connection is established. In this state, the controlled station does not send any data via this connection, except unnumbered control functions and confirmations to such functions. The controlling station must activate the user data transfer on a connection by sending a STARTDT act via this connection. The controlled station responds to this command with a STARTDT con. If the STARTDT is not confirmed, the connection is closed by the controlling station. This implies that after station initialization (see 7.1) STARTDT must always be sent before any user data transfer from the controlled station (for example, general interrogated information) is initiated. Any pending user data in the controlled station is sent only after the STARTDT con.

STARTDT/STOPDT is a mechanism for the controlling station to activate/deactivate the monitoring direction. The controlling station may send commands or setpoints even if it has not yet received the activation confirmation. Send and receive counters continue their functionality independent of the use of STARTDT/STOPDT.

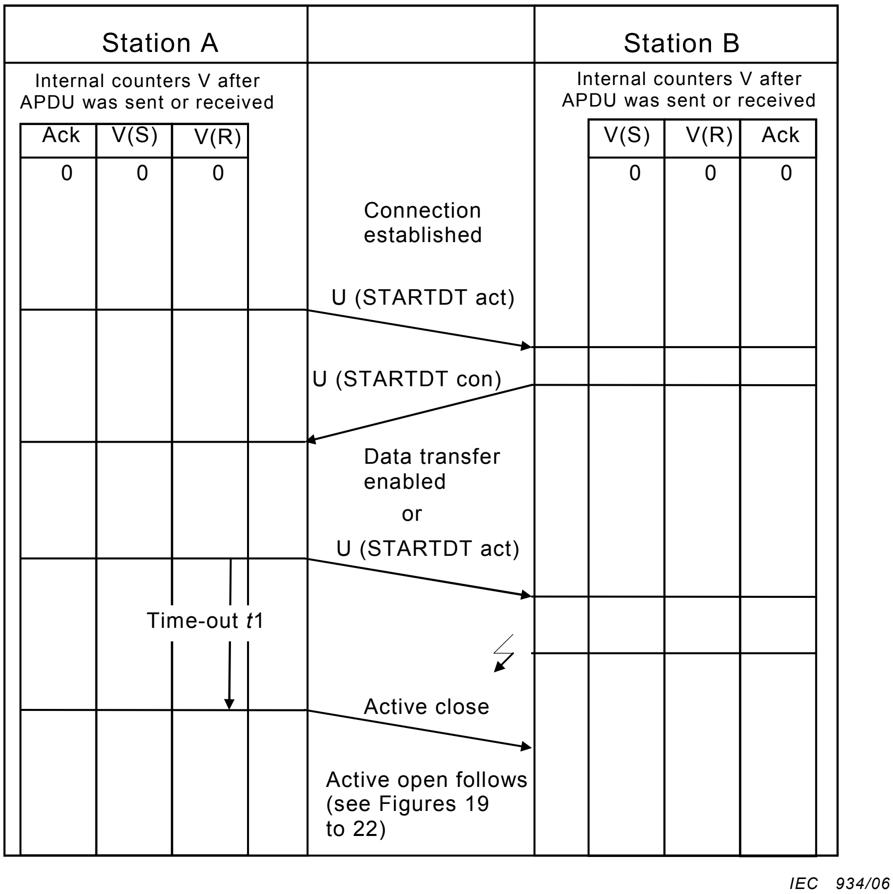


Figure 15 – Start data transfer procedure

In the case of, for example, a switchover from an active connection to another connection (for example, by an operator), the controlling station first transmits a STOPDT act on the active connection. The controlled station stops the user data transfer via this connection and returns a STOPDT con. Pending ACKs to user data can be sent from the point of time when the controlled station receives STOPDT act to the point of time when it returns STOPDT con. After receiving the STOPDT con, the controlling station may close the connection. A STARTDT on the other established connection is needed to start the data transfer from the controlled station on that connection (see figure 17).

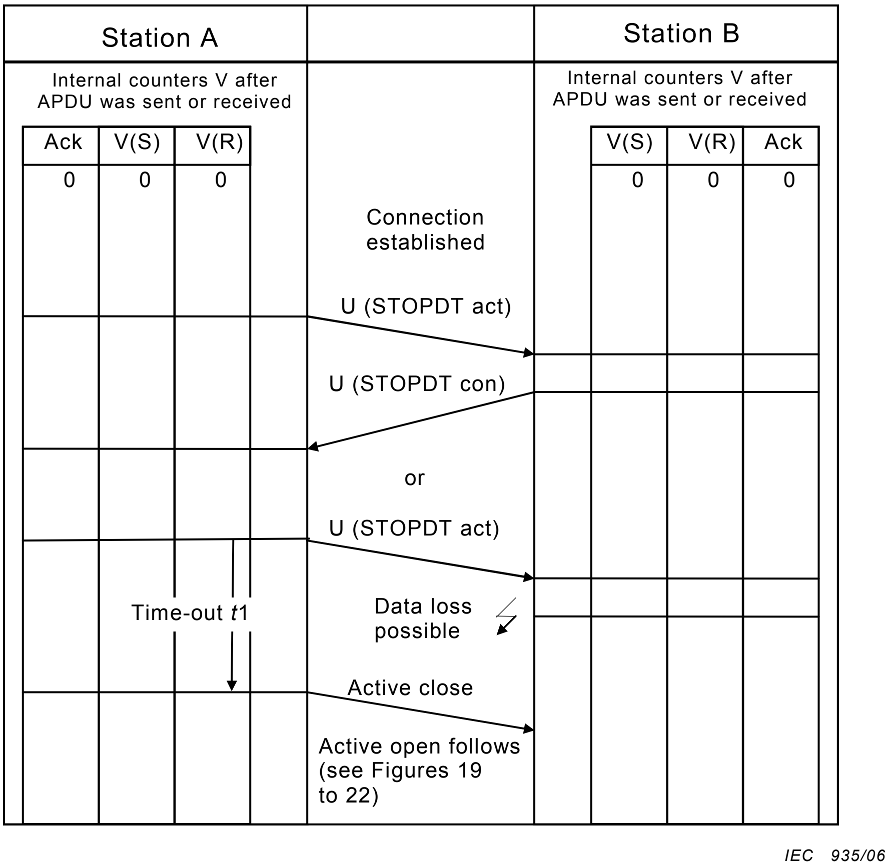
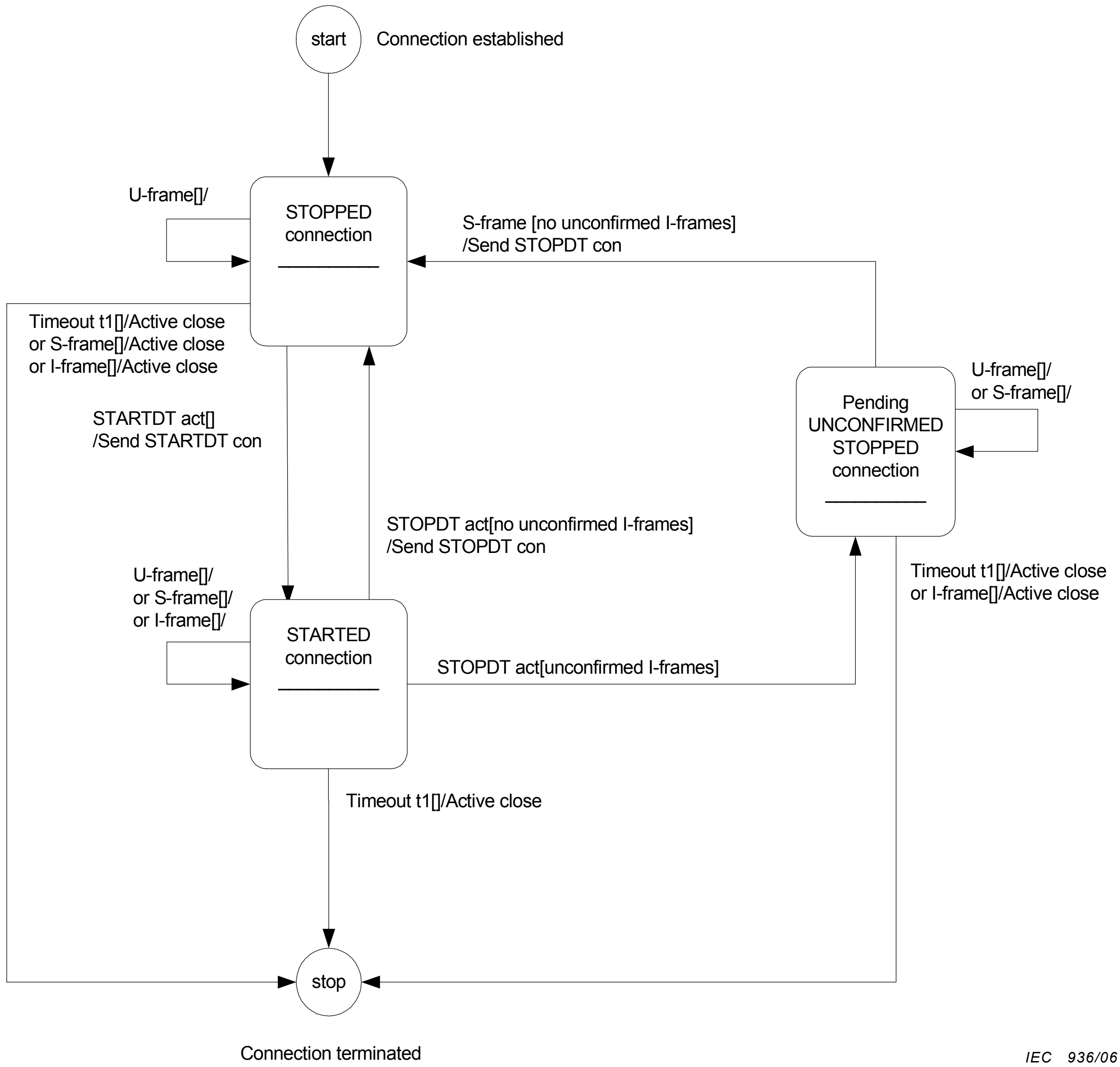


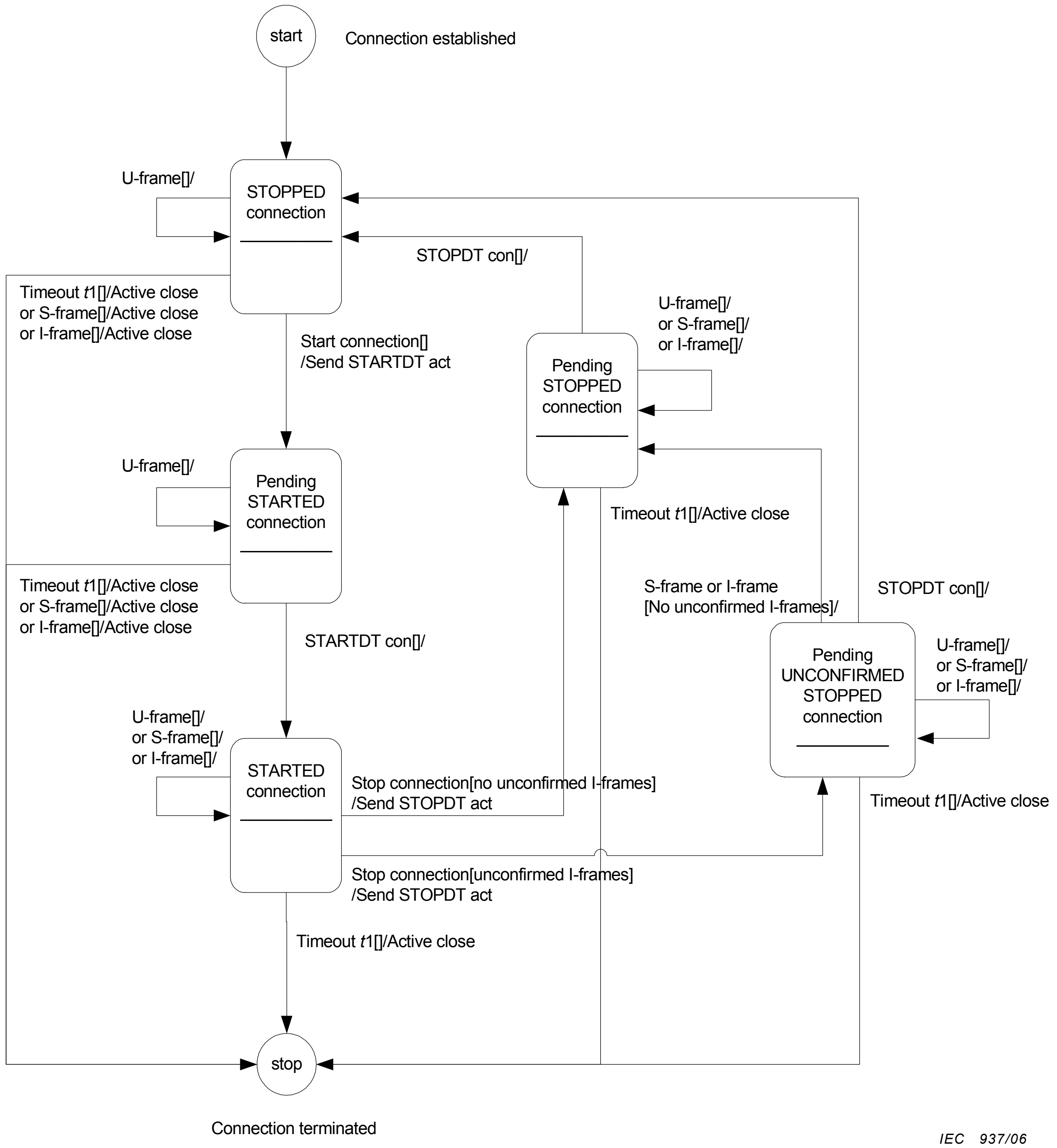
Figure 16 – Stop data transfer procedure



NOTE 1 Connection terminated means that there is no longer any data exchange betwen TCP and the application protocol (CS104).

NOTE 2 *t*1 is the timeout of a sent U-frame or I-frame.

Figure 17 – State transition diagram for Start/Stop procedure (controlled station)



NOTE 1 Connection terminated means that there is no longer any data exchange betwen TCP and the application protocol (CS104).

NOTE 2 *t*1 is the timeout of a sent U-frame or I-frame.

Figure 18 – State transition diagram for Start/Stop procedure (controlling station)

STOPDT act stops the transmission of I-frames immediately.

The controlling station should, however, confirm all received messages before sending STOPDT act, and the controlled station should confirm all received messages before returning STOPDT con. This is similar to the case with the pending unconfirmed message at connection closure, see Figure 11.

The controlling station should also immediately send an S-frame upon receiving an I-frame while in the Pending STOPPED state or Pending UNCONFIRMED STOPPED state. This will allow the controlled station to send its STOPDT con sooner (see figure 18).

If unconfirmed messages exist in the controlling station, the controlled station must confirm these messages by sending an S-frame before sending out the STOPDT con. If unconfirmed messages exist in the controlled station, the controlled station must wait for an incoming S-frame confirming these messages before sending out the STOPDT con.

After any connection re-establishment, unconfirmed messages may be transmitted when the Start procedure is completed, if required by the user process.

5.4 Portnumber

Every TCP address consists of an IP address and a port number. Every equipment connected to the TCP-LAN has its individual IP address, while the standard port number for IEC 60870-5-104 is defined to be 2404, confirmed by IANA.

The server (controlled station) uses the port number 2404 in all cases, both for the listening port and the established connections. The client (controlling station) may use other port numbers, for example ephemeral port numbers, as allocated by the client's TCP implementation.

5.5 Maximum number of outstanding I format APDUs (k)

The value of k shall indicate the maximum number of sequentially numbered I format APDUs that the DTE may have outstanding (i.e. unacknowledged) at a given time. Each I frame is sequentially numbered and may have the value 0 through modulus n minus 1, where "modulus" is the modulus of the sequence numbers which is defined by the parameter n. The value of k shall never exceed n – 1 for modulo n operation (see 2.3.2.2.1 and 2.4.8.6 of the ITU-T X.25 recommendation).

– The transmitter stops the transmission at k unacknowledged I format APDUs.
– The receiver acknowledges at the latest after receiving w = I format APDUs*
– The maximum number of k is n – 1 for modulo n operation.

Maximum range of values of k: 1 to 32767 (2^{15}–1) APDUs, accuracy 1 APDU.

Maximum range of values of w: 1 to 32767 APDUs, accuracy 1 APDU (recommendation: w should not exceed two-thirds of k).

6 Selection of ASDUs defined in IEC 60870-5-101 and additional ASDUs

The following ASDUs defined in IEC 60870-5-101 and in clause 8 of this standard are valid:

---

* Acknowledging before k is reached avoids a transmission stop.

Table 1 – Process information in monitor direction

TYPE IDENTIFICATION		:=	UI8[1..8]<0..44>	
	<0>	:=	not defined	
	<1>	:=	single-point information	M_SP_NA_1
	<3>	:=	double-point information	M_DP_NA_1
	<5>	:=	step position information	M_ST_NA_1
	<7>	:=	bitstring of 32 bits	M_BO_NA_1
	<9>	:=	measured value, normalized value	M_ME_NA_1
	<11>	:=	measured value, scaled value	M_ME_NB_1
	<13>	:=	measured value, short floating point number	M_ME_NC_1
	<15>	:=	integrated totals	M_IT_NA_1
	<20>	:=	packed single-point information with status change detection	M_PS_NA_1
	<21>	:=	measured value, normalized value without quality descriptor	M_ME_ND_1
	<22..29>	:=	reserved for further compatible definitions	
*	<30>	:=	single-point information with time tag CP56Time2a	M_SP_TB_1
*	<31>	:=	double-point information with time tag CP56Time2a	M_DP_TB_1
*	<32>	:=	step position information with time tag CP56Time2a	M_ST_TB_1
*	<33>	:=	bitstring of 32 bit with time tag CP56Time2a	M_BO_TB_1
*	<34>	:=	measured value, normalized value with time tag CP56Time2a	M_ME_TD_1
*	<35>	:=	measured value, scaled value with time tag CP56Time2a	M_ME_TE_1
*	<36>	:=	measured value, short floating point number with time tag CP56Time2a	M_ME_TF_1
*	<37>	:=	integrated totals with time tag CP56Time2a	M_IT_TB_1
*	<38>	:=	event of protection equipment with time tag CP56Time2a	M_EP_TD_1
*	<39>	:=	packed start events of protection equipment with time tag CP56Time2a	M_EP_TE_1
*	<40>	:=	packed output circuit information of protection equipment with time tag CP56Time2a	M_EP_TF_1
	<41..44>	:=	reserved for further compatible definitions	

* These types are defined on IEC 60870-5-101.

Table 2 – Process information in control direction

TYPE IDENTIFICATION := UI8[1..8]<45..69>

CON <45>	:=	single command	C_SC_NA_1
CON <46>	:=	double command	C_DC_NA_1
CON <47>	:=	regulating step command	C_RC_NA_1
CON <48>	:=	set point command, normalized value	C_SE_NA_1
CON <49>	:=	set point command, scaled value	C_SE_NB_1
CON <50>	:=	set point command, short floating point number	C_SE_NC_1
CON <51>	:=	bitstring of 32 bits	C_BO_NA_1
<52..57>	:=	reserved for further compatible definitions	

ASDUs for process information in control direction with time tag:

CON <58>	:=	single command with time tag CP56Time2a	C_SC_TA_1
CON <59>	:=	double command with time tag CP56Time2a	C_DC_TA_1
CON <60>	:=	regulating step command with time tag CP56Time2a	C_RC_TA_1
CON <61>	:=	set point command, normalized value with time tag CP56Time2a	C_SE_TA_1
CON <62>	:=	set point command, scaled value with time tag CP56Time2a	C_SE_TB_1
CON <63>	:=	set point command, short floating-point number with time tag CP56Time2a	C_SE_TC_1
CON <64>	:=	bitstring of 32 bits with time tag CP56Time2a	C_BO_TA_1
<65..69>	:=	reserved for further compatible definitions	

Process information in control direction may be sent with or without a time tag but must not be mixed when sending to a given station.

NOTE ASDUs marked "**CON**" in the control direction are confirmed application services and may be mirrored in the monitor direction with different causes of transmission. These mirrored ASDUs are used for positive/negative acknowledgements (verifications).

Table 3 – System information in monitor direction

TYPE IDENTIFICATION := UI8[1..8]<70..99>			
<70>	:=	end of initialization	M_EI_NA_1
<71..99>	:=	reserved for further compatible definitions	

Table 4 – System information in control direction

TYPE IDENTIFICATION := UI8[1..8]<100..109>			
CON <100>	:=	interrogation command	C_IC_NA_1
CON <101>	:=	counter interrogation command	C_CI_NA_1
<102>	:=	read command	C_RD_NA_1
CON <103>	:=	clock synchronization command (optional, see 7.6)	C_CS_NA_1
CON <105>	:=	reset process command	C_RP_NA_1
CON <107>	:=	test command with time tag CP56Time2a	C_TS_TA_1
<108..109>	:=	reserved for further compatible definitions	

Table 5 – Parameter in control direction

TYPE IDENTIFICATION := UI8[1..8]<110..119>			
CON <110>	:=	parameter of measured value, normalized value	P_ME_NA_1
CON <111>	:=	parameter of measured value, scaled value	P_ME_NB_1
CON <112>	:=	parameter of measured value, short floating-point number	P_ME_NC_1
CON <113>	:=	parameter activation	P_AC_NA_1
<114..119>	:=	reserved for further compatible definitions	

Table 6 – File transfer

TYPE IDENTIFICATION := UI8[1..8]<120..127>			
<120>	:=	file ready	F_FR_NA_1
<121>	:=	section ready	F_SR_NA_1
<122>	:=	call directory, select file, call file, call section	F_SC_NA_1
<123>	:=	last section, last segment	F_LS_NA_1
<124>	:=	ack file, ack section	F_AF_NA_1
<125>	:=	segment	F_SG_NA_1
<126>	:=	directory	F_DR_TA_1
<127>	:=	Query Log – Request archive file	F_SC_NB_1

NOTE ASDUs marked **CON** in the control direction are confirmed application services and may be mirrored in the monitor direction with different causes of transmission. These mirrored ASDUs are used for positive/negative acknowledgements (verifications).

7 Mapping of selected application data units and functions to the TCP services

In this clause, the functions which are selected from IEC 60870-5-5 for use in this standard are specified. The application services defined in this standard are assigned to the suitable transport services defined in RFC 793. The ASDU labels specified are as defined in IEC 60870-5-5.

The controlling station is equivalent to the client (connector), the controlled station to the server (listener).

7.1 Station initialization (6.1.5 to 6.1.7 of IEC 60870-5-5)

Release of connections may be initiated by either the controlling or the controlled station. Connection establishment is performed by

– the controlling station in case of a controlled station as a partner;

– a fixed selection (parameter) in the case of two equivalent controlling stations or partners (see figure 1).

Figure 19 shows that an established connection may be closed by the controlling station giving an active close call to its TCP, followed by the controlled station giving a passive close to its TCP. The figure then shows the establishment of a new connection by the controlling station giving an active open call to its TCP after the controlled station has previously given a passive open call to its TCP. Finally, the figure shows the alternative active close of the connection by the controlled station.

Figure 20 shows that, during the initialization of the controlling station, a connection is established with each controlled station in turn. Starting with station 1 the controlling station gives an active open call to its TCP which results in connection establishment if the TCP of station 1 has the listen status (status not shown in the figure). This is then repeated for the remaining controlled stations.

Figure 21 shows the controlling station repeatedly attempting to establish a connection with a controlled station. These attempts fail until the controlled station has performed a local initialization and given a passive open call to its TCP which has then acquired the listen status (status not shown in the figure).

Figure 22 shows the controlling station establishing a connection by giving an active open call to its TCP. The controlling station then sends Reset_Process to the connected controlled station, which confirms back the Reset_Process and gives an active close call to its TCP. The connection then closes after the controlling station has given a passive close call to its TCP. Then the controlling station tries to connect the controlled station by giving cyclic active opens to its TCP. When the controlled station is again available, after its remote initialization, it returns a CLT=SYN, ACK. This results in the establishment of a new connection if the controlling station acknowledges the CLT=SYN, ACK.

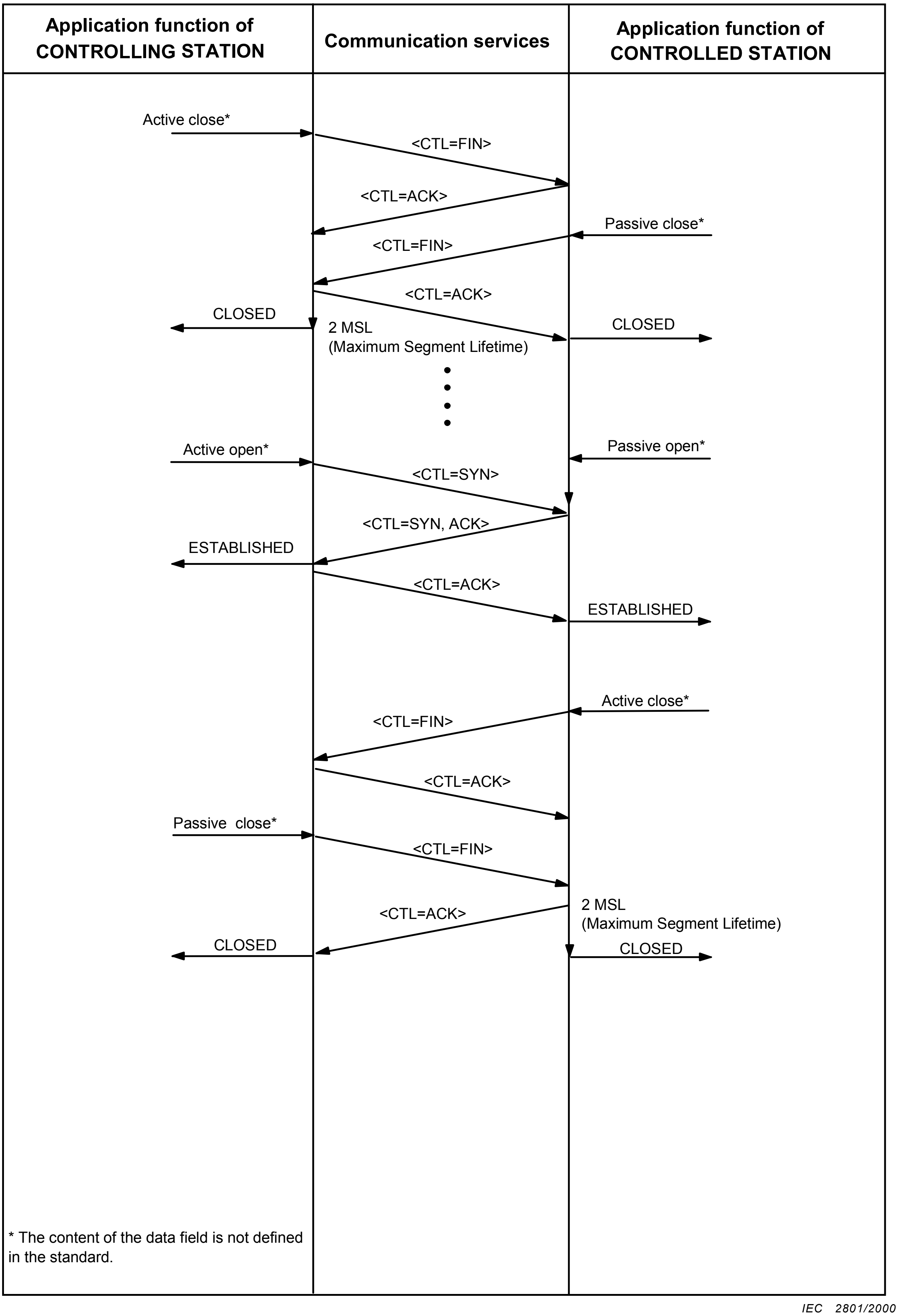


Figure 19 – TCP connection establishment and close

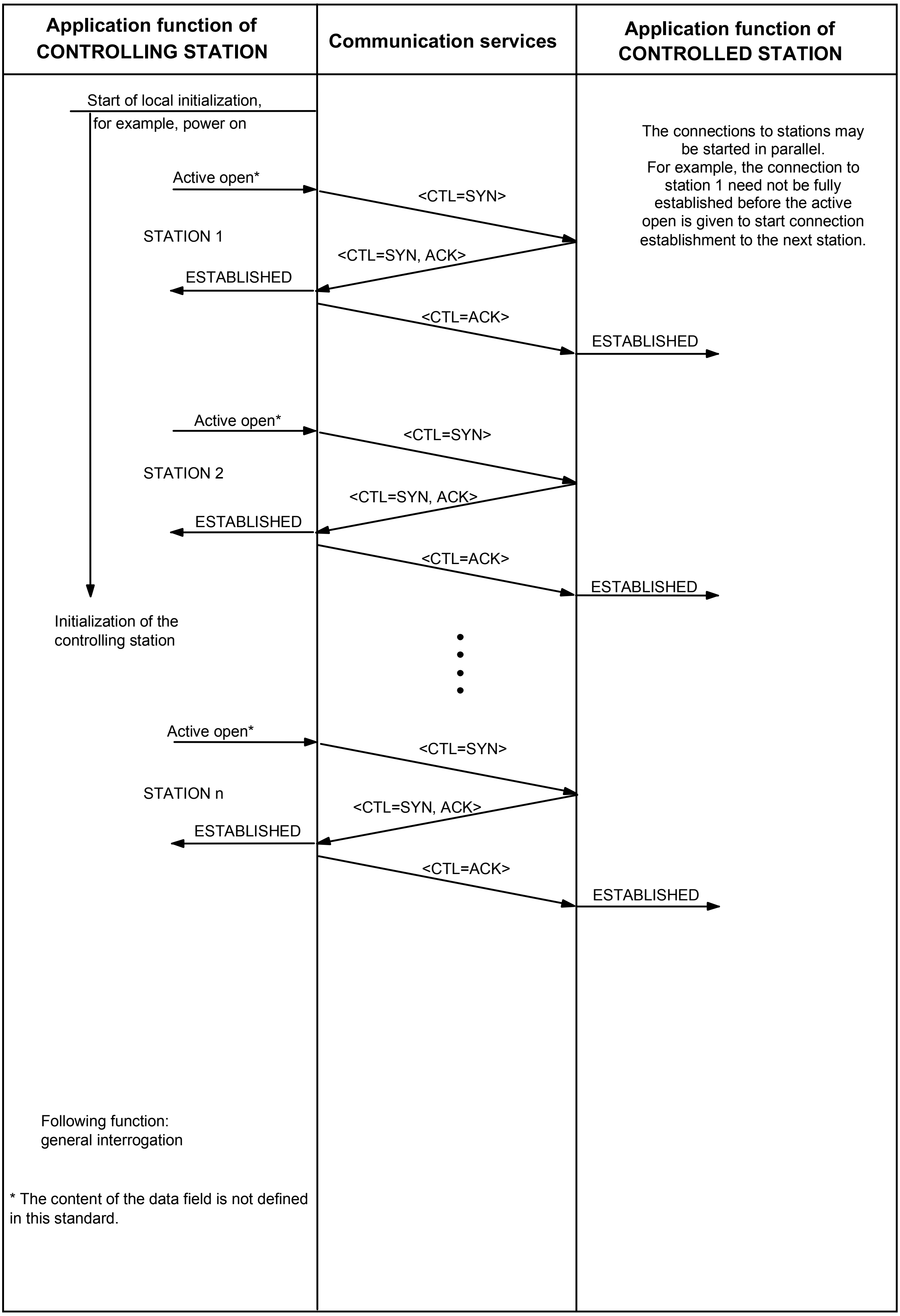


Figure 20 – Initialization of the controlling station

IEC 2802/2000

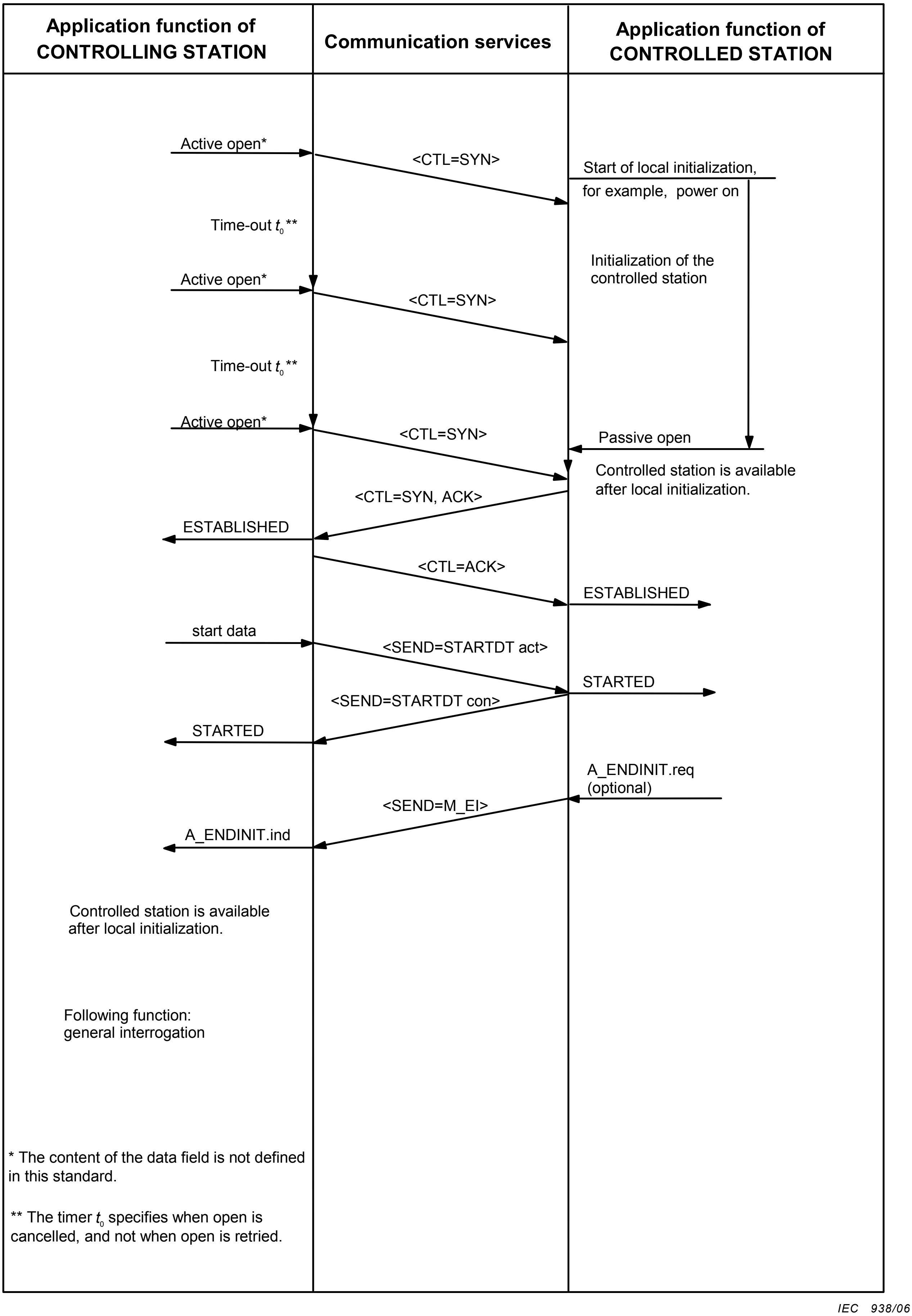
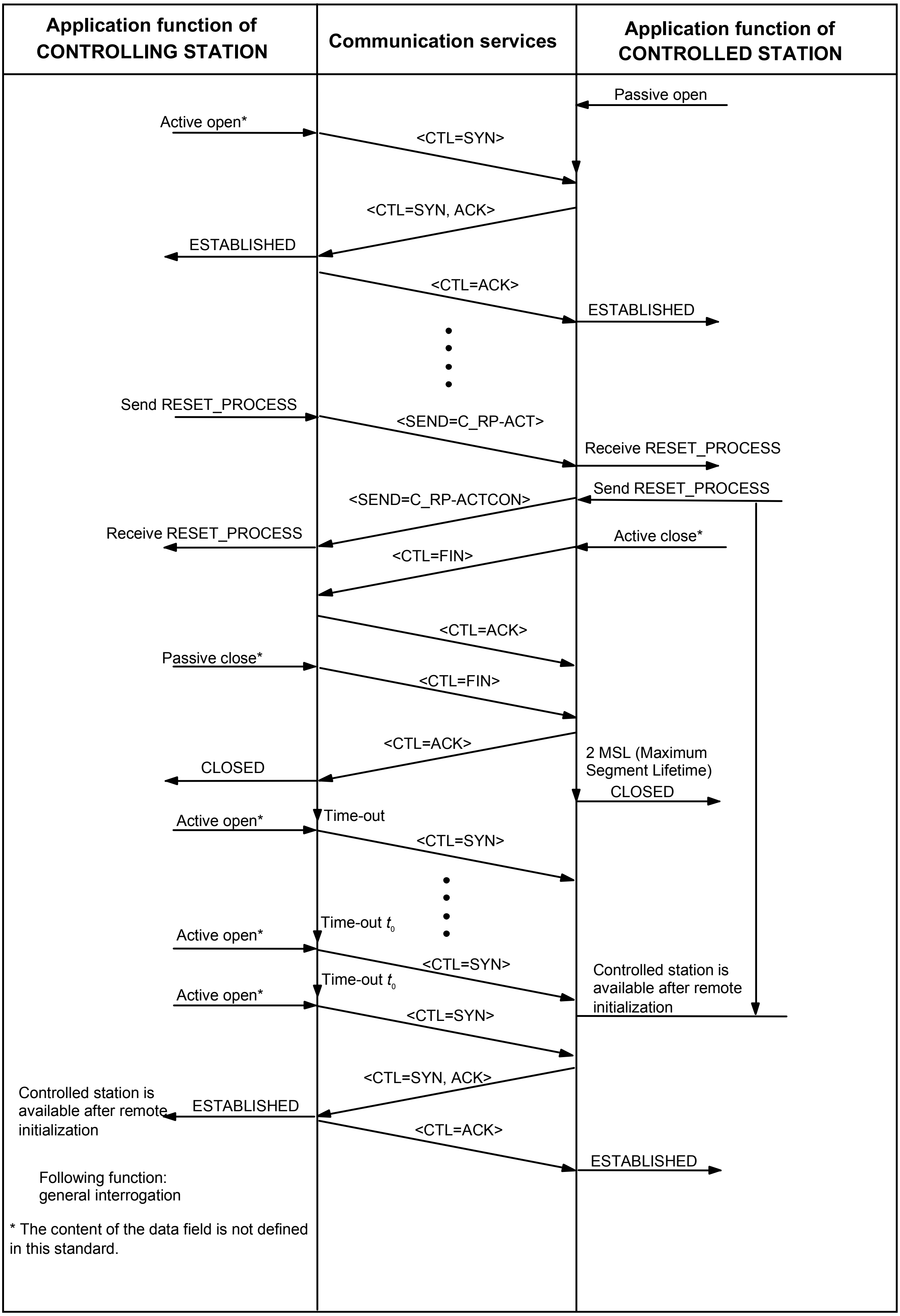


Figure 21 – Local initialization of the controlled station



IEC 2804/2000

Figure 22 – Remote initialization of the controlled station

7.2 Data acquisition by polling (6.2 of IEC 60870-5-5)

Request of user data class 1 and 2 are link functions of IEC 60870-5-2 and therefore not available in this standard. However, data may be read (requested) as shown in the bottom part of figure 10 of IEC 60870-5-5. The requesting of data by cyclic requests is permitted, but should be avoided. Such cyclic requests burden the network with excess transmission traffic.

Application Service IEC 60870-5-5	TCP Service RFC 793	ASDU Label IEC 60870-5-5
A_RD_DATA.req	send	C_RD
A_RD_DATA.ind	receive	C_RD
A_M_DATA.req	send	M
A_M_DATA.ind	receive	M

7.3 Cyclic data transmission (6.3 of IEC 60870-5-5)

Application Service IEC 60870-5-5	TCP Service RFC 793	ASDU Label IEC 60870-5-5
A_CYCLIC_DATA.req	send	M CYCLIC
A_CYCLIC_DATA.ind	receive	M CYCLIC

7.4 Acquisition of events (6.4 of IEC 60870-5-5)

Application Service IEC 60870-5-5	TCP Service RFC 793	ASDU Label IEC 60870-5-5
A_EVENT.req	send	M SPONT
A_EVENT.ind	receive	M SPONT

7.5 General interrogation (6.6 of IEC 60870-5-5)

Application Service IEC 60870-5-5	TCP Service RFC 793	ASDU Label IEC 60870-5-5
A_GENINCOM.req	send	C_IC ACT
A_GENINCOM.ind	receive	C_IC ACT
A_GENINACK.req	send	C_IC ACTCON
A_GENINACK.ind	receive	C_IC ACTCON
A_INTINF.req	send	M
A_INTINF.ind	receive	M
A_ENDINT.req	send	C_IC ACTTERM
A_ENDINT.ind	receive	C_IC ACTTERM

7.6 Clock synchronization (6.7 of IEC 60870-5-5)

Application Service IEC 60870-5-5	**TCP Service RFC 793**	**ASDU Label IEC 60870-5-5**
A_CLOCKSYN.req	send	C_CS ACT
A_CLOCKSYN.ind	receive	C_CS ACT
A_TIMEMESS.req	send	C_CS ACTCON
A_TIMEMESS.ind	receive	C_CS ACTCON

The clock synchronization procedure defined in IEC 60870-5-5 cannot be used in this standard because the link layer according to IEC 60870-5-2, which provides the exact time of sending the clock command, is no longer available.

However, clock synchronization may be used in configurations where the *maximum network delay* is *less* than the required accuracy of the clock in the receiving station. For example, if the network provider guarantees that the delay in the network will never be more than 400 ms (a typical X.25 WAN value) and the required accuracy in the controlled station is 1 s, the clock synchronization procedure is useful. Use of this procedure avoids the necessity of installing clock synchronization receivers or similar equipment in potentially several hundreds or thousands of controlled stations.

The procedure is a copy of that of 6.7 of IEC 60870-5-5, with the "first bit" and "time correction" requirements and link layer options (SEND/NO REPLY or SEND/CONFIRM) removed.

Clocks in controlled stations have to be synchronized with the clock in the controlling station to provide correct chronological sets of time-tagged events or information objects, whether they are transmitted to the controlling station or logged locally. The clocks are initially synchronized by the controlling station after system initialization and then re-synchronized periodically by agreement by transmitting C_CS ACT PDUs.

The C_CS ACT PDU contains the whole (date and time) current clock time with the required time resolution at the instant when the message is generated by the application layer. After the execution of the clock sync internally the controlled station generates a C_CS ACTCON PDU that contains the local time *before* it was synchronized. This message is transmitted after any buffered time-tagged PDUs, that may be waiting for transmission. Time-tagged events that occur *after* the internal clock synchronization are transmitted *after* the C_CS ACTCON PDU.

Controlled stations expect the reception of clock synchronization messages within agreed time intervals. When the synchronization command does not arrive within this time interval, the controlled station sets all time-tagged information objects with a mark that the time tag may be inaccurate (invalid). This mark is also set after station initializiation (warm and cold boot) of controlled stations before reception of a valid C_CS ACT PDU. Time-tagged events that occur after the reception of valid C_CS ACT PDU are transmitted without the mark.

7.6.1 Description of sequential procedure

(See figure 15 of IEC 60870-5-5.)

The application process in the controlling station sends the clock synchronization command as a CLOCKSYN.req primitive with the time as known in the application process and with the required accuracy to the communication services. The communication services transmit this request as a C_CS ACT PDU and delivers this request as a A_CLOCKSYN.ind primitive to the application process in the controlled station.

After the execution of the clock synchronization operation the application process of the controlled station produces the time message which is transmitted as a C_CS ACTCON PDU initiated by an A_TIMEMESS.req primitive. This request contains the time which is known in the application process in the controlled station *before* reception of the A_CLOCKSYN.ind. This PDU is issued to the application process of the controlling station as an A_TIMEMESS.ind primitive.

7.7 Command transmission (6.8 of IEC 60870-5-5)

Application Service IEC 60870-5-5	**TCP Service RFC 793**	**ASDU Label IEC 60870-5-5**
A_SELECT.req	send	C_SC, C_DC, C_SE, C_RC, C_BO ACT
A_SELECT.ind	receive	C_SC, C_DC, C_SE, C_RC, C_BO ACT
A_SELECT.res	send	C_SC, C_DC, C_SE, C_RC, C_BO ACTCON
A_SELECT.con	receive	C_SC, C_DC, C_SE, C_RC, C_BO ACTCON
A_BREAK.req	send	C_SC, C_DC, C_SE, C_RC, C_BO DEACT
A_BREAK.ind	receive	C_SC, C_DC, C_SE, C_RC, C_BO DEACT
A_BREAK.res	send	C_SC, C_DC, C_SE, C_RC, C_BO DEACTCON
A_BREAK.con	receive	C_SC, C_DC, C_SE, C_RC, C_BO DEACTCON
A_EXCO.req	send	C_SC, C_DC, C_SE, C_RC, C_BO ACT
A_EXCO.ind	receive	C_SC, C_DC, C_SE, C_RC, C_BO ACT
A_EXCO.res	send	C_SC, C_DC, C_SE, C_RC, C_BO ACTCON
A_EXCO.con	receive	C_SC, C_DC, C_SE, C_RC, C_BO ACTCON
A_RETURN_INF.req	send	M_SP, M_DP, M_ST
A_RETURN_INF.ind	receive	M_SP, M_DP, M_ST
A_COTERM.req	send	C_SC, C_DC, C_SE, C_RC, C_BO ACTTERM
A_COTERM.ind	receive	C_SC, C_DC, C_SE, C_RC, C_BO ACTTERM

7.8 Transmission of integrated totals (6.9 of IEC 60870-5-5)

Application Service IEC 60870-5-5	TCP Service RFC 793	ASDU Label IEC 60870-5-5
A_MEMCNT.req	send	C_CI ACT
A_MEMCNT.ind	receive	C_CI ACT
A_MEMCNT.res	send	C_CI ACTCON
A_MEMCNT.con	receive	C_CI ACTCON
A_MEMINCR.req	send	C_CI ACT
A_MEMINCR.ind	receive	C_CI ACT
A_MEMINCR.res	send	C_CI ACTCON
A_MEMINCR.con	receive	C_CI ACTCON
A_REQINTO.req	send	C_CI ACT
A_REQINTO.ind	receive	C_CI ACT
A_REQINTO.res	send	C_CI ACTCON
A_REQINTO.con	receive	C_CI ACTCON
A_INTO_INF.req	send	M_IT
A_INTO_INF.ind	receive	M_IT
A_ITERM.req	send	C_CI ACTTERM
A_ITERM.ind	receive	C_CI ACTTERM

7.9 Parameter loading (6.10 of IEC 60870-5-5)

Application Service IEC 60870-5-5	TCP Service RFC 793	ASDU Label IEC 60870-5-5
A_PARAM.req	send	P_ME ACT
A_PARAM.ind	receive	P_ME ACT
A_PARAM.res	send	P_ME ACTCON
A_PARAM.con	receive	P_ME ACTCON
A_PACTIV.req	send	P_AC ACT
A_PACTIV.ind	receive	P_AC ACT
A_PACTIV.res	send	P_AC ACTCON
A_PACTIV.con	receive	P_AC ACTCON
A_LCPACH.req	send	P_ME SPONT
A_LCPACH.ind	receive	P_ME SPONT

7.10 Test procedure (6.11 of IEC 60870-5-5)

Application Service IEC 60870-5-5	TCP Service RFC 793	ASDU Label IEC 60870-5-5
A_TEST.req	send	C_TS ACT
A_TEST.ind	receive	C_TS ACT
A_TEST.res	send	C_TS ACTCON
A_TEST.con	receive	C_TS ACTCON

7.11 File transfer (6.12 of IEC 60870-5-5) Control and monitor direction

Application Service IEC 60870-5-5	TCP Service RFC 793	ASDU Label IEC 60870-5-5
A_CALL_DIRECTORY.req	send	F_SC
A_CALL_DIRECTORY.ind	receive	F_SC
A_CALL_DIRECTORY.res	send	F_DR
A_CALL_DIRECTORY.con	receive	F_DR
A_SELECT_FILE.req	send	F_SC
A_SELECT_FILE.ind	receive	F_SC
A_FILE_READY.req	send	F_FR
A_FILE_READY.ind	receive	F_FR
A_CALL_FILE.req	send	F_SC
A_CALL_FILE.ind	receive	F_SC
A_SECTION1_READY.req	send	F_SR
A_SECTION1_READY.ind	receive	F_SR
A_CALL_SECTION1.req	send	F_SC
A_CALL_SECTION1.ind	receive	F_SC
A_SEGMENT1.req	send	F_SG
A_SEGMENT1.ind	receive	F_SG
A_SEGMENTn.req	send	F_SG
A_SEGMENTn.ind	receive	F_SG
A_LAST_SEGMENT.req	send	F_LS
A_LAST_SEGMENT.ind	receive	F_LS
A_ACK_SECTION1.req	send	F_AF
A_ACK_SECTION1.ind	receive	F_AF
A_SECTIONm_READY.req	send	F_SR
A_SECTIONm_READY.ind	receive	F_SR

Application Service IEC 60870-5-5	Transport Service RFC 793	ASDU Label IEC 60870-5-5
A_CALL_SECTIONm.req	send	F_SC
A_CALL_SECTIONm.ind	receive	F_SC
A_ACK_SECTIONm.req	send	F_AF
A_ACK_SECTIONm.ind	receive	F_AF
A_LAST_SECTION.req	send	F_LS
A_LAST_SECTION.ind	receive	F_LS
A_ACK_FILE.req	send	F_AF
A_ACK_FILE.ind	receive	F_AF
A_DIRECTORY.req	send	F_DR
A_DIRECTORY.ind	receive	F_DR

8 ASDUs for process information in control direction with time tag

This clause defines the additional ASDUs in the control direction which are extended with the time tag CP56Time2a. This time includes date and clock time in milliseconds up to years and is defined in IEC 60870-5-101. When using networks that might cause undesireable delays of commands, sending ASDUs with a time tag is recommended. A controlled station receiving a command or set point which has exceeded the maximum allowable delay (system-specific parameter) will not return a protocol response (i.e. the controlled station does not return a positive ACTCON nor a negative ACTCON). This is because the confirmation could be significantly delayed, and might not readily be associated with the original request. The command is passed to the controlled station application so that it can identify that the command was received “too late”, but must not perform any command action. The time tag contains the time at which the command is initiated in the controlling station.

8.1 TYPE IDENT 58: C_SC_TA_1
Single command with time tag CP56Time2a

Single information object (SQ = 0)

0 0 1 1 1 0 1 0	TYPE IDENTIFICATION	DATA UNIT IDENTIFIER Defined in 7.1 of IEC 60870-5-101
0 0 0 0 0 0 0 1	VARIABLE STRUCTURE QUALIFIER	
Defined in 7.2.3 of IEC 60870-5-101	CAUSE OF TRANSMISSION	
Defined in 7.2.4 of IEC 60870-5-101	COMMON ADDRESS OF ASDU	
Defined in 7.2.5 of IEC 60870-5-101	INFORMATION OBJECT ADDRESS	INFORMATION OBJECT
S/E | QU | 0 | SCS	SCO = Single command, defined in 7.2.6.15 of IEC 60870-5-101	
CP56Time2a Defined in 7.2.6.18 of IEC 60870-5-101	Seven-octet binary time (Date and clock time in milliseconds up to years)	

IEC 2805/2000

Figure 23 – ASDU: C_SC_TA_1
Single command with time tag CP56Time2a

C_SC_TA_1 := CP{Data unit identifier,Information object address,SCO,CP56Time2a}

CAUSES OF TRANSMISSION used with

TYPE IDENT 58 := C_SC_TA_1

CAUSE OF TRANSMISSION

In control direction:
<6> := activation
<8> := deactivation
In monitor direction:
<7> := activation confirmation
<9> := deactivation confirmation
<10> := activation termination
<44> := unknown type identification
<45> := unknown cause of transmission
<46> := unknown common address of ASDU
<47> := unknown information object address

8.2 TYPE IDENT 59: C_DC_TA_1
Double command with time tag CP56Time2a

Single information object (SQ = 0)

0 0 1 1 1 0 1 1	TYPE IDENTIFICATION	DATA UNIT IDENTIFIER Defined in 7.1 of IEC 60870-5-101
0 0 0 0 0 0 0 1	VARIABLE STRUCTURE QUALIFIER	
Defined in 7.2.3 of IEC 60870-5-101	CAUSE OF TRANSMISSION	
Defined in 7.2.4 of IEC 60870-5-101	COMMON ADDRESS OF ASDU	
Defined in 7.2.5 of IEC 60870-5-101	INFORMATION OBJECT ADDRESS	INFORMATION OBJECT
S/E | QU | DCS	DCO = Double command, defined in 7.2.6.16 of IEC 60870-5-101	
CP56Time2a Defined in 7.2.6.18 of IEC 60870-5-101	Seven-octet binary time (Date and clock time in milliseconds up to years)	

IEC 2806/2000

Figure 24 – ASDU: C_DC_TA_1
Double command with time tag CP56Time2a

C_DC_TA_1 := CP{Data unit identifier,Information object address,DCO,CP56Time2a }

CAUSES OF TRANSMISSION used with

TYPE IDENT 59 := C_DC_TA_1

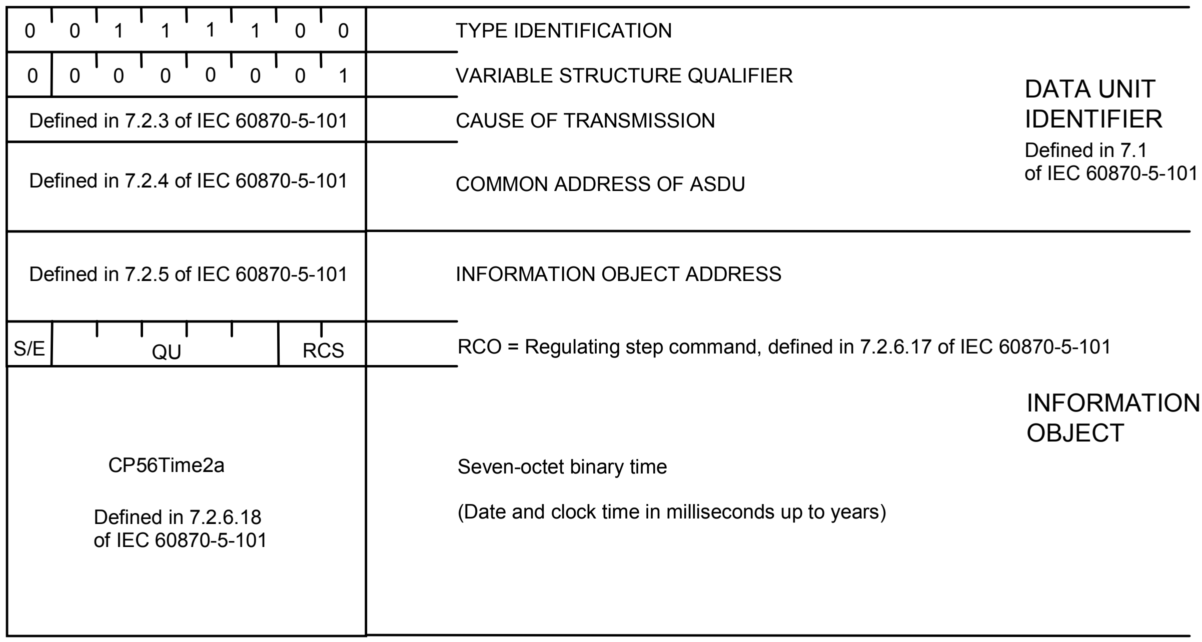
CAUSE OF TRANSMISSION

In control direction:
<6> := activation
<8> := deactivation

In monitor direction:
<7> := activation confirmation
<9> := deactivation confirmation
<10> := activation termination
<44> := unknown type identification
<45> := unknown cause of transmission
<46> := unknown common address of ASDU
<47> := unknown information object address

8.3 TYPE IDENT 60: C_RC_TA_1
Regulating step command with time tag CP56Time2a

Single information object (SQ = 0)



IEC 2807/2000

Figure 25 – ASDU: C_RC_TA_1
Regulating step command with time tag CP56Time2a

C_RC_TA_1 := CP{Data unit identifier,Information object address,RCO,CP56Time2a}

CAUSES OF TRANSMISSION used with

TYPE IDENT 60 := C_RC_TA_1

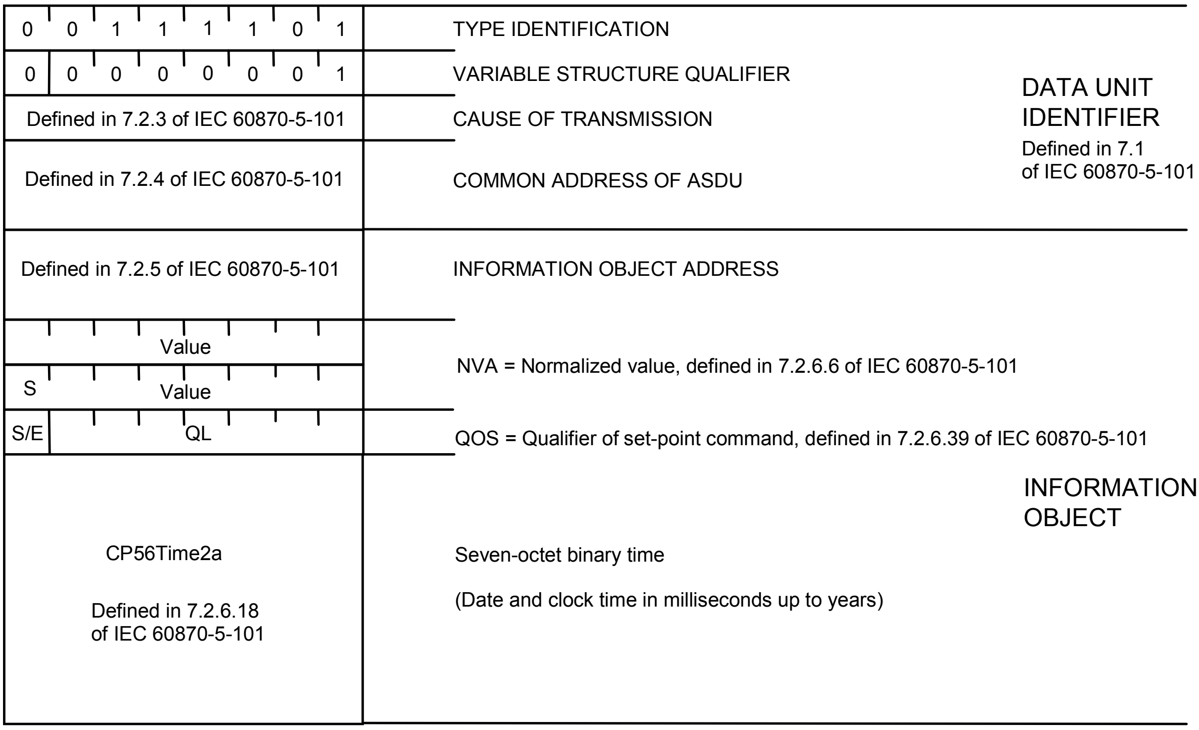
CAUSE OF TRANSMISSION

In control direction:
<6> := activation
<8> := deactivation

In monitor direction:
<7> := activation confirmation
<9> := deactivation confirmation
<10> := activation termination
<44> := unknown type identification
<45> := unknown cause of transmission
<46> := unknown common address of ASDU
<47> := unknown information object address

8.4 TYPE IDENT 61: C_SE_TA_1
Set-point command with time tag CP56Time2a, normalized value

Single information object (SQ = 0)



IEC 2808/2000

Figure 26 – ASDU: C_SE_TA_1
Set-point command with time tag CP56Time2a, normalized value

C_SE_TA_1 := CP{Data unit identifier,Information object address,NVA,QOS,CP56Time2a}

CAUSES OF TRANSMISSION used with

TYPE IDENT 61 := C_SE_TA_1

CAUSE OF TRANSMISSION

in control direction:
<6> := activation
<8> := deactivation

in monitor direction:
<7> := activation confirmation
<9> := deactivation confirmation
<10> := activation termination (opt)
<44> := unknown type identification
<45> := unknown cause of transmission
<46> := unknown common address of ASDU
<47> := unknown information object address

8.5 TYPE IDENT 62: C_SE_TB_1
Set-point command with time tag CP56Time2a, scaled value

Single information object (SQ = 0)

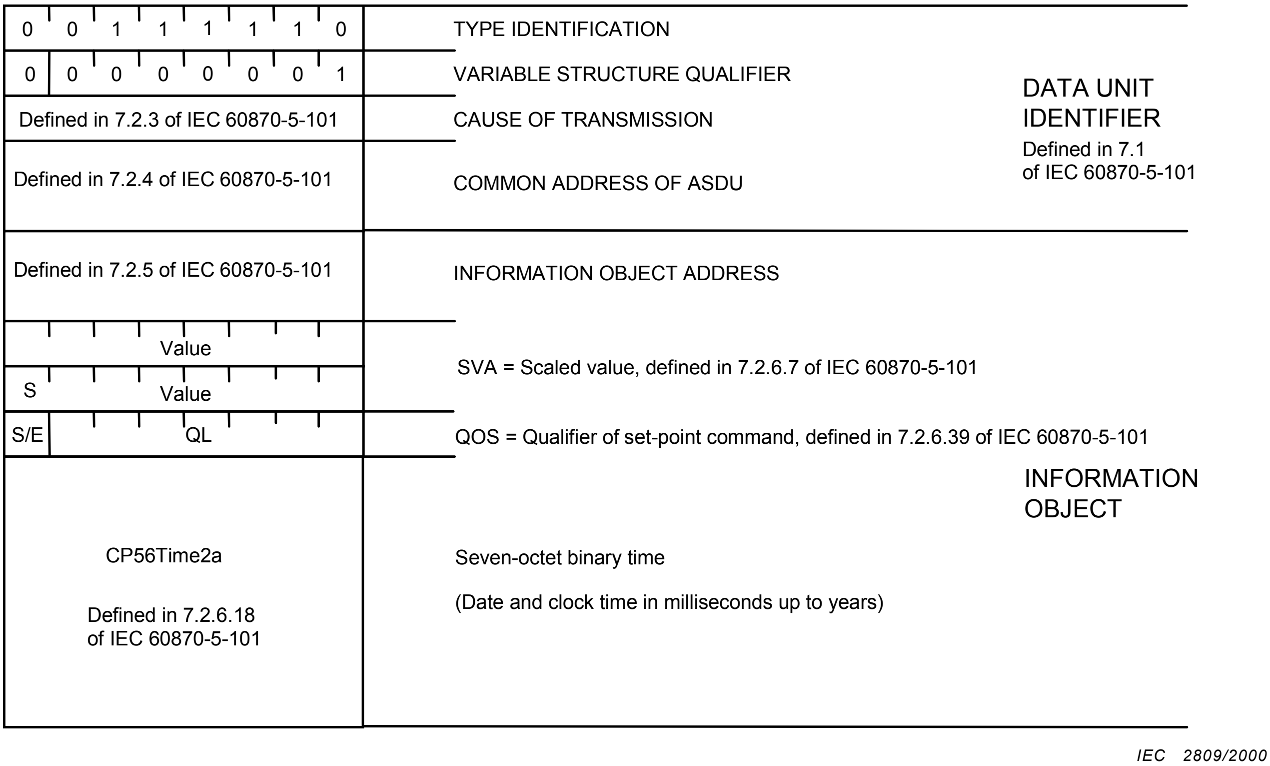


Figure 27 – ASDU: C_SE_TB_1
Set-point command with time tag CP56Time2a, scaled value

C_SE_TB_1 := CP{Data unit identifier,Information object address,SVA,QOS,CP56Time2a}

CAUSES OF TRANSMISSION used with

TYPE IDENT 62 := C_SE_TB_1

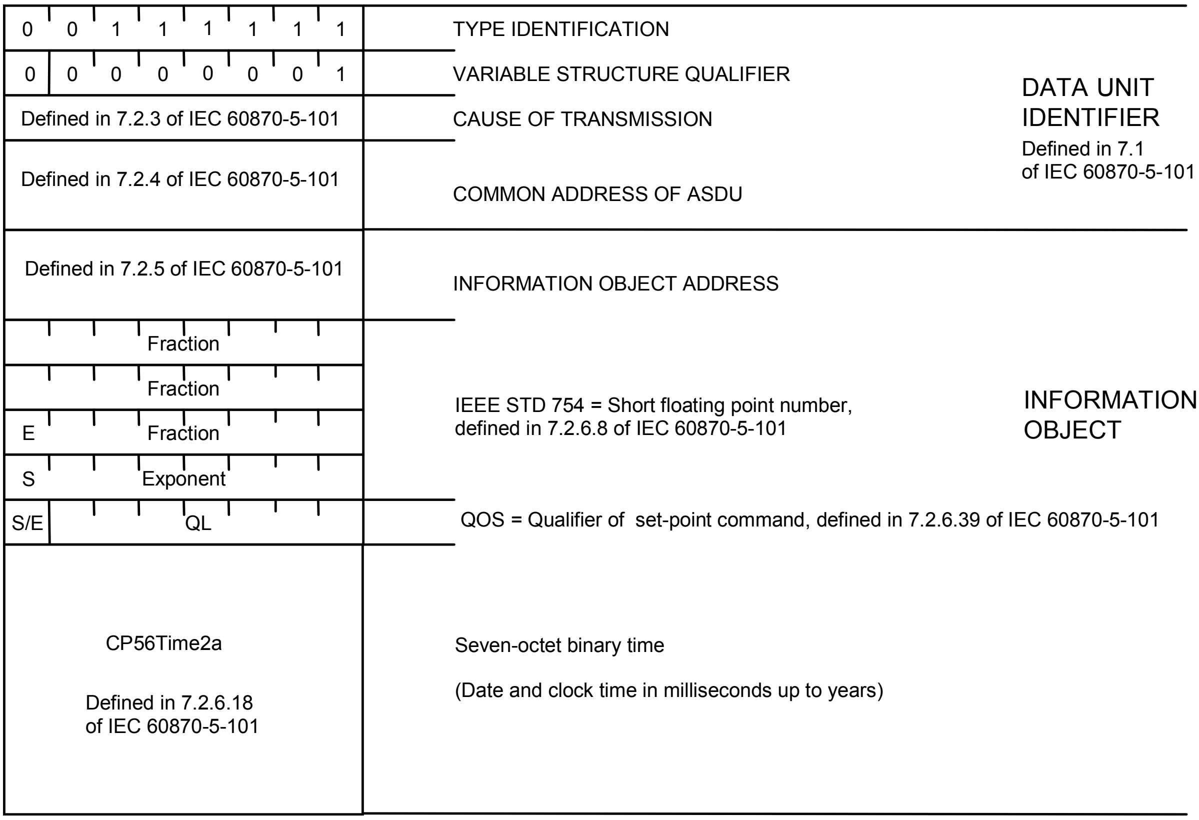
CAUSE OF TRANSMISSION

In control direction:
<6> := activation
<8> := deactivation

In monitor direction:
<7> := activation confirmation
<9> := deactivation confirmation
<10> := activation termination (opt)
<44> := unknown type identification
<45> := unknown cause of transmission
<46> := unknown common address of ASDU
<47> := unknown information object address

8.6 TYPE IDENT 63: C_SE_TC_1 Set-point command with time tag CP56Time2a, short floating point number

Single information object (SQ = 0)



IEC 2810/2000

Figure 28 – ASDU: C_SE_TC_1
Set-point command with time tag CP56Time2a, short floating point number

C_SE_TC_1 := CP{Data unit identifier,Information object address,IEEE STD 754,QOS, CP56Time2a}

CAUSES OF TRANSMISSION used with

TYPE IDENT 63 := C_SE_TC_1

CAUSE OF TRANSMISSION

In control direction:
<6> := activation
<8> := deactivation

In monitor direction:
<7> := activation confirmation
<9> := deactivation confirmation
<10> := activation termination (opt)
<44> := unknown type identification
<45> := unknown cause of transmission
<46> := unknown common address of ASDU
<47> := unknown information object address

8.7 TYPE IDENT 64: C_BO_TA_1 Bitstring of 32 bit with time tag CP56Time2a

Single information object (SQ = 0)

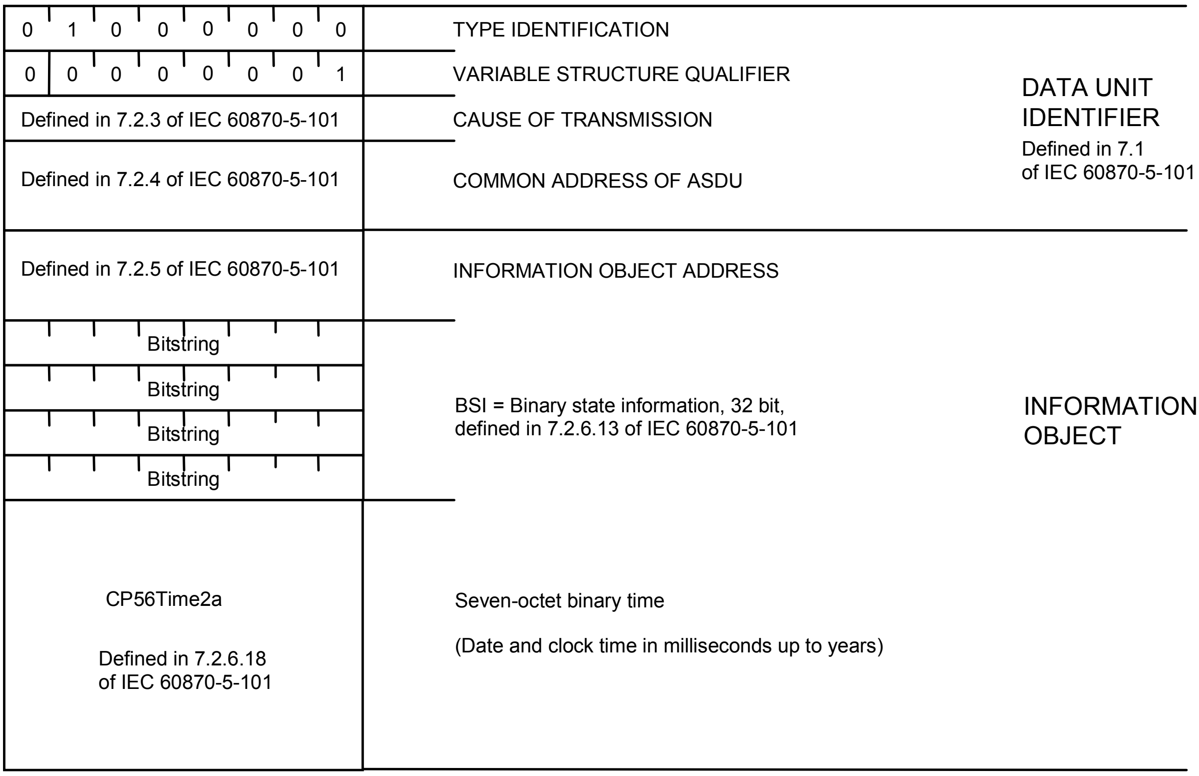


Figure 29 – ASDU: C_BO_TA_1 Bitstring of 32 bit with time tag CP56Time2a

C_BO_TA_1 := CP{Data unit identifier,Information object address,BSI,CP56Time2a}

CAUSES OF TRANSMISSION used with

TYPE IDENT 64 := C_BO_TA_1

CAUSE OF TRANSMISSION

In control direction:
<6> := activation

In monitor direction:
<7> := activation confirmation
<10> := activation termination (opt)
<44> := unknown type identification
<45> := unknown cause of transmission
<46> := unknown common address of ASDU
<47> := unknown information object address

8.8 TYPE IDENT 107: C_TS_TA_1
Test command with time tag CP56Time2a

Single information object (SQ = 0)

0 1 1 0 1 0 1 1	TYPE IDENTIFICATION	DATA UNIT IDENTIFIER Defined in 7.1 of IEC 60870-5-101
0 0 0 0 0 0 0 1	VARIABLE STRUCTURE QUALIFIER	
Defined in 7.2.3 of IEC 60870-5-101	CAUSE OF TRANSMISSION	
Defined in 7.2.4 of IEC 60870-5-101	COMMON ADDRESS OF ASDU	
Defined in 7.2.5 of IEC 60870-5-101	INFORMATION OBJECT ADDRESS	INFORMATION OBJECT
TSC	TSC = Test sequence counter, 16 bit	
CP56Time2a Defined in 7.2.6.18 of IEC 60870-5-101	Seven-octet binary time (Date and clock time in milliseconds up to years)	

IEC 2812/2000

Figure 30 – ASDU: C_TS_TA_1
Test command with time tag CP56Time2a

C_TS_TA_1 := CP{Data unit identifier,Information object address,TSC,CP56Time2a}

TSC := UI16[1..16]<0..65535>

The requesting station may choose any value of TSC. The TSC in the response shall match the request, and the time in the response shall also exactly match the time in the request.

CAUSES OF TRANSMISSION used with

TYPE IDENT 107 := C_TS_TA_1

CAUSE OF TRANSMISSION

In control direction:
<6> := activation

In monitor direction:
<7> := activation confirmation
<44> := unknown type identification
<45> := unknown cause of transmission
<46> := unknown common address of ASDU
<47> := unknown information object address

8.9 TYPE IDENT 127: F_SC_NB_1 QueryLog – Request archive file

Single information object (SQ = 0)

0 1 1 1 1 1 1 1	TYPE IDENTIFICATION	DATA UNIT IDENTIFIER Defined in 7.1 of IEC 60870-5-101
0 0 0 0 0 0 0 1	VARIABLE STRUCTURE QUALIFIER	
Defined in 7.2.3 of IEC 60870-5-101	CAUSE OF TRANSMISSION	
Defined in 7.2.4 of IEC 60870-5-101	COMMON ADDRESS OF ASDU	
Defined in 7.2.5 of IEC 60870-5-101	INFORMATION OBJECT ADDRESS	INFORMATION OBJECT
Defined in 7.2.6.33 of IEC 60870-5-101	Name of file	
CP56Time2a Defined in 7.2.6.18 of IEC 60870-5-101	Seven octet binary time (RangeStartTime)	
CP56Time2a Defined in 7.2.6.18 of IEC 60870-5-101	Seven octet binary time (RangeStopTime)	

IEC 939/06

Figure 31 – ASDU: F_SC_NB_1 QueryLog – Request archive file

CAUSES OF TRANSMISSION used with

TYPE IDENT 127

CAUSE OF TRANSMISSION

<13> := file transfer
<44> := unknown type of file
<45> := unknown cause of transmission
<46> := unknown common address of ASDU
<47> := unknown information object address

Depending on the values of the two time stamps, a part of, or the complete file (which represents the log) shall be transmitted:

RangeStartTime	RangeStopTime	Resulting file transfer
Available	Available	All records having a timestamp between RangeStartTime and RangeStopTime [a)]
0 (all zeros)	Available	All records having a timestamp from the beginning to RangeStopTime [a)]
Available	0 (all zeros)	All records having a timestamp between RangeStartTime and the end [a)]
0 (all zeros)	0 (all zeros)	All records
[a)] Including the records with timestamp RangeStartTime or RangeStopTime respectively.		

NOTE A record is assumed to have a timestamp. The timestamp is assumed to be implicit.

The file transfer (defined in IEC 60870-5-101:2003, 7.4.11) shall start after a successful query request has been received by the controlled station. The query request pre-selects the content of the file to be transmitted in the subsequent call sections.

9 Interoperability

This companion standard presents sets of parameters and alternatives from which subsets must be selected to implement particular telecontrol systems. Certain parameter values, such as the choice of "structured" or "unstructured" fields of the INFORMATION OBJECT ADDRESS of ASDUs represent mutually exclusive alternatives. This means that only one value of the defined parameters is admitted per system. Other parameters, such as the listed set of different process information in command and in monitor direction allow the specification of the complete set or subsets, as appropriate for given applications. This clause summarizes the parameters of the previous clauses to facilitate a suitable selection for a specific application. If a system is composed of equipment stemming from different manufacturers, it is necessary that all partners agree on the selected parameters.

The interoperability list is defined as in IEC 60870-5-101 and extended with parameters used in this standard. The text descriptions of parameters which are not applicable to this companion standard are strike-through (corresponding check box is marked black).

NOTE In addition, the full specification of a system may require individual selection of certain parameters for certain parts of the system, such as the individual selection of scaling factors for individually addressable measured values.

The selected parameters should be marked in the white boxes as follows:

☐ Function or ASDU is not used

☒ X Function or ASDU is used as standardized (default)

R Function or ASDU is used in reverse mode

B Function or ASDU is used in standard and reverse mode

The possible selection (blank, X, R, or B) is specified for each specific clause or parameter.

A black check box indicates that the option cannot be selected in this companion standard.

9.1 System or device

(system-specific parameter, indicate definition of a system or a device by marking one of the following with "**X**")

☐ System definition

☐ Controlling station definition (Master)

☐ Controlled station definition (Slave)

9.2 Network configuration

(network-specific parameter, all configurations that are used are to be marked "**X**")

■ ~~Point-to-point~~ ■ ~~Multipoint-~~

■ ~~Multiple point-to-point~~ ■ ~~Multipoint-star~~

9.3 Physical layer

(network-specific parameter, all interfaces and data rates that are used are to be marked "**X**")

<u>Transmission speed (control direction)</u>

Unbalanced interchange Circuit V.24/V.28 Standard	Unbalanced interchange Circuit V.24/V.28 Recommended if >1 200 bit/s	Balanced interchange Circuit X.24/X.27	
[redacted] ~~100 bit/s~~	[redacted] ~~2 400 bit/s~~	[redacted] ~~2 400 bit/s~~	[redacted] ~~56 000 bit/s~~
[redacted] ~~200 bit/s~~	[redacted] ~~4 800 bit/s~~	[redacted] ~~4 800 bit/s~~	[redacted] ~~64 000 bit/s~~
[redacted] ~~300 bit/s~~	[redacted] ~~9 600 bit/s~~	[redacted] ~~9 600 bit/s~~	
[redacted] ~~600 bit/s~~		[redacted] ~~19 200 bit/s~~	
[redacted] ~~1 200 bit/s~~		[redacted] ~~38 400 bit/s~~	

<u>Transmission speed (monitor direction)</u>

Unbalanced interchange Circuit V.24/V.28 Standard	Unbalanced interchange Circuit V.24/V.28 Recommended if >1 200 bit/s	Balanced interchange Circuit X.24/X.27	
[redacted] ~~100 bit/s~~	[redacted] ~~2 400 bit/s~~	[redacted] ~~2 400 bit/s~~	[redacted] ~~56 000 bit/s~~
[redacted] ~~200 bit/s~~	[redacted] ~~4 800 bit/s~~	[redacted] ~~4 800 bit/s~~	[redacted] ~~64 000 bit/s~~
[redacted] ~~300 bit/s~~	[redacted] ~~9 600 bit/s~~	[redacted] ~~9 600 bit/s~~	
[redacted] ~~600 bit/s~~		[redacted] ~~19 200 bit/s~~	
[redacted] ~~1 200 bit/s~~		[redacted] ~~38 400 bit/s~~	

9.4 Link layer

(network-specific parameter, all options that are used are to be marked "X". Specify the maximum frame length. If a non-standard assignment of class 2 messages is implemented for unbalanced transmission, indicate the Type ID and COT of all messages assigned to class 2.)

~~Frame format FT 1.2, single character 1 and the fixed time out interval are used exclusively in this companion standard.~~

<u>Link transmission</u>

[redacted] ~~Balanced transmission~~

[redacted] ~~Unbalanced transmission~~

<u>Frame length</u>

[redacted] ~~Maximum length L (number of octets)~~

<u>Address field of the link</u>

[redacted] ~~not present (balanced transmission only)~~

[redacted] ~~One octet~~

[redacted] ~~Two octets~~

[redacted] ~~Structured~~

[redacted] ~~Unstructured~~

When using an unbalanced link layer, the following ASDU types are returned in class 2 messages (low priority) with the indicated causes of transmission:

■ ~~The standard assignment of ASDUs to class 2 messages is used as follows:~~

Type identification	Cause of transmission
9, 11, 13, 21	<1>

■ ~~A special assignment of ASDUs to class 2 messages is used as follows:~~

Type identification	Cause of transmission

~~Note: (In response to a class 2 poll, a controlled station may respond with class 1 data when there is no class 2 data available).~~

9.5 Application layer

Transmission mode for application data

Mode 1 (Least significant octet first), as defined in 4.10 of IEC 60870-5-4, is used exclusively in this companion standard.

Common address of ASDU
(system-specific parameter, all configurations that are used are to be marked "**X**")

■ ~~One octet~~ ☒ Two octets

Information object address
(system-specific parameter, all configurations that are used are to be marked "**X**")

■ ~~One octet~~ ☐ Structured
■ ~~Two octets~~ ☐ Unstructured
☒ Three octets

Cause of transmission
(system-specific parameter, all configurations that are used are to be marked "**X**")

■ ~~One octet~~ ☒ Two octets (with originator address). Originator address is set to zero if not used

Length of APDU
(system-specific parameter, specify the maximum length of the APDU per system)

The maximum length of APDU for both directions is 253. It is a fixed system parameter.

[redacted] Maximum length of APDU per system in control direction
[redacted] Maximum length of APDU per system in monitor direction

Selection of standard ASDUs

Process information in monitor direction
(station-specific parameter, mark each Type ID "**X**" if it is only used in the standard direction, "**R**" if only used in the reverse direction, and "**B**" if used in both directions).

☐	<1> :=	Single-point information	M_SP_NA_1
■	~~<2> :=~~	~~Single-point information with time tag~~	~~M_SP_TA_1~~
☐	<3> :=	Double-point information	M_DP_NA_1
■	~~<4> :=~~	~~Double-point information with time tag~~	~~M_DP_TA_1~~
☐	<5> :=	Step position information	M_ST_NA_1
■	~~<6> :=~~	~~Step position information with time tag~~	~~M_ST_TA_1~~
☐	<7> :=	Bitstring of 32 bit	M_BO_NA_1
■	~~<8> :=~~	~~Bitstring of 32 bit with time tag~~	~~M_BO_TA_1~~
☐	<9> :=	Measured value, normalized value	M_ME_NA_1
■	~~<10> :=~~	~~Measured value, normalized value with time tag~~	~~M_ME_TA_1~~
☐	<11> :=	Measured value, scaled value	M_ME_NB_1
■	~~<12> :=~~	~~Measured value, scaled value with time tag~~	~~M_ME_TB_1~~
☐	<13> :=	Measured value, short floating point value	M_ME_NC_1
■	~~<14> :=~~	~~Measured value, short floating point value with time tag~~	~~M_ME_TC_1~~
☐	<15> :=	Integrated totals	M_IT_NA_1
■	~~<16> :=~~	~~Integrated totals with time tag~~	~~M_IT_TA_1~~
■	~~<17> :=~~	~~Event of protection equipment with time tag~~	~~M_EP_TA_1~~
■	~~<18> :=~~	~~Packed start events of protection equipment with time tag~~	~~M_EP_TB_1~~
■	~~<19> :=~~	~~Packed output circuit information of protection equipment with time tag~~	~~M_EP_TC_1~~
☐	<20> :=	Packed single-point information with status change detection	M_SP_NA_1
☐	<21> :=	Measured value, normalized value without quality descriptor	M_ME_ND_1
☐	<30> :=	Single-point information with time tag CP56Time2a	M_SP_TB_1
☐	<31> :=	Double-point information with time tag CP56Time2a	M_DP_TB_1
☐	<32> :=	Step position information with time tag CP56Time2a	M_ST_TB_1
☐	<33> :=	Bitstring of 32 bit with time tag CP56Time2a	M_BO_TB_1
☐	<34> :=	Measured value, normalized value with time tag CP56Time2a	M_ME_TD_1
☐	<35> :=	Measured value, scaled value with time tag CP56Time2a	M_ME_TE_1
☐	<36> :=	Measured value, short floating point value with time tag CP56Time2a	M_ME_TF_1
☐	<37> :=	Integrated totals with time tag CP56Time2a	M_IT_TB_1
☐	<38> :=	Event of protection equipment with time tag CP56Time2a	M_EP_TD_1
☐	<39> :=	Packed start events of protection equipment with time tag CP56Time2a	M_EP_TE_1
☐	<40> :=	Packed output circuit information of protection equipment with time tag CP56Time2a	M_EP_TF_1

In this companion standard only the use of the set <30> – <40> for ASDUs with time tag is permitted.

Process information in control direction
(station-specific parameter, mark each Type ID "**X**" if it is only used in the standard direction, "**R**" if only used in the reverse direction, and "**B**" if used in both directions).

☐	<45> :=	Single command	C_SC_NA_1
☐	<46> :=	Double command	C_DC_NA_1
☐	<47> :=	Regulating step command	C_RC_NA_1
☐	<48> :=	Set point command, normalized value	C_SE_NA_1
☐	<49> :=	Set point command, scaled value	C_SE_NB_1
☐	<50> :=	Set point command, short floating point value	C_SE_NC_1
☐	<51> :=	Bitstring of 32 bit	C_BO_NA_1
☐	<58> :=	Single command with time tag CP56Time2a	C_SC_TA_1
☐	<59> :=	Double command with time tag CP56Time2a	C_DC_TA_1
☐	<60> :=	Regulating step command with time tag CP56Time2a	C_RC_TA_1
☐	<61> :=	Set point command, normalized value with time tag CP56Time2a	C_SE_TA_1
☐	<62> :=	Set point command, scaled value with time tag CP56Time2a	C_SE_TB_1
☐	<63> :=	Set point command, short floating point value with time tag CP56Time2a	C_SE_TC_1
☐	<64> :=	Bitstring of 32 bit with time tag CP56Time2a	C_BO_TA_1

Either the ASDUs of the set <45> – <51> or of the set <58> – <64> are used.

System information in monitor direction
(station-specific parameter, mark with an “**X**” if it is only used in the standard direction, “**R**” if only used in the reverse direction, and “**B**” if used in both directions).

☐	<70> :=	End of initialization	M_EI_NA_1

System information in control direction
(station-specific parameter, mark each Type ID "**X**" if it is only used in the standard direction, "**R**" if only used in the reverse direction, and "**B**" if used in both directions).

☐	<100>:=	Interrogation command	C_IC_NA_1
☐	<101>:=	Counter interrogation command	C_CI_NA_1
☐	<102>:=	Read command	C_RD_NA_1
☐	<103>:=	Clock synchronization command (option see 7.6)	C_CS_NA_1
■	~~<104>:=~~	~~Test command~~	~~C_TS_NA_1~~
☐	<105>:=	Reset process command	C_RP_NA_1
■	~~<106>:=~~	~~Delay acquisition command~~	~~C_CD_NA_1~~
☐	<107>:=	Test command with time tag CP56Time2a	C_TS_TA_1

Parameter in control direction
(station-specific parameter, mark each Type ID "**X**" if it is only used in the standard direction, "**R**" if only used in the reverse direction, and "**B**" if used in both directions).

☐ <110>:= Parameter of measured value, normalized value P_ME_NA_1

☐ <111>:= Parameter of measured value, scaled value P_ME_NB_1

☐ <112>:= Parameter of measured value, short floating point value P_ME_NC_1

☐ <113>:= Parameter activation P_AC_NA_1

File transfer
(station-specific parameter, mark each Type ID "**X**" if it is only used in the standard direction, "**R**" if only used in the reverse direction, and "**B**" if used in both directions).

☐ <120>:= File ready F_FR_NA_1

☐ <121>:= Section ready F_SR_NA_1

☐ <122>:= Call directory, select file, call file, call section F_SC_NA_1

☐ <123>:= Last section, last segment F_LS_NA_1

☐ <124>:= Ack file, ack section F_AF_NA_1

☐ <125>:= Segment F_SG_NA_1

☐ <126>:= Directory {blank or X, only available in monitor (standard) direction} F_DR_TA_1

☐ <127>:= Query Log – Request archive file F_SC_NB_1

Type identifier and cause of transmission assignments
(station-specific parameters)

Shaded boxes: option not required.

Black boxes: option not permitted in this companion standard

Blank: functions or ASDU not used.

Mark Type Identification/Cause of transmission combinations:

"**X**" if only used in the standard direction;

"**R**" if only used in the reverse direction;

"**B**" if used in both directions.

Type identification		Cause of transmission																		
		1	2	3	4	5	6	7	8	9	10	11	12	13	20 to 36	37 to 41	44	45	46	47
<1>	M_SP_NA_1																			
~~<2>~~	~~M_SP_TA_1~~																			
<3>	M_DP_NA_1																			
~~<4>~~	~~M_DP_TA_1~~																			
<5>	M_ST_NA_1																			
~~<6>~~	~~M_ST_TA_1~~																			
<7>	M_BO_NA_1																			
~~<8>~~	~~M_BO_TA_1~~																			
<9>	M_ME_NA_1																			
~~<10>~~	~~M_ME_TA_1~~																			
<11>	M_ME_NB_1																			
~~<12>~~	~~M_ME_TB_1~~																			

Type identification		Cause of transmission																		
		1	2	3	4	5	6	7	8	9	10	11	12	13	20 to 36	37 to 41	44	45	46	47
<13>	M_ME_NC_1																			
~~<14>~~	~~M_ME_TC_1~~																			
<15>	M_IT_NA_1																			
~~<16>~~	~~M_IT_TA_1~~																			
~~<17>~~	~~M_EP_TA_1~~																			
~~<18>~~	~~M_EP_TB_1~~																			
~~<19>~~	~~M_EP_TC_1~~																			
<20>	M_PS_NA_1																			
<21>	M_ME_ND_1																			
<30>	M_SP_TB_1																			
<31>	M_DP_TB_1																			
<32>	M_ST_TB_1																			
<33>	M_BO_TB_1																			
<34>	M_ME_TD_1																			
<35>	M_ME_TE_1																			
<36>	M_ME_TF_1																			
<37>	M_IT_TB_1																			
<38>	M_EP_TD_1																			
<39>	M_EP_TE_1																			
<40>	M_EP_TF_1																			
<45>	C_SC_NA_1																			
<46>	C_DC_NA_1																			
<47>	C_RC_NA_1																			
<48>	C_SE_NA_1																			
<49>	C_SE_NB_1																			
<50>	C_SE_NC_1																			
<51>	C_BO_NA_1																			
<58>	C_SC_TA_1																			
<59>	C_DC_TA_1																			
<60>	C_RC_TA_1																			
<61>	C_SE_TA_1																			
<62>	C_SE_TB_1																			
<63>	C_SE_TC_1																			
<64>	C_BO_TA_1																			
<70>	M_EI_NA_1*																			
<100>	C_IC_NA_1																			
<101>	C_CI_NA_1																			
<102>	C_RD_NA_1																			
<103>	C_CS_NA_1																			
~~<104>~~	~~C_TS_NA_1~~																			
<105>	C_RP_NA_1																			
~~<106>~~	~~C_CD_NA_1~~																			
<107>	C_TS_TA_1																			
<110>	P_ME_NA_1																			
<111>	P_ME_NB_1																			
<112>	P_ME_NC_1																			
<113>	P_AC_NA_1																			
<120>	F_FR_NA_1																			
<121>	F_SR_NA_1																			
<122>	F_SC_NA_1																			
<123>	F_LS_NA_1																			
<124>	F_AF_NA_1																			
<125>	F_SG_NA_1																			
<126>	F_DR_TA_1*																			
<127>	F_SC_NB_1*																			

* Blank or X only

9.6 Basic application functions

Station initialization
(station-specific parameter, mark "**X**" if function is used)

☐ Remote initialization

Cyclic data transmission
(station-specific parameter, mark "**X**" if function is only used in the standard direction, "**R**" if only used in the reverse direction, and "**B**" if used in both directions)

☐ Cyclic data transmission

Read procedure
(station-specific parameter, mark "**X**" if function is only used in the standard direction, "**R**" if only used in the reverse direction, and "**B**" if used in both directions)

☐ Read procedure

Spontaneous transmission
(station-specific parameter, mark "**X**" if function is only used in the standard direction, "**R**" if only used in the reverse direction, and "**B**" if used in both directions)

☐ Spontaneous transmission

Double transmission of information objects with cause of transmission spontaneous
(station-specific parameter, mark each information type "**X**" where both a Type ID without time and corresponding Type ID with time are issued in response to a single spontaneous change of a monitored object)

The following type identifications may be transmitted in succession caused by a single status change of an information object. The particular information object addresses for which double transmission is enabled are defined in a project-specific list.

☐ Single-point information M_SP_NA_1, M_SP_TA_1, M_SP_TB_1 and M_PS_NA_1
☐ Double-point information M_DP_NA_1, M_DP_TA_1 and M_DP_TB_1
☐ Step position information M_ST_NA_1, M_ST_TA_1 and M_ST_TB_1
☐ Bitstring of 32 bit M_BO_NA_1, M_BO_TA_1 and M_BO_TB_1 (if defined for a specific project)
☐ Measured value, normalized value M_ME_NA_1, M_ME_TA_1, M_ME_ND_1 and M_ME_TD_1
☐ Measured value, scaled value M_ME_NB_1, M_ME_TB_1 and M_ME_TE_1
☐ Measured value, short floating point number M_ME_NC_1, M_ME_TC_1 and M_ME_TF_1

Station interrogation
(station-specific parameter, mark "**X**" if function is only used in the standard direction, "**R**" if only used in the reverse direction, and "**B**" if used in both directions).

☐ global
☐ group 1
☐ group 2
☐ group 3
☐ group 4
☐ group 5
☐ group 6
☐ group 7
☐ group 8
☐ group 9
☐ group 10
☐ group 11
☐ group 12
☐ group 13
☐ group 14
☐ group 15
☐ group 16

Information object addresses assigned to each group must be shown in a separate table.

Clock synchronization
(station-specific parameter, mark "**X**" if function is only used in the standard direction, "**R**" if only used in the reverse direction, and "**B**" if used in both directions).

☐ Clock synchronization

☐ Day of week used

☐ RES1, GEN (time tag substituted/ not substituted) used

☐ SU-bit (summertime) used

optional, see 7.6

Command transmission
(object-specific parameter, mark "**X**" if function is only used in the standard direction, "**R**" if only used in the reverse direction, and "**B**" if used in both directions).

☐ Direct command transmission
☐ Direct set point command transmission
☐ Select and execute command
☐ Select and execute set point command
☐ C_SE ACTTERM used

☐ No additional definition
☐ Short-pulse duration (duration determined by a system parameter in the outstation)
☐ Long-pulse duration (duration determined by a system parameter in the outstation)
☐ Persistent output

☐ Supervision of maximum delay in command direction of commands and set point commands

☐ Maximum allowable delay of commands and set point commands

Transmission of integrated totals
(station- or object-specific parameter, mark "**X**" if function is only used in the standard direction, "**R**" if only used in the reverse direction, and "**B**" if used in both directions).

☐ Mode A: Local freeze with spontaneous transmission
☐ Mode B: Local freeze with counter interrogation
☐ Mode C: Freeze and transmit by counter-interrogation commands
☐ Mode D: Freeze by counter-interrogation command, frozen values reported

☐ Counter read
☐ Counter freeze without reset
☐ Counter freeze with reset
☐ Counter reset

☐ General request
☐ Request counter group 1
☐ Request counter group
☐ Request counter group 3
☐ Request counter group 4

Parameter loading
(object-specific parameter, mark "**X**" if function is only used in the standard direction, "**R**" if only used in the reverse direction, and "**B**" if used in both directions).

☐ Threshold value
☐ Smoothing factor
☐ Low limit for transmission of measured values
☐ High limit for transmission of measured values

Parameter activation
(object-specific parameter, mark "**X**" if function is only used in the standard direction, "**R**" if only used in the reverse direction, and "**B**" if used in both directions).

☐ Act/deact of persistent cyclic or periodic transmission of the addressed object

Test procedure
(station-specific parameter, mark "**X**" if function is only used in the standard direction, "**R**" if only used in the reverse direction, and "**B**" if used in both directions).

☐ Test procedure

File transfer
(station-specific parameter, mark "**X**" if function is used).

File transfer in monitor direction

☐ Transparent file
☐ Transmission of disturbance data of protection equipment
☐ Transmission of sequences of events
☐ Transmission of sequences of recorded analogue values

File transfer in control direction

☐ Transparent file

Background scan
(station-specific parameter, mark "**X**" if function is only used in the standard direction, "**R**" if only used in the reverse direction, and "**B**" if used in both directions).

☐ Background scan

Acquisition of transmission delay
(station-specific parameter, mark "**X**" if function is only used in the standard direction, "**R**" if only used in the reverse direction, and "**B**" if used in both directions).

■ ~~Acquisition of transmission delay~~

Definition of time outs

Parameter	Default value	Remarks	Selected value
t_0	30 s	Time-out of connection establishment	
t_1	15 s	Time-out of send or test APDUs	
t_2	10 s	Time-out for acknowledges in case of no data messages $t_2 < t_1$	
t_3	20 s	Time-out for sending test frames in case of a long idle state	

Maximum range for timeouts t_0 to t_2: 1 s to 255 s, accuracy 1 s.
Recommended range for timeout t_3: 1 s to 48 h, resolution 1 s.
Long timeouts for t_3 may be needed in special cases where satellite links or dialup connections are used (for instance to establish connection and collect values only once per day or week).

Maximum number of outstanding I format APDUs *k* and latest acknowledge APDUs (*w*)

Parameter	Default value	Remarks	Selected value
k	12 APDUs	Maximum difference receive sequence number to send state variable	
w	8 APDUs	Latest acknowledge after receiving *w* I format APDUs	

Maximum range of values *k*: 1 to 32767 (2^{15}–1) APDUs, accuracy 1 APDU

Maximum range of values w: 1 to 32767 APDUs, accuracy 1 APDU (Recommendation: w should not exceed two-thirds of k).

Portnumber

Parameter	Value	Remarks
Portnumber	2404	In all cases

Redundant connections

☐ Number N of redundancy group connections used

RFC 2200 suite

RFC 2200 is an official Internet Standard which describes the state of standardization of protocols used in the Internet as determined by the Internet Architecture Board (IAB). It offers a broad spectrum of actual standards used in the Internet. The suitable selection of documents from RFC 2200 defined in this standard for given projects has to be chosen by the user of this standard.

☐ Ethernet 802.3

☐ Serial X.21 interface

☐ Other selection from RFC 2200:

List of valid documents from RFC 2200

1. ....
2. ....
3. ....
4. ....
5. ....
6. ....
7. etc.

10 Redundant connections

10.1 General

This companion standard defines network access for IEC 60870-5-101 using the well known TCP/IP transport profile, and mainly focuses on the use of a single TCP connection.

In many cases, however, redundancy is required to increase the availability of the communication system. In these cases, multiple redundant connections should be established between the two stations. This clause describes the interoperability issues that arise when standby connections are used as redundant connections.

10.2 General requirements

Redundant communication in a system using IEC 60870-5-104 can be achieved by providing the possibility to establish more than one logical connection between two stations. A logical connection is defined by a unique combination of two IP-addresses and two port-numbers, namely controlling station IP-address/port-number pair and controlled station IP-address/port-number pair.

Connection establishment is performed by the controlling station in the case of a controlled station as a partner, or by a fixed selection (parameter) in case of two equivalent controlling stations or partners, as stated in 7.1. The station that performs the connection establishment is in either case referred to as the controlling station (station A) in the subsequent description, while the partner station is referred to as the controlled station (station B).

The following general rules apply to this clause concerning redundant connections:

1) The controlling and controlled station shall be able to handle multiple (N) logical connections.
2) The N logical connections represent one redundancy group.
3) Only one logical connection is in the started state and sending/receiving user data at a time for one redundancy group.
4) The controlling station decides which one of the N connections is be in started state.
5) All logical connections of a redundancy group shall be supervised by test frames as described in 5.2.
6) A redundancy group shall rely upon only one process image (database/event buffer).
7) If more than one controlling station need to access the same controlled station simultaneously, each controlling station must be assigned to a different redundancy group (process image).

The logical connection which is enabled for user data transfer (started) at any time is defined to be the started connection, while the others are stopped connections. Selection of started connection is performed by means of the unnumbered control functions (U-frames) STARTDT/STOPDT as in 5.3 and according to the State transition diagrams in Figure 36 and Figure 37.

As stated in rule 4 above, the selection and switchover of the started connection is always initiated by the controlling station, and is managed by the transport interface or higher layers. Selection of the started connection after station initialisation is performed by transmitting a STARTDT_ACT on the desired connection. Similarly, connection switchover in the case of a failure (connection failover) is performed by transmitting a STARTDT_ACT on the stopped connection that is selected to take over.

The controlled station (station B) always understands the connection on which it last received a STARTDT_ACT as the started connection. It confirms the activation request by issuing a STARTDT_CON. The whole activation procedure is completed when the STARTDT_CON is received in the controlling station.

Manual connection switchover can be performed by first issuing a STOPDT_ACT on the currently started connection and then a STARTDT_ACT on the selected new started connection. This will gracefully terminate data transfer on the first connection before it is resumed on the new connection.

The controlling and/or controlled station shall regularly check the status of all established connections to detect any communication problems as soon as possible. This is done by sending TESTFR frames as described in 5.2.

Send and receive counters on each connection within a redundancy group continue their functionality independently of the use of STARTDT/STOPDT.

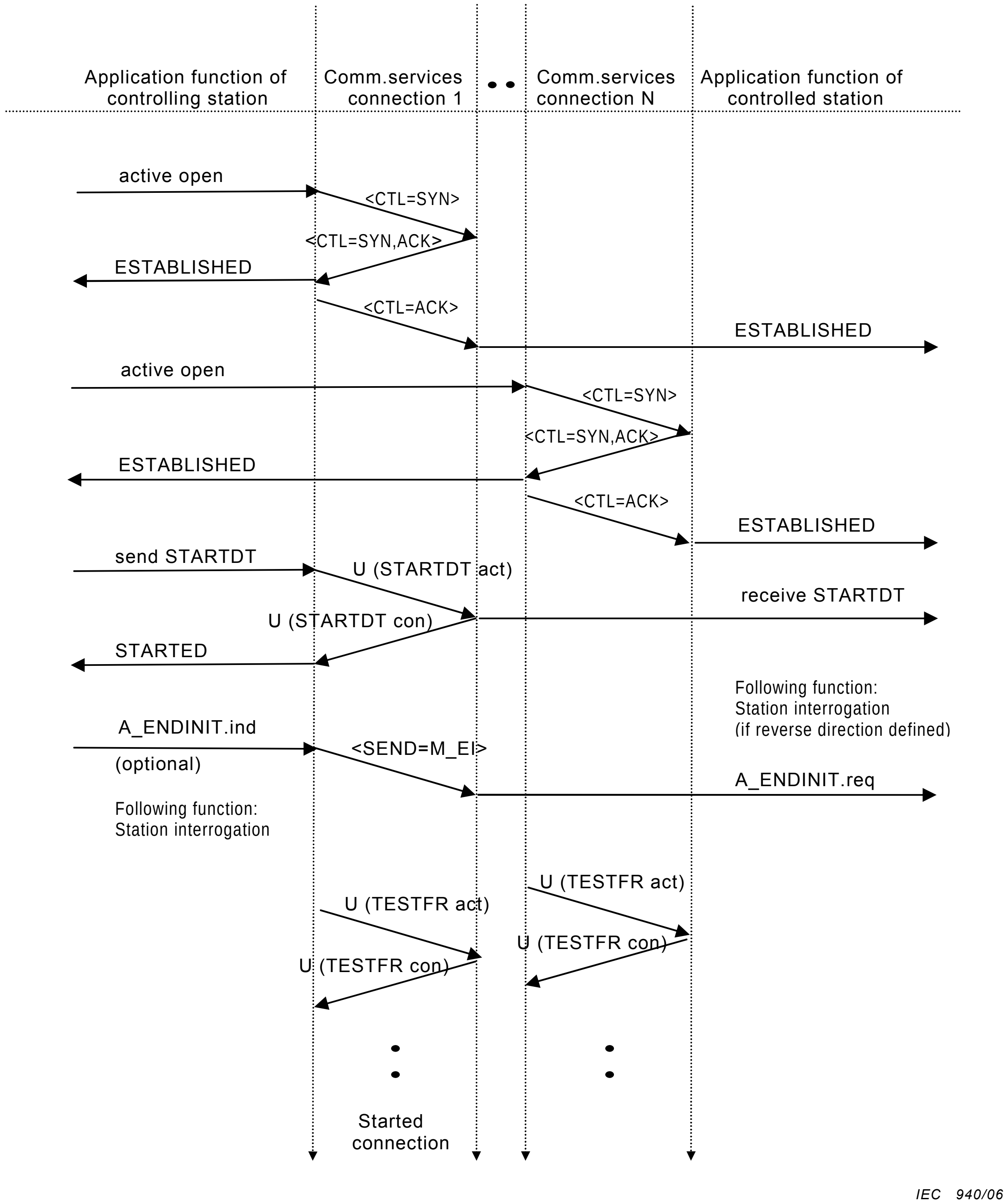
10.3 Initialisation of controlling station

The sequential procedure for initialisation of the controlling station with N redundant connections is shown in Figure 32.

After connection establishment, the stopped state is always default, and one of the connections (e.g. connection 1) is therefore changed from the stopped into the started state to enable user data transfer on this connection.

The ENDINIT.req (optional but recommended, Figures 32 and 33) may always be useful to advise the other station that the sending station is now ready to respond to an interrogation request. In case of initialisation of the controlling station, it is only issued if data in the reverse direction is defined.

The controlling station shall initiate a station interrogation procedure as soon as possible after the completion of making one of the connections in started state as shown in Figures 32 and 33.



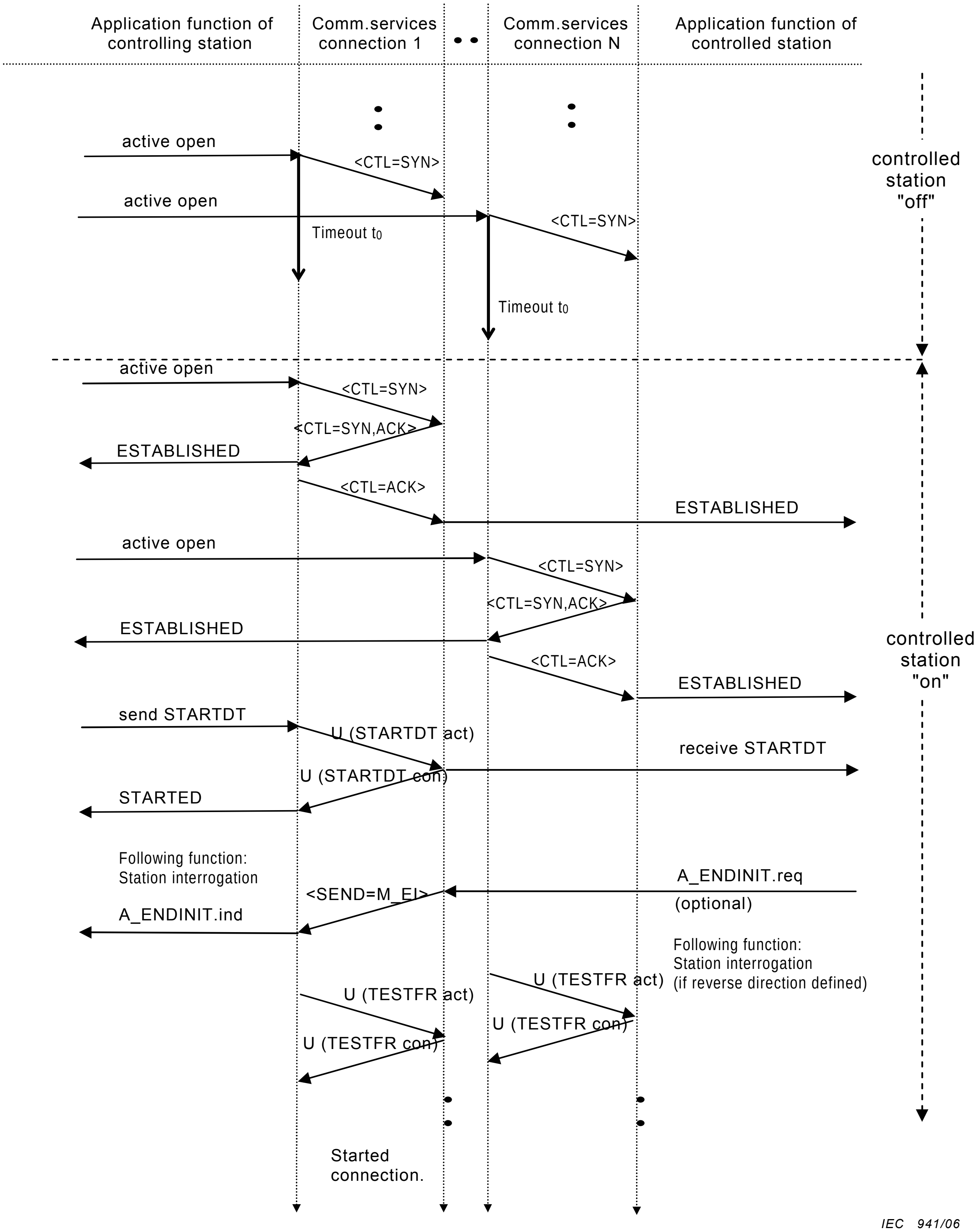
NOTE The sequential interrelationship between the procedures on the connections is not fixed. For example, establishment of the connections may be started and go on in parallel.

Figure 32 – Initialisation of controlling station with redundant connections

10.4 Initialisation of controlled station

The sequential procedure for initialisation of the controlled station with N redundant connections within a single redundancy group is shown in Figure 33.

After restart of the controlled station, the connections are established according to 7.1, but no user data is transmitted from the controlled station until started state on one connection is established.



NOTE The sequential interrelationship between the procedures on the connections is not fixed. For example, establishment of the connections may be started and go on in parallel.

Figure 33 – Initialisation of controlled station with redundant connections

10.5 User data from controlling station

If communication fails on the currently started connection (e.g. connection m) when the controlling station attempts to transmit user data (e.g. a command ASDU), a connection switchover will be performed (preferably automatic). The sequential procedure in this case is shown in Figure 34. It is up to the controlling station to select a new started connection.

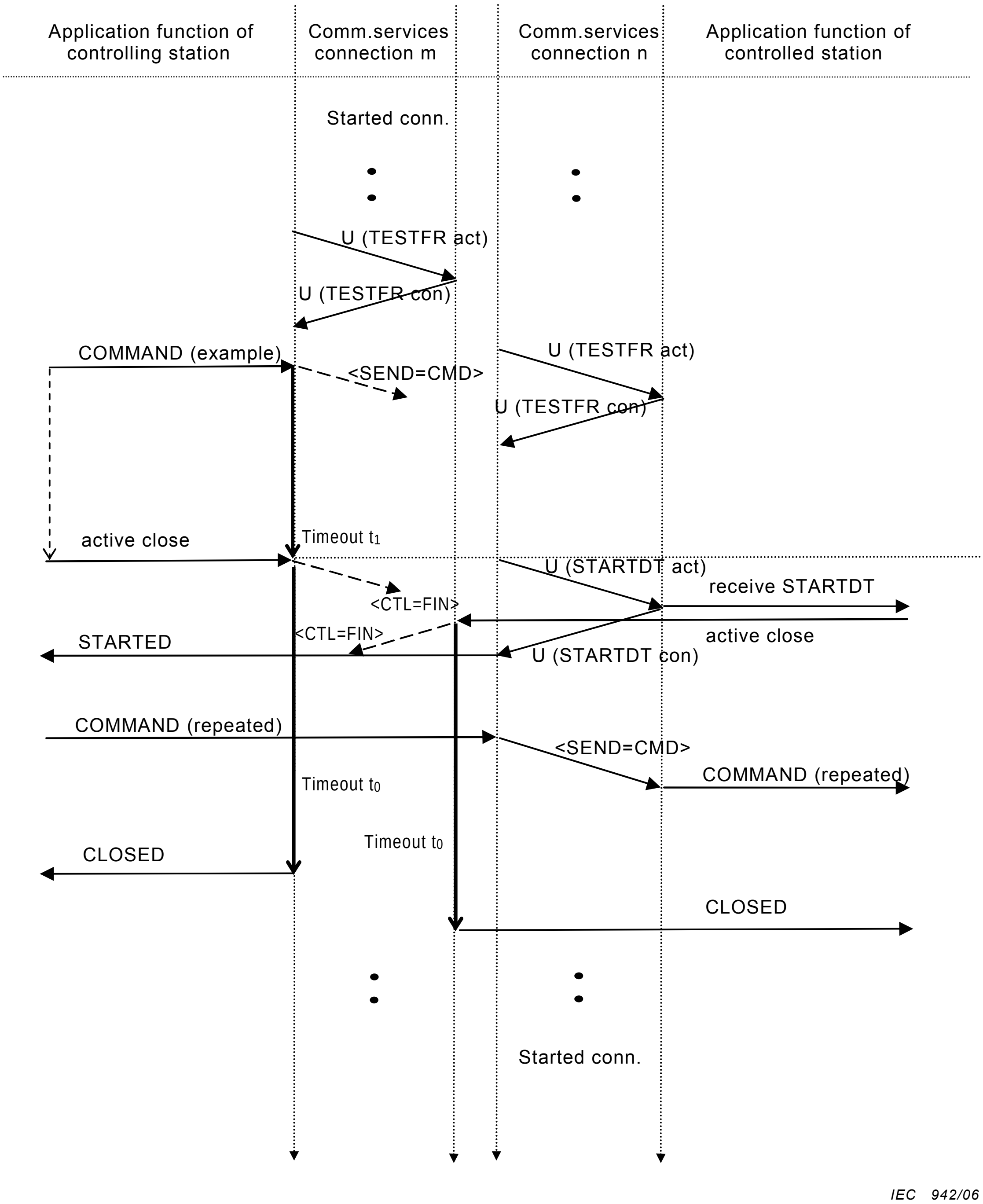
When transmission timeout (t_1) has elapsed, one of the stopped connections (connection n) is started using the STARTDT function, The command is then directed to the new started connection, either by re-transmitting the ASDU on this connection or by terminating the ongoing application function and reinitiating it towards the new connection (it is left to the application if the ESDU is retransmitted). The failed connection is eventually closed by both sides, and reopening is regularly retried by the controlling station until the error has been corrected and the connection is re-established.

Any subsequent user data (e.g. events) are now transmitted on the new started connection.

A connection switchover will also be performed whenever a TESTFR_ACT on the started connection fails and hence reports a communication error on this connection.

Care shall be taken that data are not lost during a connection switchover, for example by doing a station interrogation procedure after a switchover has been performed.

The controlled station shall only acknowledge user data received on the connection on which it last received a STARTDT_ACT (the started connection).



NOTE The sequential interrelationship between the procedures on the two connections is not fixed, except when connection switch occurs.

Figure 34 – Redundant connections – User data from controlling station

10.6 User data from controlled station

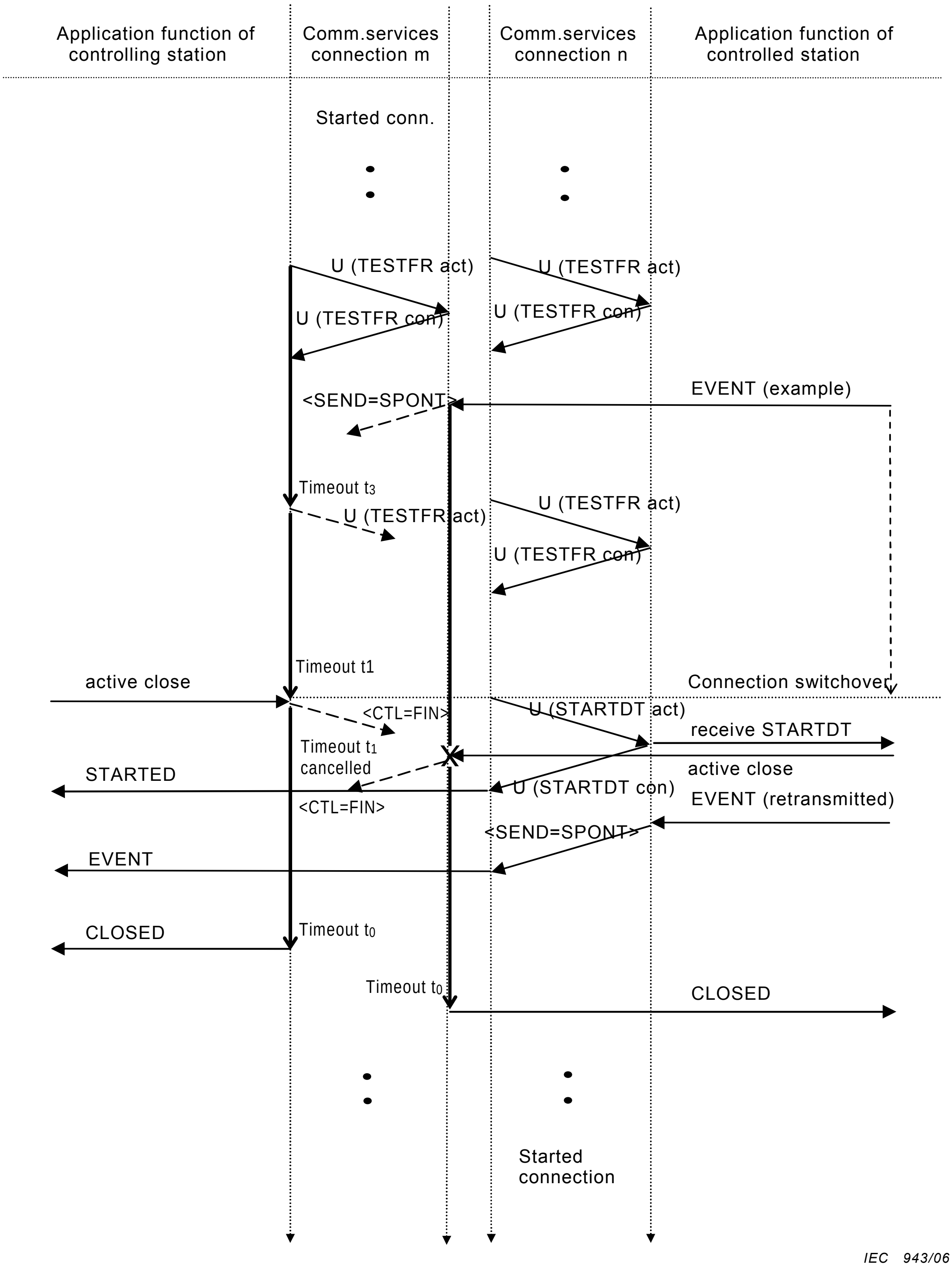
If communication fails on the started connection when the controlled station attempts to transmit user data (e.g. an event ASDU), the controlling station shall detect the failure and perform a connection switchover before the ASDU can be retransmitted on one of the previously stopped connections. A sequential procedure to illustrate this case is shown in Figure 35, with the use of asymmetric timeouts as explained in 10.7.

A STARTDT_ACT will eventually be received on one of the stopped connections (connection m) as a result of a timeout (t_1) in the controlling station to a TESTFR frame on the currently started but failed connection. The selected stopped connection now becomes the new started connection, and the pending event is retransmitted on this connection.

In general, any unconfirmed user data will be retransmitted on the new started connection after a connection switchover has been performed, including potential unconfirmed ACTCONs or ACTTERMs.

The failed connection is eventually closed by both sides, and reopening is then regularly retried until the error has been corrected and the connection is re-established.

The controlling station shall not acknowledge user data received on a connection which is not started.



NOTE 1 The sequential interrelationship between the procedures on the two connections is not fixed, except when connection switch occurs.

NOTE 2 The figure shows the use of asymmetric timeouts t_1 as described in 10.7.

Figure 35 – Redundant connections – User data from controlled station

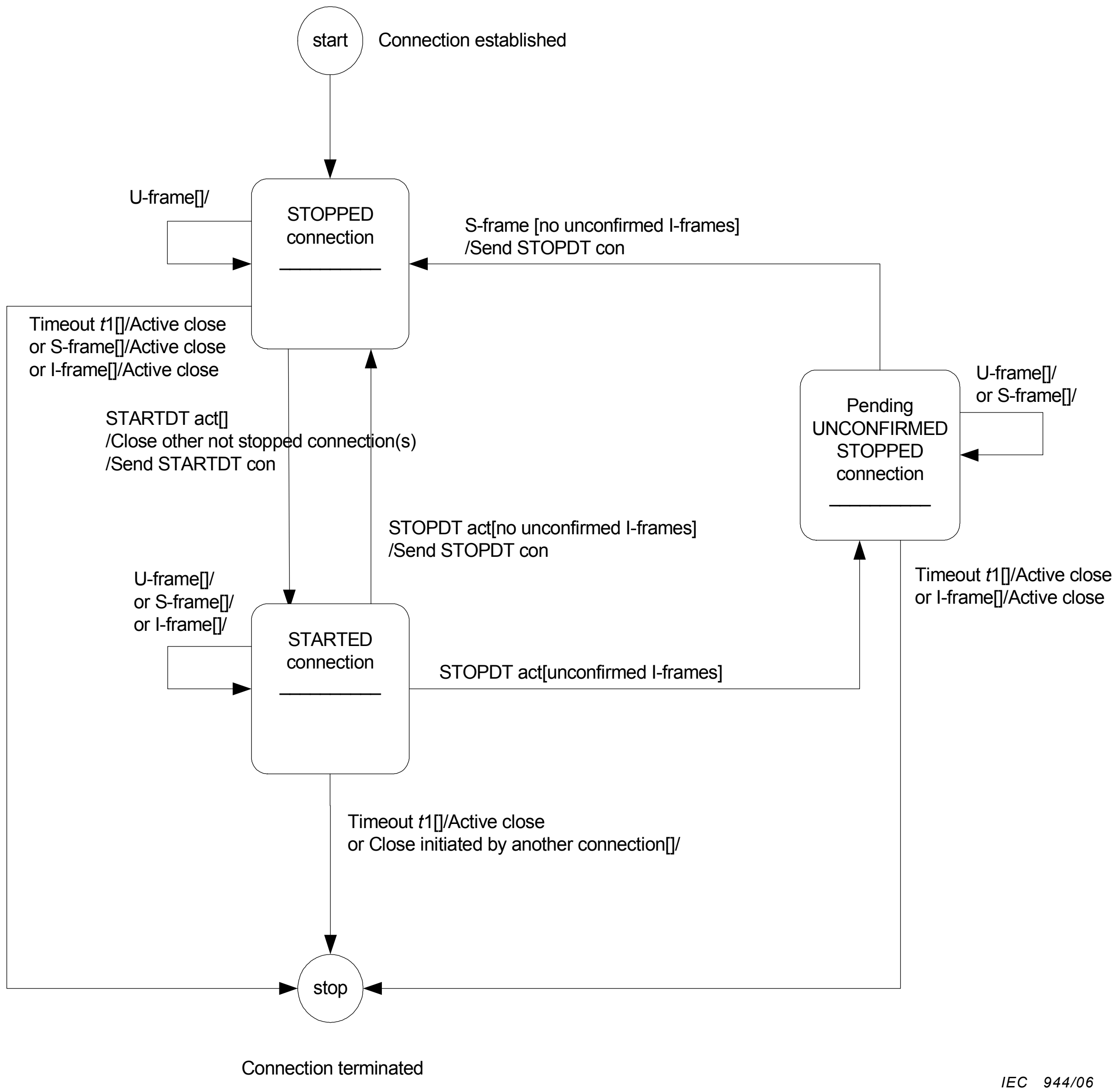
10.7 State transition diagrams

Figures 36 and 37 show state transition diagrams for the Start/Stop procedure of a connection that also supports automatic connection switchover, in case of redundant connections.

A timeout t_1 in the controlling station on the started connection may automatically trigger the user application to issue a connection change request, and hence cause the start of a new (redundant) connection and an automatic connection switchover. Manual switchover is initiated by the user application either by a Stop on the started connection followed by a Start on another connection, or simply by issuing a connection change request.

Any connection that is not in the STOPPED state is immediately closed at the event of a Start on a new connection. This means that asymmetric timeouts t_1 can also be used (and t_2 correspondingly), i.e. shorter t_1 in the controlling station than in the controlled station to reduce switchover time.

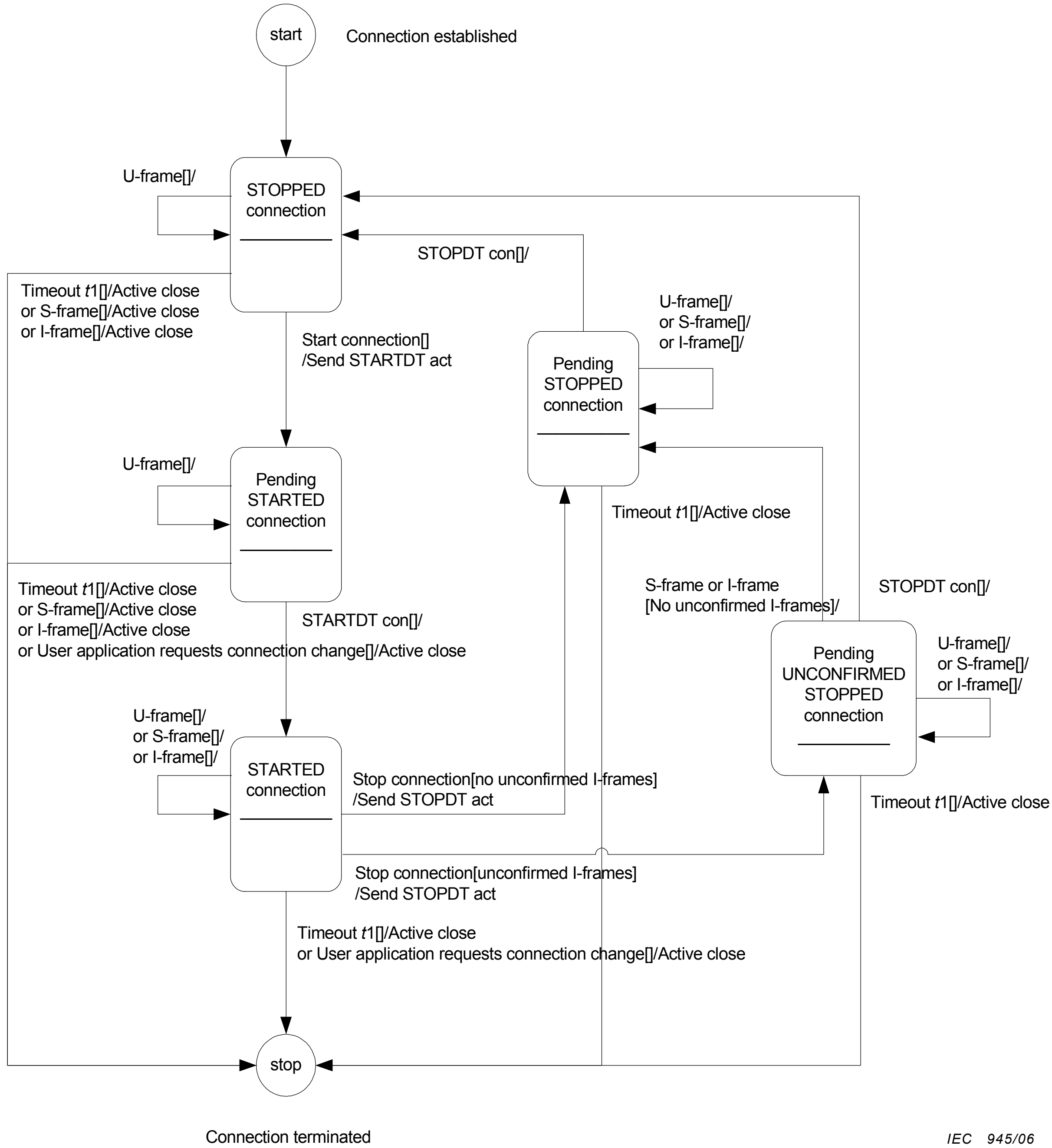
It should be possible to set the values of the timers t_0 to t_3 individually for each connection within a redundancy group.



NOTE 1 Connection terminated means that there is no longer any data exchange between TCP and the application protocol (CS104).

NOTE 2 t_1 is the time out of a sent U-frame or I-frame.

Figure 36 – State transition diagram for redundant connections (controlled station)



NOTE 1 Connection terminated means that there is no longer any data exchange between TCP and the application protocol (CS104).

NOTE 2 *t*1 is the time out of a sent U-frame or I-frame.

Figure 37 – State transition diagram for redundant connections (controlling station)

ISBN 2-8318-8657-0

ICS 33.200

Typeset and printed by the IEC Central Office
GENEVA, SWITZERLAND