IEC TS 60870-5-7

Edition 2.0 2025-03

TECHNICAL SPECIFICATION

Telecontrol equipment and systems – Part 5-7: Transmission protocols – Security extensions to IEC 60870-5-101 and IEC 60870-5-104 protocols (applying IEC 62351)

INTERNATIONAL ELECTROTECHNICAL COMMISSION

ICS 33.200

ISBN 978-2-8327-0275-8

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

TELECONTROL EQUIPMENT AND SYSTEMS –

Part 5-7: Transmission protocols – Security extensions to IEC 60870-5-101 and IEC 60870-5-104 protocols (applying IEC 62351)

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 itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
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) IEC draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). IEC takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, IEC had not received notice of (a) patent(s), which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at https://patents.iec.ch. IEC shall not be held responsible for identifying any or all such patent rights.

IEC TS 60870-5-7 has been prepared by IEC technical committee 57: Power systems management and associated information exchange. It is a Technical Specification.

This second edition cancels and replaces the first edition published in 2013. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

a) This edition has been completely revised with respect to the previous edition;
b) Alignment with updated versions of IEC 62351-3:2023 and IEC 62351-5:2023;
c) Definition of specific profiles for application layer and transport layer;

d) Introduction of Session Initiation Request to handle situations in which the called station reestablishes a connection;

e) Inclusion of multicast security for the unbalanced mode of IEC 60870-5-101 including key management;

f) Consideration of RBAC based on IEC 62351-8.

This Technical Specification is to be used in conjunction with IEC 62351-5:2023 and IEC 60870-5-104:2016.

The text of this Technical Specification is based on the following documents:

Draft	Report on voting
57/2740/DTS	57/2762/RVDTS

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

The language used for the development of this Technical Specification is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/publications.

NOTE The following print types are used:

- Encoding in ASN.1: in `courier new type`.

A list of all the parts in the IEC 60870 series, published under the general title *Telecontrol equipment and systems*, can be found on the IEC website.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under webstore.iec.ch in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn, or
- revised.

TELECONTROL EQUIPMENT AND SYSTEMS –

Part 5-7: Transmission protocols – Security extensions to IEC 60870-5-101 and IEC 60870-5-104 protocols (applying IEC 62351)

1 Scope

This part of IEC 60870, which is a technical specification, describes messages and data formats for implementing IEC 62351-5:2023 for secure communication as an extension to IEC 60870-5-101 and IEC 60870-5-104.

The purpose of this document is to permit the receiver of any IEC 60870-5-101/-104 Application Protocol Data Unit (APDU) to verify that the APDU was transmitted by an authorized user and that the APDU was not modified in transit.

This document is also intended to be used, together with the definitions of IEC 62351-3:2023, in conjunction with the IEC 60870-5-104 companion standard.

The state machines, message sequences, and procedures for exchanging these messages are defined in IEC 62351-5:2023. This document describes only the message formats, selected options, critical operations, addressing considerations and other adaptations required to implement IEC 62351 in the IEC 60870-5-101 and IEC 60870-5-104 protocols.

NOTE The version handling is controlled by configuration and not dynamically changed, therefore unexpected / unknown messages are neglected and not processed.

In addition to the previous edition, this new edition of this document also addresses role-based access control, by utilizing the IEC 62351-8 RBAC approach and the already defined role to permission mapping from IEC 62351-5:2023.

The scope of this document does not include security for IEC 60870-5-102 or IEC 60870-5-103. IEC 60870-5-102 is in limited use only and will therefore not be addressed. Users of IEC 60870-5-103 desiring a secure solution need to implement IEC 61850 using the security measures from in IEC 62351 referenced in IEC 61850.

Management of keys, certificates or other cryptographic credentials within devices or on communication links other than IEC 60870-5-101/104 is out of the scope of this document and might be addressed by other IEC 62351 publications in the future.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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 60870-5-101:2003, *Telecontrol equipment and systems – Part 5-101: Transmission protocols – Companion standard for basic telecontrol tasks*

IEC 60870-5-104:2006, *Telecontrol equipment and systems – Part 5-104: Transmission protocols – Network access for IEC 60870-5-101 using standard transport profiles*

IEC TS 62351-2, *Power systems management and associated information exchange – Data and communications security – Part 2: Glossary of terms*

IEC 62351-3:2023, *Power systems management and associated information exchange – Data and communications security – Part 3: Communication network and system security – Profiles including TCP/IP*

IEC 62351-5:2023, *Power systems management and associated information exchange – Data and communications security – Part 5: Security for IEC 60870-5 and derivatives*

IEC 62351-8, *Power systems management and associated information exchange – Data and communications security – Part 8: Role-based access control for power system management*

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- IEC Electropedia: available at https://www.electropedia.org/
- ISO Online browsing platform: available at https://www.iso.org/obp

NOTE Terms 3.1.1 to 3.1.7 are included here because they are specific to the IEC 60870-5 standard series and can be useful for reading this document as an independent document. Terms 3.1.8 and 3.1.9 are included here because they are specific to IEC 62351-5:2023.

3.1.1
A-Profile
application security profile described in IEC 62351-5:2023

3.1.2
T-Profile
transport security profile described in IEC 62351-3:2023

3.1.3
Application Protocol Data Unit
APDU
complete application layer message transmitted by a station

3.1.4
Application Service Data Unit
ASDU
application layer message submitted to lower layers for transmission

3.1.5
controlling station
device or application that initiates most of the communications and issues commands

3.1.6
controlled station
remote device that transmits data gathered in the field to the controlling station

3.1.7
control direction
data transmitted by the controlling station to the controlled station(s)

3.1.8
Message Authentication Code
MAC
calculated value used by a transmitting and a receiving station to authenticate and ensure the integrity of an Application Protocol Data Unit

3.1.9
Monitoring Direction
data transmitted by the controlled station to the controlling stations

3.2 Abbreviated terms

For the purposes of this document, the abbreviated terms given in IEC TS 62351-2, as well as the following apply. Terms 3.2.2 to 3.2.4 are included here because they are specifically used in the affected protocols and used in the discussion of this security mechanism.

3.2.1
AEAD
Authenticated encryption with authenticated data

3.2.2
APDU
Application Protocol Data Unit

3.2.3
ASDU
Application Service Data Unit

3.2.4
ASN
ASDU segment number

3.2.5
FIN
Final segment

3.2.6
FIR
First segment

3.2.7
HKDF
Key Derivation Function

3.2.8
MAC
Message Authentication Code

3.2.9
RBAC
Role-based access control

4 Overview of IEC 60870-5-7 profiles

This document specifies two different security profiles to protect IEC 60870-5-101 and IEC 60870-5-104 communication, namely:

- A-Profile based on IEC 62351-5:2023, as described in Clause 5 of this document. This profile targets the protection of IEC 60870-5-101 and IEC 60870-5-104 communications at the application level.
- T-Profile based on IEC 62351-3:2023, as described in Clause 6 of this document. This profile targets the protection only for IEC 60870-5-104 communication, at transport (TCP/IP) level.

Figure 1 illustrates the protocol stack for IEC 60870-5-101 and IEC 60870-5-104 and how the different security profiles or their combination defined in this document relate to these protocol stacks.

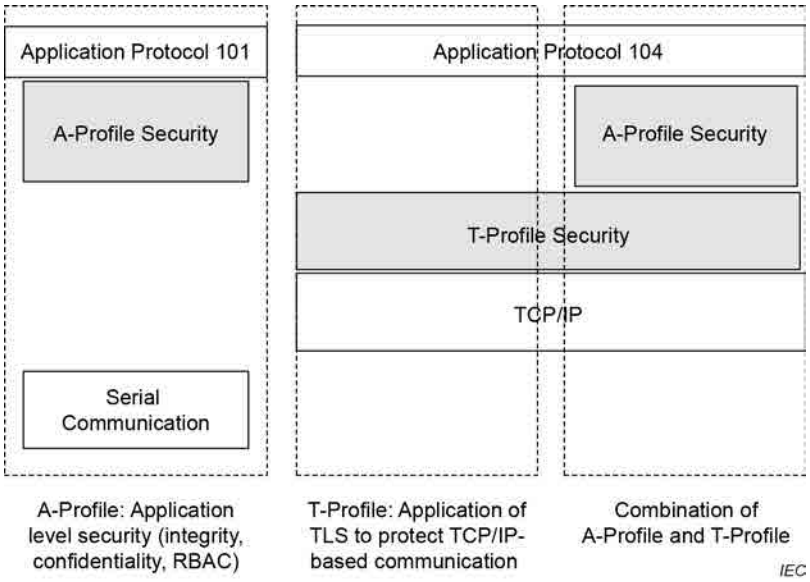


Figure 1 – IEC 60870-5-7 Profiles

Note that the A-Profile as well as the T-Profile security allow mutual authentication in combination with or without RBAC. In addition, protection with integrity only or integrity combined with confidentiality is possible.

5 A-Profile: Implementation of IEC 62351-5

5.1 General

This clause specifies the application of A-Profile security, which provides security as part of the application layer. A-Profile security relies on specification of messages and procedures as described in IEC 62351-5:2023 and outlined in 5.2. 5.3 and 5.4 and in Annex A.

If the A-Profile is used in conjunction with RBAC, the procedure defined in IEC 62351-5:2023, 8.3.12.2, shall be followed.

5.2 Selected options

5.2.1 Overview of clause

This clause describes which of the options specified in IEC 62351-5:2023 shall be implemented in IEC 60870-5-101 and IEC 60870-5-104.

5.2.2 MAC algorithms

IEC 60870-5 stations shall implement all the mandatory MAC algorithms listed in IEC 62351-5:2023, and may implement any of the optional MAC algorithms listed there.

5.2.3 Encryption algorithms

IEC 60870-5 stations shall implement all the mandatory encryption algorithms listed in IEC 62351-5:2023 and may implement any of the optional encryption algorithms listed there.

5.3 Implementation of procedures

5.3.1 Overview of clause

Stations implementing this document for security of IEC 60870-5-101/IEC 60870-5-104 shall implement the procedures and state machines described in Clause 8 of IEC 62351-5:2023. They shall also implement the additional procedures described in the remainder of this clause.

5.3.2 Detection of communication failures

IEC 60870-5-2:1992 describes the serial link transmission procedures allowing the detection of connection failures when using IEC 60870-5-101 communication.

IEC 60870-5-104:2006 describes network transmission procedures using TCP/IP, which also allow detection of connection failures.

In case a communication failure is detected, the implementation of the security mechanism described in this document shall stop sending of any further messages and stop all related timers except the Session Key Usage Timer (as defined in IEC 62351-5:2023).

5.3.3 Algorithm selection for Update Keys derivation

During the Station Association procedure, the Update Keys shall be derived as described in 8.3.10 of IEC 62351-5:2023.

The hash function to be used in both HKDF extract and expand steps shall be the same hash function used in the MAC algorithm selected by the controlling station in the Update Key Change message.

5.3.4 Session keys – Application and management

5.3.4.1 General

If this security mechanism is applied to IEC 60870-5-104, the Control Direction Session Key shall be used to authenticate Secure Data messages in control direction with any common address value, including the broadcast common address.

If this security mechanism is applied to IEC 60870-5-101, the Control Direction Session Key shall be used to protect Secure Data messages in control direction with unicast common address value only. If broadcast common address ASDUs are supported in control direction, Secure Data messages with this common address value shall be protected with a different Session Key, as described in 5.3.4.2.

This security mechanism requires the controlling station to support the option of executing the Session Key Change procedure also when it is solicited by the controlled station, as described in 5.3.4.3.

5.3.4.2 Session key to authenticate broadcast ASDU in IEC 60870-5-101

5.3.4.2.1 General

If this security mechanism is applied to IEC 60870-5-101 and broadcast common address ASDU in control direction are supported, the Secure Data messages with broadcast common address shall be authenticated using a separate Broadcast Session Key.

The Broadcast Session Key is unique and has the same value for all the stations (controlling and controlled) connected. The controlling station shall create Broadcast Session Key and distribute it to each controlled station connected by performing the Session Key Change procedure described in IEC 62351-5:2023, 8.4. Subclause 5.4.3.11 of this document describes the data to be included in the Session Key Change Request message when this procedure is used to initialize or change the Broadcast Session Key.

According to IEC 62351-5:2023, 8.4.2.4.5, the length of the Broadcast Session Key shall be 256 bits.

The Broadcast Session Key has its own independent usage timer (the Broadcast Session Key Usage Timer) and usage counter (the Broadcast Session Key Usage Counter) as well as the corresponding configurable parameters (Max Broadcast Session Key Usage Time and Max Broadcast Session Key Usage Count) in both controlling and controlled stations as described in 9.6. It is recommended to set duration of the Max Broadcast Session Key Usage Time greater than is set for the Max Session Key Usage Time, considering the frequency of use of broadcast messages.

As with the Monitor Direction and Control Direction Session Keys, the Broadcast Session Key shall be managed as described in IEC 62351-5:2023, 8.4.5. When the Broadcast Session Key Change Usage Timer expires, or the Broadcast Session Key Usage Count has exceeded, the controlling station shall perform the Session Key Change procedure for Broadcast Session Key to each controlled station connected. Figure 16 describes the initial procedure to distribute the Broadcast Session Key whereas the update procedure is described in Figure 17.

If the Session Key Change procedure has to be performed for all Session Keys (Monitor Direction, Control Direction and Broadcast Session Keys) at the same time, priority shall be given to the Session Key Change procedure for Monitor Direction and Control Direction Session Keys. The Session Key Change procedure for the Broadcast Session Key shall be executed whenever the Session Key Change procedure for Monitor Direction and Control Direction Session Keys has been successfully completed or has failed.

5.3.4.2.2 Broadcast Session Key management on controlling station

When a new Broadcast Session Key to is distributed to all the controlled stations connected by performing the Session Key Change procedure, the controlling station shall maintain the current Broadcast Session Key still valid, and shall continue to use it to protect Broadcast Secure Data messages, until the Session Key Change procedure has been completed for all the controlled station connected. The Broadcast Session Key distribution is considered completed even if the Session Key Change procedure has failed for one or more controlled station.

During the Broadcast Session Key update procedure both the Current Broadcast Session Key and the New Broadcast Session Key are sent to each controlled station. When the Broadcast Session Key distribution is completed, the controlling station shall use the New Broadcast Session Key to protect all subsequent secure data messages with the broadcast address.

The controlled stations, which could not be updated, will use the Session Initiation Request to establish the current Session Keys and the Current Broadcast Session Key, and, if necessary, the New Broadcast Session Key.

5.3.4.2.3 Broadcast Session Key management on controlled station

When the controlled station is provisioned with a new Broadcast Session Key, by performing the Session Key Change procedure (initiated by the controlling station), the controlled station shall maintain both the new and the current Broadcast Session Keys. Either key may be valid to authenticate Broadcast Secure Data messages received during the key distribution period.

When the controlled station receives the first Secure Data message (see 5.4.3.13) with the broadcast address, that is protected with the new Broadcast Session Key provisioned, the controlled station shall invalidate the current Broadcast Session Key and apply the new Broadcast Session Key to all subsequent Broadcast Secure Data messages received.

5.3.4.3 Session Key Change procedure solicited by controlled station

5.3.4.3.1 General

As described in IEC 62351-5:2023, 8.4.2.6, the controlled station may optionally solicit the controlling station to initiate the Session Key Change procedure by sending a Session Initiation Request message. The affected protocol referencing standards may define the Session Initiation Request message and its management.

This document makes use of the Session Initiation Request when controlled station has reinitialized because in this condition the controlled station Session Keys shall be considered not valid and its Data Sequence Number (DSQ, described in IEC 62351-5:2023, 8.5.2.2.4) is reset.

Applying the security mechanism defined in IEC 62351-5:2023 to IEC 60870-5-101 and IEC 60870-5-104 protocols, devices claiming conformance to this document shall support the Session Initiation Request message, defined in 5.4.3.8 as well as the additional Session Keys management described in 5.3.4.3.2 and 5.3.4.3.3 for each association established.

5.3.4.3.2 Session Keys management on controlled station

On controlled station, the current session keys shall be stored in a way that will be retained over a restart of the device. This shall occur when they are initialized and each time they are changed (i.e., when the Session Key Change procedure is successfully executed).

After reinitialization of the controlled station, if the Session Keys are available, the controlled station shall mark the Session Keys invalid. The initial session key establishment is described in IEC 62351-5:2023, 8.4.

The existing Session Key is used after restart to secure the Session Initiation Message.

If the Session Keys are marked invalid while Session Key Change state machine is in Session Idle State, the controlled station shall perform the following actions:

a) Send the Session Initiation Requests to the controlling station

b) Start the Request Timer

If the Request Timer expires, the controlled station shall repeat the actions above.

If the controlled station receives a valid Session Request, it shall stop the Request Timer and execute the Session Key Change procedure described in IEC 62351-5:2023, 8.4.4.

5.3.4.3.3 Session Keys management on controlling station

On the controlling station, the current session keys shall be stored in a way that will be retained over a restart of the device. This shall occur when they are initialized and each time they are changed (i.e. when the Session Key Change procedure is successfully executed).

After reinitialization of the controlling station, if the Session Keys are available, the controlling station shall perform the following actions:

a) Mark the Session Keys invalid

b) Initiate the Session Key Change procedure at the earliest opportunity.

The initial session key establishment is described in IEC 62351-5:2023, 8.4.

If the controlling station Session Key Change state machine is in the Key Management Idle state, it shall accept a valid Session Initiation Request sent by the controlled station and shall perform the following actions:

a) Mark the Session Keys invalid.

b) Initiate the Session Key Change procedure at the earliest opportunity.

If this security mechanism is applied to IEC 60870-5-101 and broadcast common address messages are used, the Session Key Change procedure for the Broadcast Session Key shall be also executed immediately after the Session Key Change procedure for Monitor and Control Direction Session Keys.

If the controlling station Session Key Change state machine is in the Key Management Idle state and it receives an invalid Session Initiation Request message, it shall perform the following actions:

a) Discard the message.

b) Increment the Discarded Messages statistic.

c) If MAC is invalid, increment the Key Authentication Failures statistic.

If the controlling station Session Key Change state machine is not in the Key Management Idle state and it receives a Session Initiation Request sent by the controlled station, it shall perform the following actions.

a) Increment the Unexpected Messages statistic.

b) Discard the message.

c) Increment the Discarded Messages statistic.

5.3.5 Co-existence with non-secure implementations

It shall be configurable at the controlling station whether to apply this specification on a per-connection and per data link address basis. This will permit secure and non-secure controlled station implementations to communicate with the same controlling station at the same time.

Controlled stations may be configurable to permit secure and non-secure communication with controlling station.

All stations shall deny unsecured communication when configured to use secured communication for that connection.

5.4 Implementation of messages

5.4.1 Overview of clause

This clause describes how the secure authentication messages described in IEC 62351-5:2023 are implemented in IEC 60870-5-101 and IEC 60870-5-104.

5.4.2 Data definitions

5.4.2.1 Causes of transmission

Stations implementing secure authentication shall use the causes of transmission listed in Table 1 in addition to those described in 7.2.3 of IEC 60870-5-101:2003.

Table 1 – Additional cause of transmission

Cause	:=	UI6[1..6]<14..17>
<14>	:=	application data authentication
<15>	:=	maintenance of session key
<16>	:=	maintenance of association and update key
<17>	:=	operation not authorized [1)]

[1)] This cause of transmission is used by the controlled station only and shall be managed by the application. If the controlled station receives a request from the controlling station, which the controlling station is not authorized to perform, the controlled station shall respond with a negative acknowledge containing cause of transmission <17>.

5.4.2.2 Type identifiers

Stations implementing secure authentication shall use the Type Identifications listed in Table 2 in addition to those described in 7.2.1 of IEC 60870-5-101:2003 and Clause 6 of IEC 60870-5-104:2006. This range of Type Identifications was previously allocated for system information in the monitor direction. Some ASDUs identified by these types may be transmitted in the control direction.

Table 2 – Additional type identifiers

TYPE IDENTIFICATION	:=	UI8[1..8]<81..91>	
<81>	:=	Association request	S_AQ_NA_1
<82>	:=	Association response	S_AP_NA_1
<83>	:=	Update key change request	S_UH_NA_1
<84>	:=	Update key change response	S_UP_NA_1
<85>	:=	Session initiation request	S_SI_NA_1
<86>	:=	Session request	S_SQ_NA_1
<87>	:=	Session response	S_SP_NA_1
<88>	:=	Session key change request	S_KH_NA_1
<89>	:=	Session key change response	S_KP_NA_1
<91>	:=	Secure data	S_SD_NA_1

5.4.2.3 Security statistics

Stations implementing secure authentication shall use the ASDU Type 37*:* Integrated totals with time tag CP56Time2a, defined in 7.3.1.29 of IEC 60870-5-101*,* to report the values of the security statistics described in 7.5 of IEC 62351-5:2023. The Information Object Address of each security statistic shall be recorded in the Protocol Implementation Conformance Statement for each station as described in 9.7.

The procedures used by the controlled station to report the security statistics shall be the same as for the existing integrated totals, as described in 7.4.8 of IEC 60870-5-101:2003, particularly including the ability for these totals to be reported using spontaneous transmission.

It is recommended to report all security statistics in a single integrated totals group. The value of each BCR field is in the range between 0 and 231-1.

5.4.2.4 Information object address

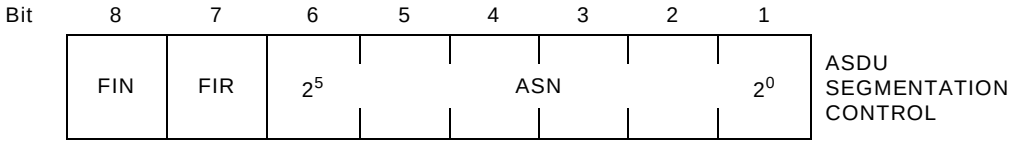
The Information Object Address (IOA) does not apply to the ASDUs described in IEC TS 60870-5-7 and is not included in these ASDUs. It is replaced by the ASDU Segmentation Control octet specified in 5.4.2.5.

5.4.2.5 Transmitting extended ASDUs using segmentation

Several of the messages defined in IEC 62351-5:2023 are longer than the maximum length of an IEC 60870-5 data link or APCI frame. Figure 2 defines a field that shall be used to control reassembly when an IEC 60870-5-7 ASDU is transmitted in a series of several segments such that each segment will fit in a data link or APCI frame.

The ASDU segmentation described here is a frame transport feature. Security is applied to ASDU before segmentation. Therefore, the segmentation field is not included in the protected data.

The transmitting station shall add the MAC value into or encrypt application data in the ASDU prior to applying ASDU segmentation and transmission. Symmetrically, the receiving station shall reassemble the entire ASDU, from the ASDU segments received, prior to verify MAC value or decrypt the application data.



ASDU SEGMENTATION CONTROL:= CP8{FIN, FIR, ASN}

ASN := UI6[1..6]<0..63>

FIR := BS[7]<0..1>

<0> := This is not the first segment of an ASDU

<1> := This is the first segment of an ASDU

FIN := BS[8]<0..1>

<0> := This is not the final segment of an ASDU

<1> := This is the final segment of an ASDU

Figure 2 – ASDU segmentation control

If an ASDU is too long to fit in a lower-level data link or APCI frame, the excess application layer data shall be divided into segments as illustrated in Figure 3. The Data Unit Identifier fields of the ASDU (Type Id, VSQ, COT, CASDU, and ASDU SEGMENTATION CONTROL) shall be prepended to each segment so the receiving station can recognize the type, address and disposition of each segment. The station shall transmit the segments in sequence as if they were separate ASDUs, but without any data of a different Type ID interspersed.

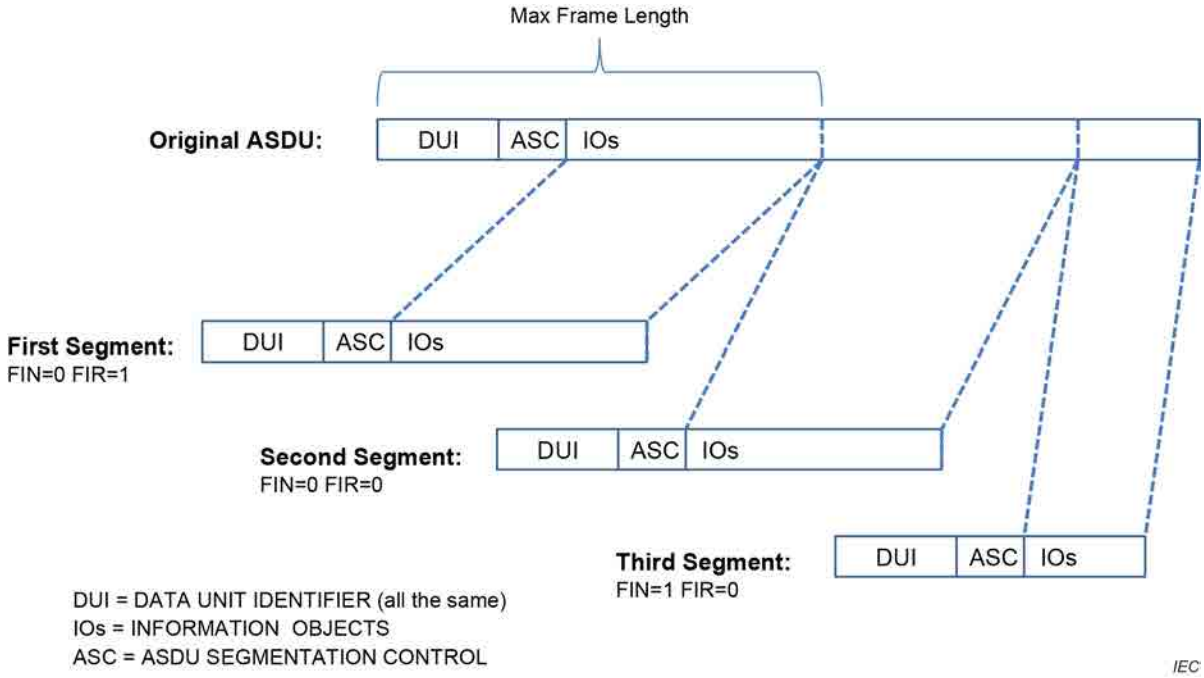


Figure 3 – Segmenting extended ASDUs

The ASN (ASDU Segment Sequence Number) shall be used to verify that segments are received in the correct order and shall help detect duplicated or missing segments. The ASN shall increment by one, modulo 64. After sequence number 63, the next sequence number value shall be 0.

The following rules shall apply when segmenting ASDUs:

1) A segment series shall begin with a segment having the FIR bit set.
2) A segment series shall end with a segment having the FIN bit set.
3) When no segment series is in progress, the receiving station shall discard any segment received without the FIR bit set.
4) A segment with the FIR bit set may have any sequence number from 0 to 63 without regard to prior history.
5) After a segment series has been started:
   a) Each subsequent segment shall have an ASN that is incremented by one (modulo 64) from the preceding segment. A received segment that meets this requirement shall become the next member of the segment series. The station shall treat all the data following the ASDU SEGMENTATION CONTROL field as if it was appended to the end of the previous data in the series.
   b) If a station receives a segment having the FIR bit set, it shall discard the entire, in-progress segment series and start a new segment series with the newly received segment as its first member.
   c) If a station receives a segment that is octet-for-octet identical to the preceding segment it shall discard the segment.
   d) If a station receives a segment having the FIR bit cleared and a sequence number other than the expected incremental number, that is not octet-for-octet identical to the preceding segment, the station shall discard the segment and the entire in-progress segment series and terminate the series.
6) A segment series may consist of a single segment having both FIR and FIN bits set.
7) When a receiving station receives a segment with the FIN bit set and therefore assembles a complete segment series, only then may the station evaluate the complete ASDU.

8) If a station receives a segment in which the Type ID, VSQ, CASDU, or COT does not match that of the first ASDU in the sequence, the station shall discard the segment and the entire series.

Whenever a segment series is discarded, the Discarded Messages statistic shall be incremented.

It is recommended that transmitting stations make each segment as large as possible for maximum efficiency of transmission. However, this is not a requirement and receiving stations shall accept varying segment lengths within the same series.

The state machine described in Table 3 defines how the station shall reassemble ASDUs from segments. This state machine assumes the reception software uses an ASDU buffer in which application data from the received segments are temporarily stored before presenting the completed ASDU to the application layer process.

There are two states:

- Idle state: The station is idle waiting for a segment to arrive with the FIR bit set.
- Assembly state: The ASDU buffer holds application data from at least one segment. While in this state, the station is awaiting additional segments to complete the ASDU.

The terminology used in Table 3 is defined as follows:

- X means "don’t care"
- SAME means the ASN is identical to the ASN in the segment immediately preceding this segment
- +1 means the ASN is incremented by one count, modulo 64, from the sequence number in the segment immediately preceding this segment
- +M, $1 < M < 64$ means the sequence number is incremented by more than one count and fewer than 64 counts from the sequence number in the segment immediately preceding this segment

Table 3 – ASDU segment reception state machine

Current state	Event that triggers an action and possible transition				Action	Transition to state	
A	B			C	D	E	
If the software state is	And a segment with these fields is received			The meaning is	then perform this action	and go to this state	
	FIR	FIN	ASN				
Idle	0	X	X	Not a first segment	Discard segment.	Idle	1
	1	1	X	Entire ASDU fits within the segment	Clear the ASDU buffer, place segment's Information Object data into the ASDU buffer and pass ASDU buffer to application layer.	Idle	2
	1	0	X	First of multiple segments	Clear the ASDU buffer and place segment's Information Object data into the ASDU buffer.	Assembly	3
Assembly	0	X	SAME	IF segment is octet-for-octet identical to previous, it is a duplicate	Discard segment.	Assembly	4
	0	X	SAME	IF segment is NOT octet-for-octet identical to previous, it may be from another series	Discard segment and the entire, in-progress segment-series.	Idle	5
	0	0	+1	Expected segment received, more segments are expected	Append segment's Information Object data to contents of ASDU buffer.	Assembly	6
	0	1	+1	Expected segment received, final segment	Append segment's Information Object data to contents of ASDU buffer and pass ASDU buffer to application layer.	Idle	7
	0	X	+M 1 < M < 64	ASN is out of order	Discard segment and the entire, in-progress segment-series.	Idle	8
	1	0	X	First of multiple segments	Clear contents of ASDU buffer and place segment's Information Object data into the ASDU buffer.	Assembly	9
	1	1	X	Entire ASDU fits within the segment	Clear contents of ASDU buffer, place segment's Information Object data into the ASDU buffer and pass ASDU buffer to Application Layer.	Idle	10
	0	X	X	IF segment is not the first of multiple segments and the Type ID, VSQ, CASDU, or COT does not match the first segment	Discard segment and the entire, in-progress segment-series.	Idle	11

Figure 4 illustrates the same state machine described in Table 3. If the two differ, Table 3 shall be considered correct.

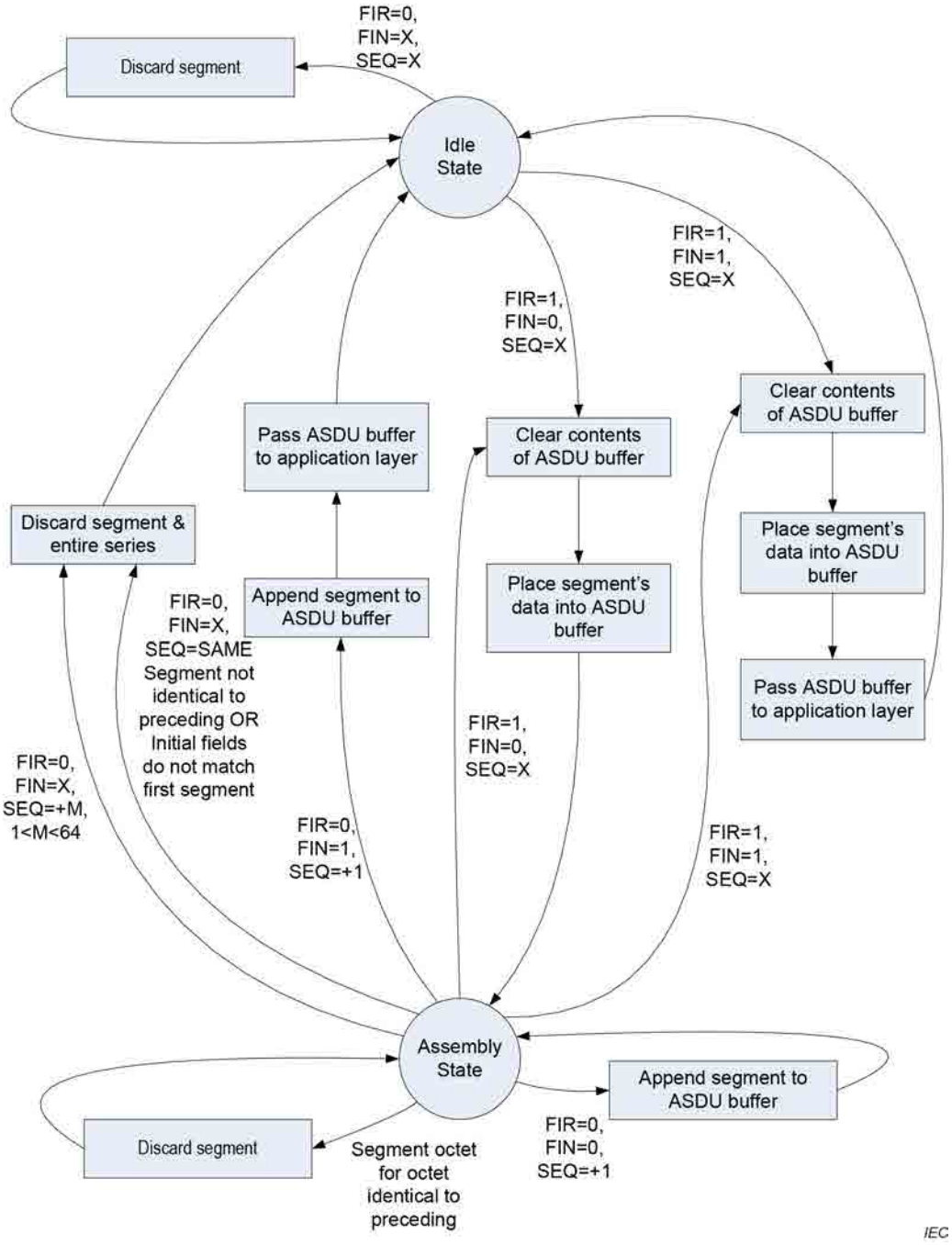


Figure 4 – Illustration of ASDU segment reception state machine

5.4.3 Application Service Data Units

5.4.3.1 General

In IEC 62351-5:2023 the security mechanism described is not backward compatible with the previous version of this standard (IEC 62351-5:2013). The message types (Type ID) and the cause of transmission (CoT) values have been redefined (see Table 2).

5.4.3.2 Cryptographic protection of messages

Messages with the Type IDs 83, 84, 85, 87, 88 and 89 are MAC protected. The message with the Type ID 91 (Secure Data) is either MAC-protected or AEAD-protected.

Regarding the MAC calculation in this document, when IEC 62351-5 indicates that an entire message is included in the MAC calculation for this document, this means that also the Data Unit Identifier of an ASDU must be included at the beginning.

For MAC calculation, this can be depicted as shown in Figure 5 for the message "Secure Data" (see 5.4.3.13).

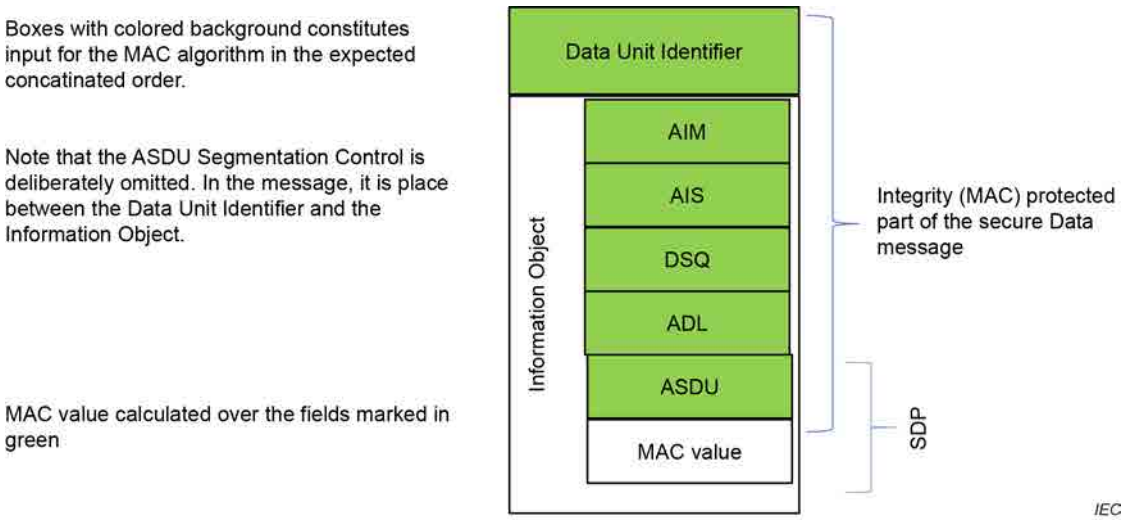


Figure 5 – Example of a MAC calculation of a Secure Data message

NOTE The information contained in an AEAD calculation in the Secure Data message is indicated in 5.4.3.13.

5.4.3.3 TYPE IDENT 81: S_AQ_NA_1 Association Request

The structure of this ASDU is defined in Figure 6.

Single information object (SQ=0)

0 1 0 1 0 0 0 1	TYPE IDENTIFICATION	DATA UNIT IDENTIFIER Defined in 7.1 of IEC 60870-5-101:2003
0 0 0 0 0 0 0 1	VARIABLE STRUCTURE QUALIFIER	
Defined in 7.2.3 of IEC 60870-5-101:2003	CAUSE OF TRANSMISSION	
Defined in 7.2.4 of IEC 60870-5-101:2003	COMMON ADDRESS OF ASDU	
FIN FIR ASN	ASDU Segmentation Control, defined in 5.4.2.5	
Value Value	AIM = Controlling station Association ID, defined in 8.3.5.2.2 of IEC 62351-5:2023	INFORMATION OBJECT
Value Value	AIS = Controlled station Association ID, defined in 8.3.5.2.3 of IEC 62351-5:2023	
Value Value	PRI = Protocol Information, described in 8.3.5.2.4 of IEC 62351-5:2023 and defined in 5.4.3.4	
Value Value	CDL = Controlling station certificate data length, defined in 8.3.5.2.5 of IEC 62351-5:2023	
Number of octets specified in CDL	CDC = Controlling station certificate data, defined in 8.3.5.2.6 of IEC 62351-5:2023	

Figure 6 – ASDU: S_AQ_NA_1 Association Request

S_AQ_NA_1:= CP{Data Unit Identifier, AIM, AIS, PRI, CDL, Controlling station certificate data}

CAUSES OF TRANSMISSION used with
TYPE IDENT 81:= S_AQ_NA_1

CAUSE OF TRANSMISSION

In control direction:

<16>:= maintenance of association and update key

In monitor direction:

Not permitted.

5.4.3.4 Protocol information

5.4.3.4.1 General

The controlling station uses this field to provide protocol information, including the protocol version, it intends to use to the controlled station. Figure 7 illustrates the structure of this field.

Major version / Minor version	Protocol Version	Protocol Information
0x00	reserved for the future use	

Figure 7 – Association Request PRI field

5.4.3.4.2 Protocol version: minor version

Minor Version:= UI4[1-4]<0..15>

Devices claiming conformance to this document shall set this value to 0

5.4.3.4.3 Protocol version: major version

Major Version:= UI4[5-8]<0..15>

Devices claiming conformance to this document shall set this value to 1

5.4.3.5 TYPE IDENT 82: S_AP_NA_1 Association Response

The structure of this ASDU is defined in Figure 8.

Single information object (SQ=0)

0 1 0 1 0 0 1 0	TYPE IDENTIFICATION	DATA UNIT IDENTIFIER Defined in 7.1 of IEC 60870-5-101:2003
0 0 0 0 0 0 0 1	VARIABLE STRUCTURE QUALIFIER	
Defined in 7.2.3 of IEC 60870-5-101:2003	CAUSE OF TRANSMISSION	
Defined in 7.2.4 of IEC 60870-5-101:2003	COMMON ADDRESS OF ASDU	
FIN FIR ASN	ASDU Segmentation Control, defined in 5.4.2.5	
Value	AIM = Controlling station Association ID, defined in 8.3.5.3.2 of IEC 62351-5:2023	INFORMATION OBJECT
Value		
Value	AIS = Controlled station Association ID, defined in 8.3.5.3.3 of IEC 62351-5:2023	
Value		
Value	CDL = Controlled station certificate data length, defined in 8.3.5.3.4 of IEC 62351-5:2023	
Value		
Value	CGL = Controlled station random data length, defined in 8.3.5.3.5 of IEC 62351-5:2023	
Value		
Number of octets specified in CDL	CDC = Controlled station certificate data, defined in 8.3.5.3.6 of IEC 62351-5:2023	
Number of octets specified in CGL	CGD = Controlled station random data, defined in 8.3.5.3.7 of IEC 62351-5:2023	

Figure 8 – ASDU: S_AP_NA_1 Association Response

S_AP_NA_1:= CP{Data Unit Identifier, AIM, AIS, CDL, CGL, Controlled station certificate data, Controlled station random data}

CAUSES OF TRANSMISSION used with
TYPE IDENT 82:= S_AP_NA_1

CAUSE OF TRANSMISSION

In control direction:

Not permitted.

In monitor direction:

<16>:= maintenance of association and update key

5.4.3.6 TYPE IDENT 83: S_UH_NA_1 Update Key Change Request

The structure of this ASDU is defined in Figure 9.

Single information object (SQ=0)

0 1 0 1 0 0 1 1	TYPE IDENTIFICATION	DATA UNIT IDENTIFIER Defined in 7.1 of IEC 60870-5-101:2003
0 0 0 0 0 0 0 1	VARIABLE STRUCTURE QUALIFIER	
Defined in 7.2.3 of IEC 60870-5-101:2003	CAUSE OF TRANSMISSION	
Defined in 7.2.4 of IEC 60870-5-101:2003	COMMON ADDRESS OF ASDU	
FIN FIR ASN	ASDU Segmentation Control, defined in 5.4.2.5	INFORMATION OBJECT
Value	AIM = Controlling station Association ID, defined in 8.3.5.4.2 of IEC 62351-5:2023	
Value		
Value	AIS = Controlled station Association ID, defined in 8.3.5.4.3 of IEC 62351-5:2023	
Value		
Enumerated value	KWA = Session Key wrap algorithm, defined in 8.3.5.4.4 of IEC 62351-5:2023	
Enumerated value	MAL = MAC algorithm, defined in 8.3.5.4.5 of IEC 62351-5:2023	
Value	CGL = Controlling station random data length, defined in 8.3.5.4.6 of IEC 62351-5:2023	
Number of octets in CGL	CGD = Controlling station random data, defined in 8.3.5.4.7 of IEC 62351-5:2023	
Number of octets specified by the MAC algorithm (MAL) selected in the Update Key Change Request message, described in 8.3.5.4.5 of IEC 62351-5:2023	MAC = Message Authentication Code, defined in 8.3.5.4.8 of IEC 62351-5:2023 and in 5.4.3.1 of this document	

Figure 9 – ASDU: S_UH_NA_1 Update Key Change Request

S_UH_NA_1:= CP{Data Unit Identifier, AIM, AIS, KWA, MAL, CGL, Controlling station random data, Message authentication code}

CAUSES OF TRANSMISSION used with
TYPE IDENT 83:= S_UH_NA_1

CAUSE OF TRANSMISSION

In control direction:

<16>:= maintenance of association and update key

In monitor direction:

Not permitted

5.4.3.7 TYPE IDENT 84: S_UP_NA_1 Update Key Change Response

The structure of this ASDU is defined in Figure 10**.**

Single information object (SQ=0)

0 1 0 1 0 1 0 0	TYPE IDENTIFICATION	DATA UNIT IDENTIFIER Defined in 7.1 of IEC 60870-5-101:2003
0 0 0 0 0 0 0 1	VARIABLE STRUCTURE QUALIFIER	
Defined in 7.2.3 of IEC 60870-5-101:2003	CAUSE OF TRANSMISSION	
Defined in 7.2.4 of IEC 60870-5-101:2003	COMMON ADDRESS OF ASDU	
FIN FIR ASN	ASDU Segmentation Control, defined in 5.4.2.5	INFORMATION OBJECT
Value	AIM = Controlling station Association ID, defined in 8.3.5.5.2 of IEC 62351-5:2023	
Value		
Value	AIS = Controlled station Association ID, defined in 8.3.5.5.3 of IEC 62351-5:2023	
Value		
Number of octets specified by the MAC algorithm (MAL) selected in the Update Key Change Request message, described in 8.3.5.4.5 of IEC 62351-5:2023	MAC = Message Authentication Code, defined in 8.3.5.5.4 of IEC 62351-5:2023 and in 5.4.3.1 of this document	

Figure 10 – ASDU: S_UP_NA_1 Update Key Change Response

S_UP_NA_1:= CP{Data Unit Identifier, AIM, AIS, Message authentication code}

CAUSES OF TRANSMISSION used with
TYPE IDENT 84:= S_UP_NA_1

CAUSE OF TRANSMISSION

In control direction:

Not permitted

In monitor direction:

<16>:= maintenance of association and update key

5.4.3.8 TYPE IDENT 85: S_SI_NA_1 Session Initiation Request

5.4.3.8.1 General

The structure of this ASDU is defined in Figure 11.

Single information object (SQ=0)

0 1 0 1 0 1 0 1	TYPE IDENTIFICATION	DATA UNIT IDENTIFIER Defined in 7.1 of IEC 60870-5-101:2003
0 0 0 0 0 0 0 1	VARIABLE STRUCTURE QUALIFIER	
Defined in 7.2.3 of IEC 60870-5-101:2003	CAUSE OF TRANSMISSION	
Defined in 7.2.4 of IEC 60870-5-101:2003	COMMON ADDRESS OF ASDU	
FIN FIR ASN	ASDU Segmentation Control, defined in 5.4.2.5	INFORMATION OBJECT
Value	AIM = Controlling station Association ID, defined in 5.4.3.8.2	
Value		
Value	AIS = Controlled station Association ID, defined in 5.4.3.8.3	
Value		
Value	CGL = Controlled station random data length, defined in 5.4.3.8.4	
Value		
Number of octets specified in CGL	CGD = Controlled station random data, defined in 5.4.3.8.5	
Number of octets specified by the MAC algorithm (MAL) selected in the Update Key Change Request message, described in 8.3.5.4.5 of IEC 62351-5:2023	MAC = Message Authentication Code, defined in 5.4.3.8.6 and in 5.4.3.1 .	

Figure 11 – ASDU: S_SI_NA_1 Session Initiation Request

S_SI_NA_1:= CP{Data Unit Identifier, AIM, AIS, CGL, Controlled station random data, Message authentication code}

CAUSES OF TRANSMISSION used with
TYPE IDENT 85:= S_SI_NA_1

CAUSE OF TRANSMISSION

In control direction:

Not permitted

In monitor direction:

<15>:= maintenance of session key

5.4.3.8.2 Controlling Station Association ID

This is the value the controlling station has chosen to represent the communication link with this controlled station. This value shall match the AIM in the last Update Key Change Request received by the controlled station during the successful Station Association procedure most recently performed for this communication link, described in IEC 62351-5:2023, 8.3.5.4.2.

AIM:= UI16[1..16]<1..65535>

5.4.3.8.3 Controlled Station Association ID

This is the value the controlled station has chosen to represent the communication link with this controlling station. This value shall match the AIS in the last Update Key Change Response sent by the controlled station during the successful Station Association procedure most recently performed for this communication link, described in IEC 62351-5:2023, 8.3.5.5.3.

AIS:= UI16[1..16]<1..65535>

5.4.3.8.4 Controlled Station Random Data Length

This value shall specify the length in octets of the random data that follows. The minimum length of the random data in this message shall be four octets, the maximum length is 64 octets.

CGL:= UI8[1..8]<4..64>

5.4.3.8.5 Controlled Station Random Data

The controlled station shall include this random data in the Session Initiation Request message to ensure that the contents of the subsequent Session Request message are not predictable and to protect the controlled station against replay attacks. Random number generators are responsible for providing statistically adequate random data. Guidance for random number generation can be found in NIST SP 800-90A Rev.1, NIST SP 800-90B, NIST SP 800-90C, IETF RFC 4086 as well as in Clause B.12 of IEC 62351-9:2023.

CGD:= OS8i[1..8i]; i:=CGL

5.4.3.8.6 Message Authentication Code

The controlled station shall use this field to authenticate the data included in Session Initiation Request message being transmitted.

This value shall be calculated using the MAC algorithm selected in the last Update Key Change Request received by the controlled station during the successful Station Association procedure most recently performed for this communication link, described in IEC 62351-5:2023, subclause 8.3.5.4.5, using the corresponding Authentication Update Key generated as described in IEC 62351-5:2023, 8.3.10.

The controlling station shall pass the data through the MAC Algorithm in the order described in Table 4, the length of the resulting MAC value, depending by the MAC algorithm selected, shall be truncated as indicated in IEC 62351-5:2023, 8.3.5.4.5 (see also Figure 5).

Table 4 – Session Initiation Request: data Included in MAC calculation (in order)

Data	Description	Described in	Source
Control Direction Session Key See NOTE below	The key used to authenticate data from the controlling station.	IEC 62351-5:2023, Table 2	The last Session Key Change procedure successfully performed (IEC 62351-5:2023, subclause 8.4)
Monitoring Direction Session Key See NOTE below	The key used to authenticate data from the controlled station.	IEC 62351-5:2023, Table 2	The last Session Key Change procedure successfully performed (IEC 62351-5:2023, subclause 8.4)
Session Initiation Request values	The entire Session Initiation Request message being transmitted up to and including CGD (excluding the MAC field).	5.4.3.8	Session Initiation Request
Padding data	Additional padding data required by the MAC algorithm.	Algorithm specification.	Required by algorithm.
NOTE The monitoring and control direction session keys are included in the MAC calculation even they are marked invalid.			

MAC:= OS8i[1..8i]; i:= as specified in MAL of the Update Key Change Request message most recently received, defined in IEC 62351-5:2023, 8.3.5.4.5.

5.4.3.9 TYPE IDENT 86: S_SQ_NA_1 Session Request

5.4.3.9.1 General

The structure of this ASDU is defined in Figure 12.

Single information object (SQ=0)

0 1 0 1 0 1 1 0	TYPE IDENTIFICATION	DATA UNIT IDENTIFIER Defined in 7.1 of IEC 60870-5-101:2003
0 0 0 0 0 0 0 1	VARIABLE STRUCTURE QUALIFIER	
Defined in 7.2.3 of IEC 60870-5-101:2003	CAUSE OF TRANSMISSION	
Defined in 7.2.4 of IEC 60870-5-101:2003	COMMON ADDRESS OF ASDU	
FIN FIR ASN	ASDU Segmentation Control, defined in 5.4.2.5	
Value Value	AIM = Controlling station Association ID, defined in 8.4.2.2.2 of IEC 62351-5:2023	INFORMATION OBJECT
Value Value	AIS = Controlled station Association ID, defined in 8.4.2.2.3 of IEC 62351-5:2023	
Value Value	PRI = Protocol Information, defined in 8.4.2.2.4 of IEC 62351-5:2023 and defined in 5.4.3.9.2	
Value	CGL = Controlling station random data length, defined in 8.4.2.2.5 of IEC 62351-5:2023	
Number of octets in CGL	CGD = Controlling station random data, defined in 8.4.2.2.6 of IEC 62351-5:2023	

Figure 12 – ASDU: S_SQ_NA_1 Session Request

S_SQ_NA_1:= CP{Data Unit Identifier, AIM, AIS, PRI, CGL, Controlling station random data}

CAUSES OF TRANSMISSION used with
TYPE IDENT 86:= S_SQ_NA_1

CAUSE OF TRANSMISSION

In control direction:

<15>:= maintenance of session key

In monitor direction:

Not permitted

5.4.3.9.2 Protocol information

5.4.3.9.2.1 General

The controlling station uses this field to provide protocol information, including the protocol version, it intends to use to the controlled station. Figure 13 illustrates the structure of this field.

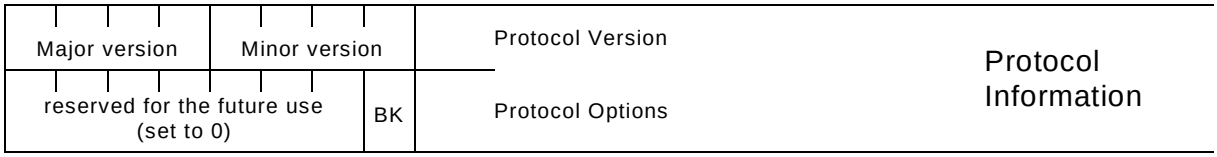


Figure 13 – Session Request PRI field

5.4.3.9.2.2 Protocol version: minor version

Minor Version:= UI4[1-4]<0..15>

Devices claiming conformance to this document shall set this value to 0

5.4.3.9.2.3 Protocol version: major version

Major Version:= UI4[5-8]<0..15>

Devices claiming conformance to this document shall set this value to 1

5.4.3.9.2.4 Broadcast session key indication: BK (IEC 60870-5-101 only)

With this flag the controlling station indicates to the controlled station the type of session key (Monitor Direction and Control Direction Session Keys or Broadcast Session Key) is initialized or changed in the Session Key Change procedure being executed. If broadcast messages are not supported or not used, the value of this flag shall be set to 0. If this security mechanism is applied to IEC 60870-5-104 the value of this flag shall be always set to 0.

BK:= BS1[1]<0..1>

<0>:= Control Direction and Monitor Direction Session Keys

<1>:= Broadcast Session Key

5.4.3.10 TYPE IDENT 87: S_SP_NA_1 Session Response

5.4.3.10.1 General

The structure of this ASDU is defined in Figure 14.

Single information object (SQ=0)

0 1 0 1 0 1 1 1	TYPE IDENTIFICATION	DATA UNIT IDENTIFIER Defined in 7.1 of IEC 60870-5-101:2003
0 0 0 0 0 0 0 1	VARIABLE STRUCTURE QUALIFIER	
Defined in 7.2.3 of IEC 60870-5-101:2003	CAUSE OF TRANSMISSION	
Defined in 7.2.4 of IEC 60870-5-101:2003	COMMON ADDRESS OF ASDU	
FIN FIR ASN	ASDU Segmentation Control, defined in 5.4.2.5	INFORMATION OBJECT
Value	AIM = Controlling station Association ID, defined in 8.4.2.3.2 of IEC 62351-5:2023	
Value		
Value	AIS = Controlled station Association ID, defined in 8.4.2.3.3 of IEC 62351-5:2023	
Value		
Value	CGL = Controlled station random data length, defined in 8.4.2.3.4 of IEC 62351-5:2023	
Value		
Number of octets specified in CGL	CGD = Controlled station random data, defined in 8.4.2.3.5 of IEC 62351-5:2023	
Number of octets specified by the MAC algorithm (MAL) selected in the Update Key Change Request message, described in 8.3.5.4.5 of IEC 62351-5:2023	MAC = Message Authentication Code, defined in 5.4.3.10.2 and in 5.4.3.1 of this document	

Figure 14 – ASDU: S_SP_NA_1 Session Response

S_SP_NA_1:= CP{Data Unit Identifier, AIM, AIS, CGL, Controlled station random data}

CAUSES OF TRANSMISSION used with
TYPE IDENT 87:= S_SP_NA_1

CAUSE OF TRANSMISSION

In control direction:

Not permitted

In monitor direction:

<15>:= maintenance of session key

5.4.3.10.2 MAC calculation in the Session Key Response message

If the Session Key Change procedure currently running has not been solicited by the controlled station, the MAC value in the Session Response message shall be calculated including the data as listed in Table 20 of IEC 62351-5:2023, 8.4.2.3.6.

Instead, if the Session Key Change procedure currently running has been solicited by the controlled station, through the Session Initiation Request described in 5.4.3.8, the MAC value in the Session Response message shall be calculated including the data as listed in Table 5 that follows (see also Figure 5).

Table 5 – Session Response: data Included in MAC calculation (in order)

Data	Description	Described in	Source
Session Request values	The entire Session Request message most recently received.	Subclause 5.4.3.9	Session Request
Session Response values	The entire Session Response message being transmitted up to and including CGD (excluding the MAC field).	Subclause 5.4.3.10	Session Response
Session Initiation Request values	The entire Session Initiation Request message most recently transmitted.	Subclause 5.4.3.8	Session Initiation Request
Padding data	Additional padding data required by the MAC algorithm.	Algorithm specification.	Required by algorithm.

5.4.3.11 TYPE IDENT 88: S_KH_NA_1 Session Key Change Request

5.4.3.11.1 General

The structure of this ASDU is defined in Figure 15.

Single information object (SQ=0)

0 1 0 1 1 0 0 0	TYPE IDENTIFICATION	DATA UNIT IDENTIFIER Defined in 7.1 of IEC 60870-5-101:2003
0 0 0 0 0 0 0 1	VARIABLE STRUCTURE QUALIFIER	
Defined in 7.2.3 of IEC 60870-5-101:2003	CAUSE OF TRANSMISSION	
Defined in 7.2.4 of IEC 60870-5-101:2003	COMMON ADDRESS OF ASDU	
FIN FIR ASN	ASDU Segmentation Control, defined in 5.4.2.5	
Value Value	AIM = Controlling station Association ID, defined in 8.4.2.4.2 of IEC 62351-5:2023	INFORMATION OBJECT
Value Value	AIS = Controlled station Association ID, defined in 8.4.2.4.3 of IEC 62351-5:2023	
Enumerated value	DPA = Data Protection Algorithm, defined in 8.4.2.4.4 of IEC 62351-5:2023	
Value Value	WKL = Wrapped key data length, defined in 8.4.2.4.5 of IEC 62351-5:2023	
Number of octets specified in WKL	WKD = Wrapped key data, defined in 8.4.2.4.6 of IEC 62351-5:2023 and in 5.4.3.11.2	
Number of octets specified by the MAC algorithm (MAL) selected in the Update Key Change Request message, described in 8.3.5.4.5 of IEC 62351-5:2023	MAC = Message Authentication Code, defined in 8.4.2.4.7 of IEC 62351-5:2023 and in 5.4.3.1	

Figure 15 – ASDU: S_KH_NA_1 Session Key Change Request

S_KH_NA_1:= CP{Data Unit Identifier, AIM, AIS, DPA, WKL, Wrapped key data, Message authentication code}

CAUSES OF TRANSMISSION used with
TYPE IDENT 88:= S_KH_NA_1

CAUSE OF TRANSMISSION

In control direction:

<15>:= maintenance of session key

In monitor direction:

Not permitted

5.4.3.11.2 Wrapped Key Data content for Broadcast Session Key change (IEC 60870-5-101 only)

According to IEC 62351-5, 8.4.2.4.6, the Session Keys shall be wrapped in the WKD field of the Session Key Change message. If the Session Key Change procedure is performed to initialize or change the Broadcast Session Key, the controlling station shall pass the data through the Key Wrap Algorithm in the order described in Table 6.

Table 6 – Data Included in WKD for Broadcast Session Key change (in order)

Data	Description	Described in	Source
Current Broadcast Session Key	The key currently used to protect data in the Secure Data messages with broadcast common address transmitted from the controlling station.	5.3.4.2	Generated by the controlling station
New Broadcast Session Key	The new key that will be used to protect data in the next Secure Data messages with broadcast common address that will be transmitted from the controlling station.	5.3.4.2	Generated by the controlling station
Padding data	As required by the key wrap algorithm.	Algorithm specification.	Required by algorithm.

During the Broadcast Session Key distribution phase, the controlling station shall always transmit the Current Broadcast Session Key and the New Broadcast Session Key.

Once the Broadcast Session Key distribution phase is completed, the controlling station shall invalidate the Current Broadcast Session Key and replace it with the New Broadcast Session Key transmitted; the New Broadcast Session Key value (all octets) is then set to 0 (zero)

When no Broadcast Session Key is available (not previously generated) on the controlling station (for example, at the first startup), the controlling station shall derive and provide the first Broadcast Session key as the Current Broadcast Session Key value in this field, while the New Broadcast Session Key value (all octets) shall be set to 0 (zero) in this field. Depending by the application, the controlling station may or may not send Broadcast Secure Data messages before that the distribution of this first Broadcast Session Key is completed.

If the controlled stations receives both Current Broadcast Session Keys and New Broadcast Session Key in this message, the controlled station shall consider both keys valid and applicable to the subsequent broadcast Secure Data message received. When the controlled station receives the first broadcast Secure Data Message protected with the New Broadcast Session Key received, the controlled station shall invalidate the Current Broadcast Session Key and apply the New Broadcast Session Key to all subsequent broadcast Secure Data messages received.

If the controlled station receives the New Broadcast Session Key value set to 0, the controlled station shall apply only the Current Broadcast Session Key value immediately to the subsequent broadcast Secure Data messages received.

Figure 16 and Figure 17 show Examples of an initial Broadcast Session Key distribution and of the Broadcast Session Key update procedures and utilize the following abbreviations:

- SC Key – Control Direction Session Key;
- SM Key – Monitoring Direction Session Key;
- BCx Key – Broadcast Session Key for the BC Key use period x;
- TX – Transmitted message;
- RX – Received message.

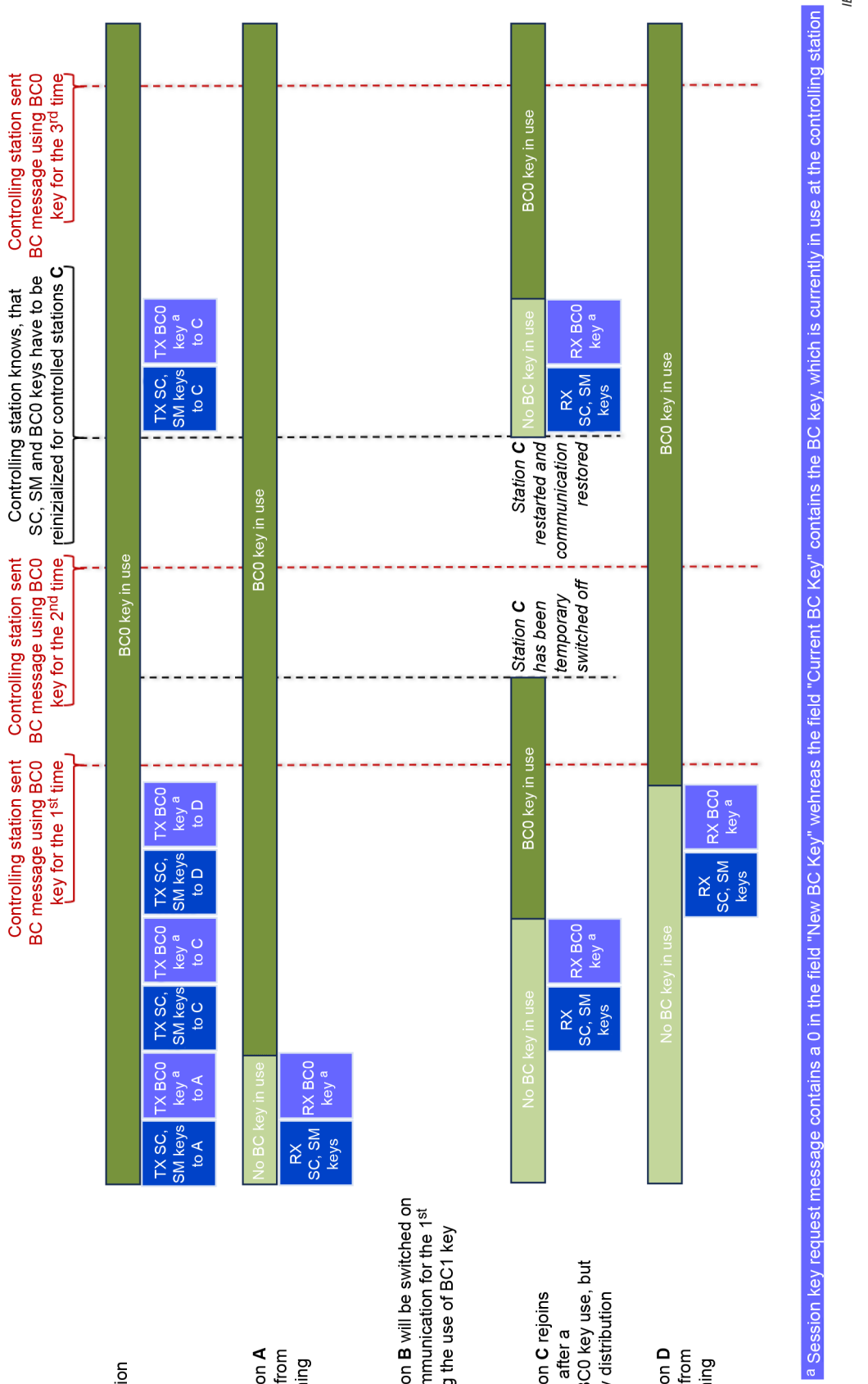


Figure 16 – Example of an initial Broadcast Session Key distribution

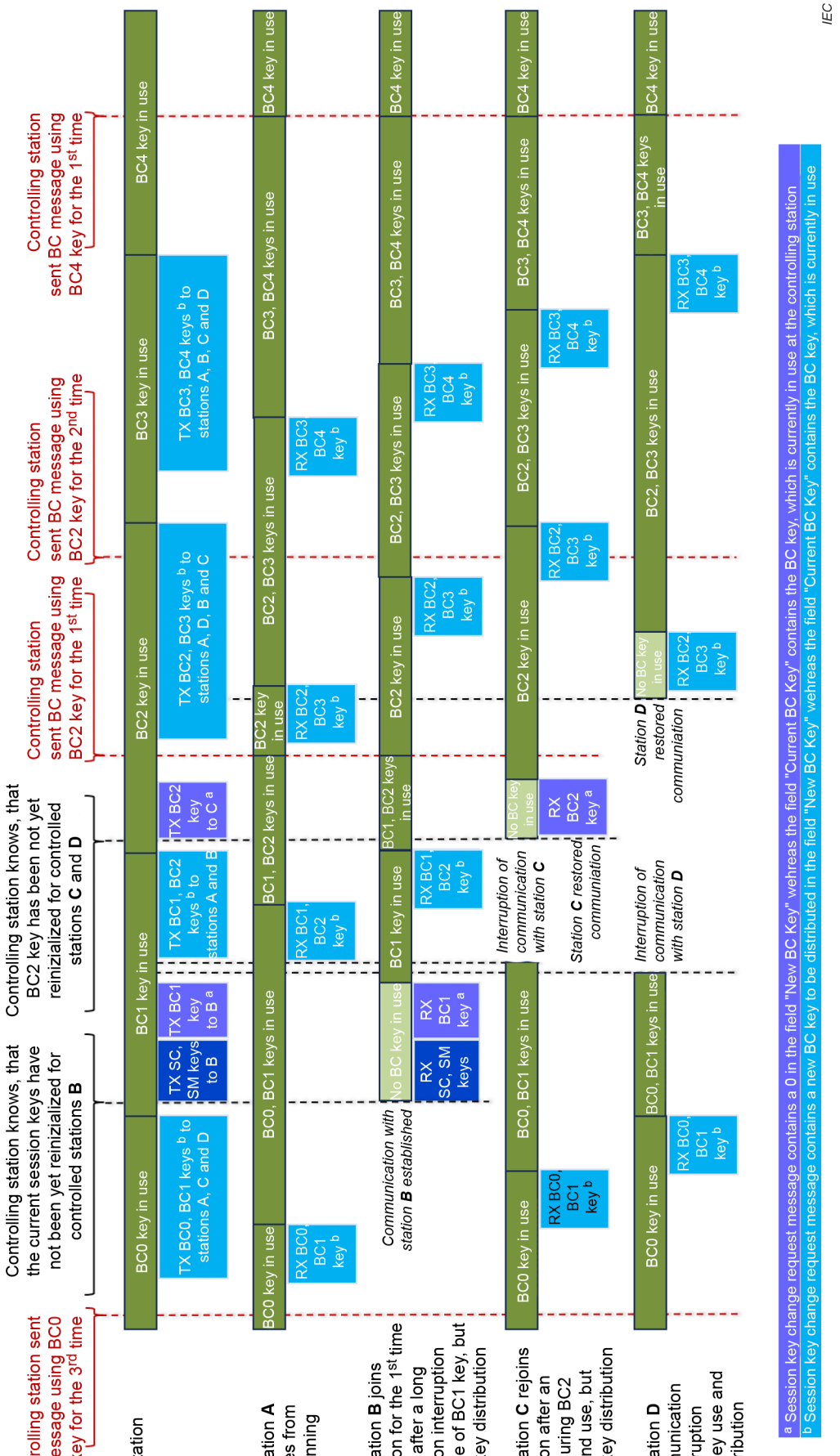


Figure 17 – Examples of Broadcast Session Key update

5.4.3.12 TYPE IDENT 89: S_KP_NA_1 Session Key Change Response

The structure of this ASDU is defined in Figure 18**.**

Single information object (SQ=0)

0 1 0 1 1 0 0 1	TYPE IDENTIFICATION	DATA UNIT IDENTIFIER Defined in 7.1 of IEC 60870-5-101:2003
0 0 0 0 0 0 0 1	VARIABLE STRUCTURE QUALIFIER	
Defined in 7.2.3 of IEC 60870-5-101:2003	CAUSE OF TRANSMISSION	
Defined in 7.2.4 of IEC 60870-5-101:2003	COMMON ADDRESS OF ASDU	
FIN FIR ASN	ASDU Segmentation Control, defined in 5.4.2.5	
Value	AIM = Controlling station Association ID, defined in 8.4.2.5.2 of IEC 62351-5:2023	INFORMATION OBJECT
Value		
Value	AIS = Controlled station Association ID, defined in 8.4.2.5.3 of IEC 62351-5:2023	
Value		
Number of octets specified by the MAC algorithm (MAL) selected in the Update Key Change Request message, described in 8.3.5.4.5 of IEC 62351-5:2023	MAC = Message Authentication Code, defined in 8.4.2.5.4 of IEC 62351-5:2023 and in 5.4.3.1 of this document	

Figure 18 – ASDU: S_KP_NA_1 Session Key Change Response

S_KP_NA_1:= CP{Data Unit Identifier, AIM, AIS, Message authentication code}

CAUSES OF TRANSMISSION used with
TYPE IDENT 89:= S_KP_NA_1

CAUSE OF TRANSMISSION

In control direction:

Not permitted

In monitor direction:

<15>:= maintenance of session key

5.4.3.13 TYPE IDENT 91: S_SD_NA_1 Secure Data

The structure of this ASDU is defined in Figure 19.

If the MAC algorithm is used to protect the Secure Data message, the MAC calculation shall start with and include the Data Unit Identifier defined in this sub-clause before the Secure Data message as described in Table 29 of IEC 62351-5:2023. An example is shown in Figure 5 as it applies to all messages with integrity protection.

If the AEAD algorithm is used to protect the Secure Data message, the Data Unit Identifier defined in this sub-clause shall be included as Additional Data parameter before the AIM and AIS fields concatenated as described in Table 32 of IEC 62351-5:2023.

An example is provided for the AEAD calculation of a Secure Data message following the explanation above:

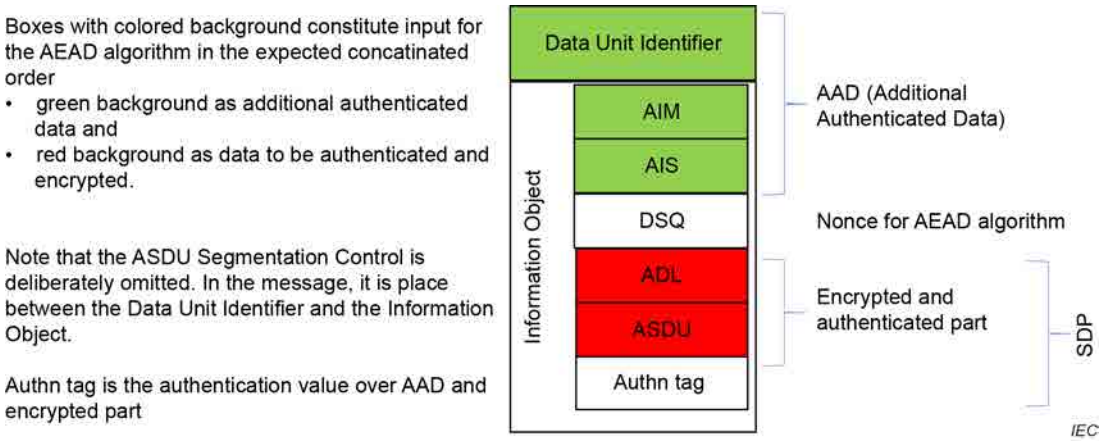


Figure 19 – Example of an AEAD calculation of a Secure Data message

NOTE This picture is also provided as tissue to IEC 62351-5:2023 for integration to have a visualization of the intended packet processing. This is intended to support an interoperable implementation.

Single information object (SQ=0)

0 1 0 1 1 0 1 1	TYPE IDENTIFICATION	DATA UNIT IDENTIFIER Defined in 7.1 of IEC 60870-5-101:2003
0 0 0 0 0 0 0 1	VARIABLE STRUCTURE QUALIFIER	
Defined in 7.2.3 of IEC 60870-5-101:2003	CAUSE OF TRANSMISSION	
Defined in 7.2.4 of IEC 60870-5-101:2003	COMMON ADDRESS OF ASDU	
FIN FIR ASN	ASDU Segmentation Control, defined in 5.4.2.5	INFORMATION OBJECT
Value	AIM = Controlling station Association ID, defined in 8.5.2.2.2 of IEC 62351-5:2023	
Value		
Value	AIS = Controlled station Association ID, defined in 8.5.2.2.3 of IEC 62351-5:2023	
Value		
Value	DSQ = Data Sequence Number, defined in 8.5.2.2.4 of IEC 62351-5:2023	
Value		
Value		
Value		
Value	ADL = Application Data Length, defined in 8.5.2.2.5 of IEC 62351-5:2023	
Value		
Number of octets specified in ADL	SDP = Secure Data Payload, defined in 8.5.2.2.6 of IEC 62351-5:2023	

Figure 20 – ASDU: S_SD_NA_1 Secure Data

S_SD_NA_1:= CP{Data Unit Identifier, AIM, AIS, DSQ, ADL, Secure data payload}

CAUSES OF TRANSMISSION used with
TYPE IDENT 91:= S_SD_NA_1

CAUSE OF TRANSMISSION

In control direction:

<14>:= application data protection

In monitor direction:

<14>:= application data protection

6 T-Profile Security: Implementation of IEC 62351-3

This clause specifies the T-Profile security, which provides security for TCP/IP based communication. T-Profile security relies on the application of IEC 62351-3:2023, profiling the use of TLS to protect TCP/IP based communication. TLS parameters like cipher suites, parameters for session renegotiation and session resumptions as well as certificate handling are defined in IEC 62351-3:2023.

The stand-alone application of the T-Profile is foreseen in use cases in which only IEC 60870-5-104 is applied and there is a direct connection between the controlling station and controlled station.

If the T-Profile is used stand-alone, RBAC may be achieved by including the access token information in the X.509 public key certificate (IEC 62351-8 Profile A) or in a X.509 attribute certificate (IEC 62351-8 Profile B) in the context of the TLS handshake.

7 Security profiles for IEC 60870-5-101 and IEC 60870-5-104

7.1 General

This clause describes how A-Profile (described in Clause 5) and T-Profile (described in Clause 6) are applied in IEC 60870-5-101 and IEC 60870-5-104 communication.

Devices claiming conformance to this document shall permit each security profile implemented (A-Profile, T-Profile) to be enabled or disabled separately by configuration options.

7.2 Security profiles for IEC 60870-5-101

Devices implementing IEC 60870-5-101 communication, and claiming conformance to this document, shall support the A-Profile described in Clause 5 of this document.

NOTE For IEC 60870-5-101 security, the T-profile is not applicable, only the A-Profile security described in Clause 5 can be applied.

7.3 Security profiles for IEC 60870-5-104

7.3.1 General

For IEC 60870-5-104 security, which is a TCP/IP based communication, both A-Profile security described in Clause 5 and T-Profile security described in Clause 6 are applicable as follows.

Devices implementing IEC 60870-5-104 communication, and claiming conformance to this standard, shall support the T-Profile security described in Clause 6.

For devices implementing IEC 60870-5-104 communication, the support of A-Profile security described in Clause 5 is optional.

To ensure interoperability between devices and flexibility against the organizations security policy, the support of both A-Profile security and T-Profile security is highly recommended.

Devices claiming conformance to IEC 60870-5-104 T-Profile security and T-Profile security is enabled by configuration shall use the TCP port number 19998 by default to initiate secure connections. Other port may optionally be used by configuration, depending on the organisation security policy.

IEC 60870-5-104 implementations that do not support the T-Profile security or where T-Profile security is disabled by configuration, shall continue to use port 2404 by default as specified in IEC 60870-5-104.

7.3.2 Use with redundant channels

When redundant channels are used with the A-Profile in IEC 60870-5-104, the A-Profile cryptographic information are shared by all connections within the associated redundancy group.

When redundant channels are used with the T-Profile in IEC 60870-5-104, each single TLS connection in a redundancy group is considered to be independent. TLS connections between the same stations in the same redundancy group may use TLS session resumption to optimize the connection setup.

IEC 60870-5-104 APCI messages such as test frames cannot be authenticated; only ASDUs shall be authenticated. Therefore, when data on a connection is stopped and only test frames are being exchanged, the stations shall not transmit authentication messages.

8 Considerations for role-based access control (RBAC)

8.1 General

This clause defines the RBAC handling for IEC 60870-5 telecontrol systems. It relates to the already pre-defined roles (see IEC 62351-8) and the assigned permissions (see IEC 62351-5:2023). While IEC 62351-5:2023 defines the role-to-permission mapping, the permissions themselves are not specified. IEC 62351-8 does not define the mapping for this document.

Figure 21 visualizes the interrelation between the IEC 60870-5-101/-104 specific roles and permissions taking the IEC 62351-8 approach.

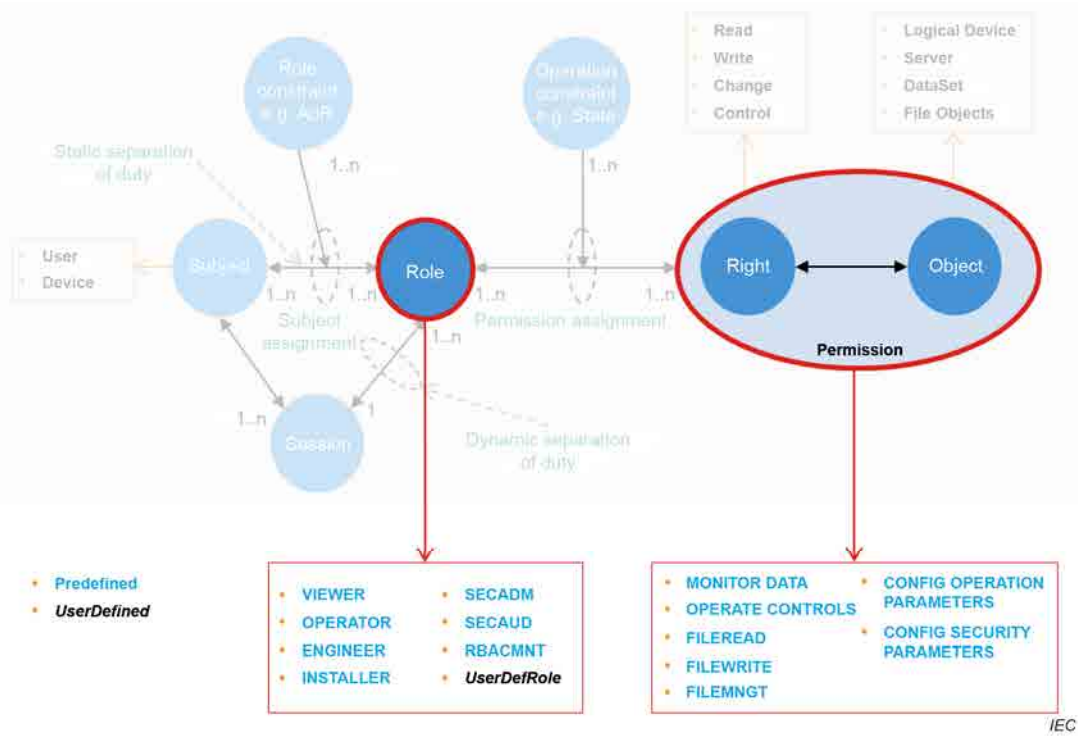


Figure 21 – RBAC mapped to IEC 60870-5-101/-104

To achieve interoperability, it is necessary to define the permissions but also potential constraints of the permissions, depending on the objects they are assigned to.

IEC 62351-8 defines different approaches to handle constraints depending on the objects, which may be used by the referencing standards. These approaches relate to the definition of specific `permissions` as rights-on-objects or the definition of so-called `operationSets`, which bind roles and selected permissions for later assignment to objects. Based on the simplicity of the underlying data model, this document considers the verbal description of the constraints as sufficient for implementation, as noted in 8.3.

8.2 Permission definition

The permissions defined in this subclause are defined based on the IEC 60870-5-7 data model. The description follows the approach descried in IEC 62351-8. The mandatory permissions to be supported are listed in Table 7 and described below.

Table 7 – List of pre-defined permissions

Predefined permissions			
AttributeName	AttributeType	Comments	M/O M: mandatory to support but conditional, depending on the object model. Examples: – an IED without a controllable object shall not support the permission CONTROL; – an IED without a file system shall not support the permission FILE. O: optional
MONITOR DATA	BOOLEAN		M
OPERATE CONTROLS	BOOLEAN		M
FILEREAD	BOOLEAN		M
FILEWRITE	BOOLEAN		M
FILEMNGT	BOOLEAN		M
CONFIG OPERATION PARAMETERS	BOOLEAN		M
CONFIG SECURITY PARAMETERS	BOOLEAN		M

The following list described the permissions more elaborately.

– MONITOR DATA permission. Allows the subject/role to view the type of data and the runtime data values present within a device whether sent spontaneously or sent in response to a request.

– OPERATE CONTROLS permission. Allows the subject/role to request control actions (select and/or operate) to the device on all or some controllable object within a device.

– FILEREAD permission: Allows the subject/role to perform read actions on files within a device.

– FILEWRITE permission: Allows the subject/role to perform write actions on files within a device. This permission includes the FILEREAD permission.

– FILEMNGT permission: Allows the subject/role to delete existing files on a device.

– CONFIG OPERATION PARAMETERS permission. Allows the subject/role to configure process control parameters (e.g., thresholds, timeouts).

– CONFIG SECURITY PARAMETERS permission: Allows a subject/role to perform configuration on all security related parameters.

8.3 Role-to-permission assignment

IEC 62351-5:2023 already defines the roles-to-permission assignment applicable for IEC 60870-5-101/-104 based on IEC 62351-8:2020. Since IEC 62351-8:— in Edition 2[1] changes the number range for the role ID to be only in the positive range, the following table contains the role-to-permission assignments and is taken from IEC 62351-5:2023, 8.3.12.2.1, and adopted according to the changed number range in IEC 62351-8:— (Edition 2). It is provided here to better relate to the permission definition.

Table 8 – List of pre-defined role-to-permission assignments for IEC 60870-5-101/-104 (updated version from IEC 62351-5:2023)

RoleID	Role Name	Permission						
		MONITOR DATA	OPERATE CONTROLS	FILEREAD	FILEWRITE	FILEMNGT	CONFIG OPERATION	CONFIG SECURITY
<0>	VIEWER	X		C_1				
<1>	OPERATOR	X	X	C_1				
<2>	ENGINEER	X		C_2	C_2	C_2	X	
<3>	INSTALLER	X		C_3	C_3		X	
<4>	SECADM			C_5	C_5	C_5		X
<5>	SECAUD			C_4				
<6>	RBACMNT			C_5	C_5	C_5		X
<7...255>	Reserved for IEC usage for potential further pre-defined role definitions IEC 62351-8.							
<256...32767>	Reserved for definitions of roles in referencing documents or custom defined roles.							

C_1 = Conditional read access to files of other filetypes than listed above

C_2 = Access to files of type data and config

C_3 = Access to files of type config and firmware (updates)

C_4 = Access to files of type audit log

C_5 = Access to files of type security (config)

Note that the number range <-32768 ... -1> originally stated in IEC 62351-5 is omitted here as IEC 62351-8:— (Edition 2) relaxes the requirements for using the `roleIDs`. This relaxation was introduced, as the uniqueness of roles is already ensured by the triplet of `roleID`, `roleDefinition`, and `revision`. These values are already defined in IEC 62351-5:2023.

[1] Under preparation. Stage at the time of publication: IEC/ACDV 62351-8:2024.

It is expected that implementors of this document will respect the permissions defined in Table 8 when determining what protocol services are performed by devices when operating in the various Roles defined here. For example, the VIEWER role may be permitted to issue interrogation commands and to receive spontaneous data. It is up to the implementor to determine if each role may allow additional functions such as setting the controlled station clock to be permitted. It might be necessary for all roles to be able to perform basic protocol housekeeping to permit establishment of communication between the controlling station and controlled station.

9 Protocol Implementation Conformance Statement

9.1 Overview of clause

Devices claiming conformance to this document shall supply the information in this clause on request. An "X" in a box means that the implementation supports the listed feature. A distinction is made if the A-profile is used over a serial link (A-profile alone) or over a TCP/IP link (A-profile combined with T-profile).

9.2 Algorithms for digital certificates

9.2.1 Cryptographic curves for key pair generation

☐ Curve 25519 (mandatory)

☐ Curve 448 (mandatory)

☐ SECP256k1 (mandatory)

☐ SECP256r1 (mandatory)

☐ BrainpoolP256r1 (optional)

☐ Other

9.2.2 Certificate signature algorithms

☐ ECDSA-with-SHA256 (mandatory)

- ☐ SECP256k1 (mandatory)
- ☐ SECP256r1 (mandatory)
- ☐ BrainpoolP256r1 (optional)
- ☐ Other

☐ RSA-2048-with-SHA256 (mandatory)

☐ Other

9.3 MAC algorithms

9.3.1 General

These are the MAC algorithms to be used in the station association procedure and the session key change procedure.

9.3.2 MAC algorithms for serial links

☐ HMAC-SHA256 truncated to 8 octets (mandatory)

☐ HMAC-SHA3-256 truncated to 8 octets

☐ BLAKE2s-256 truncated to 8 octets

☐ Other _____

9.3.3 MAC algorithms for TCP/IP links

☐ HMAC-SHA-256 truncated to 16 octets (mandatory)

☐ HMAC-SHA3-256 truncated to 16 octets

☐ BLAKE2s-256 truncated to 16 octets

☐ Other _____

9.4 Key wrap algorithms

☐ AES-256 Key Wrap (mandatory)

☐ Other _____

9.5 Data protection algorithms

9.5.1 General

These are the data protection algorithms to be used in the secure data exchange procedure.

9.5.2 Data protection algorithms for serial links

☐ HMAC-SHA-256 truncated to 8 octets (mandatory)

☐ HMAC-SHA3-256 truncated to 8 octets

☐ BLAKE2s-256 truncated to 8 octets

☐ AEAD-AES-256-GCM encryption

☐ Other _____

9.5.3 Data protection algorithms for TCP/IP links

☐ HMAC-SHA-256 truncated to 16 octets (mandatory)

☐ HMAC-SHA3-256 truncated to 16 octets

☐ BLAKE2s-256 truncated to 16 octets

☐ AEAD-AES-256-GCM encryption

☐ Other _____

9.6 Configurable parameters

The default values defined in the following Table may be changed according to the organization security policy. Implementations claiming conformance to this specification shall allow configuration of the parameters listed in Table 9.

Table 9 – List of the configurable parameters

Parameter	Configured at station	Default value according to IEC 62351-5: 2023
Remote station's public key[1)]	Both	NA
Expected Reply Time	Controlling	2 s
Expected Request Time[4)]	Controlled	6 s
Max Session Key Usage Time[2)]	Both	Recommended range between 24 h and 1 week
Max Session Key Usage Count[3)]	Both	Recommended range between 2^{16}-1 and 2^{31}-1
Max Broadcast Session Key Usage Time[5)]	Both	Recommended range between 24 h and 1 week
Max Broadcast Session Key Usage Count[6)]	Both	Recommended range between 2^{16}-1 and 2^{31}-1
Max Reply Timeout	Controlling	3
Authorized remote stations	Both	NA
Disable secure communication	Both	off

1) Only applicable if self-signed certificates are used

2) In order that the controlled station does not invalidate the current Session Keys before the controlling station changes the Session Keys, it is recommended that the value of the controlled station Max Session Key Usage Time is set to be double the value of the Max Session Key Usage Time set in the controlling station. The recommended range given is for the controlling station.

3) In order that the controlled station does not invalidate the current Session Keys before the controlling station changes the Session Keys, it is recommended that the value of the controlled station Max Session Key Usage Count is set to be double the value of the Max Session Key Usage Count set in the controlling station. The recommended range given is for the controlling station. In case if the Max. Session Key Usage Time is disabled, this value shall be chosen to ensure that the session keys are changed at least every 1 week (based on the estimated number of the messages usually transmitted in this application in accordance with the recommendations for the Max Session Key Usage Time).

4) As noted in IEC 62351-5:2023 the value of the Expected Request Time should be the value of Expected Reply Time multiplied by Max Reply Timeouts.

5) In order that the controlled station does not invalidate the current Broadcast Session Keys before the controlling station changes the Broadcast Session Keys, it is recommended that the value of the controlled station Max Broadcast Session Key Usage Time is set to be double the value of the Max Broadcast Session Key Usage Time set in the controlling station. The recommended range given is for the controlling station.

6) In order that the controlled station does not invalidate the current Broadcast Session Keys before the controlling station changes the Broadcast Session Keys, it is recommended that the value of the controlled station Max Broadcast Session Key Usage Count is set to be double the value of the Max Broadcast Session Key Usage Count set in the controlling station. The recommended range given is for the controlling station. In case if the Max. Broadcast Session Key Usage Time is disabled, this value shall be chosen to ensure that the session keys are changed at least every 1 week (based on the estimated number of the messages usually transmitted in this application in accordance with the recommendations for the Max Broadcast Session Key Usage Time).

9.7 Configurable statistic thresholds and statistic information object addresses

The default values defined in Table 10 may be changed according to the organization security policy.

Table 10 – Security statistic

Security Statistic Counter	Station type	Default value of statistic threshold (per IEC 62351-5:2023)	Configured value of statistic threshold	Information object address of the integrated total for the statistic
Successful Station Associations	Controlling and Controlled	1		
Station Association Failures	Controlling and Controlled	1		
Successful Session Key Changes	Controlling and Controlled	10		
Session Key Change Failures	Controlling and Controlled	1		
Session Key Invalidations due Max Session Key Usage Time expired	Controlled	1		
Session Key Invalidations due Max Session Key Usage Count reached.	Controlled	1		
Protocol Information Errors	Controlled	1		
Key Authentication Algorithm Support Failures	Controlled	1		
Key Wrap Algorithm Support Failures	Controlled	1		
Data Protection Algorithm Support Failures	Controlled	1		
Key Authentication Errors	Controlling and Controlled	1		
Data Authentication Errors	Controlling and Controlled	1		
Unexpected Messages	Controlling and Controlled	10		
Max Reply Timeouts	Controlling	1		
Remote Station's Authorization Failures.	Controlling and Controlled	1		
Operation Authorization Failures	Controlled	1		
Remote Station's Certificate Validity Check Failures.	Controlling and Controlled	1		
Remote Station's Certificate Expirations.	Controlling and Controlled	1		
Remote Station's Certificate Revocations.	Controlling and Controlled	1		
Local Station's Certificate Expirations.	Controlling and Controlled	1		
Local Station's Certificate Revocations.	Controlling and Controlled	1		

Security Statistic Counter	Station type	Default value of statistic threshold (per IEC 62351-5:2023)	Configured value of statistic threshold	Information object address of the integrated total for the statistic
Cryptographic Keys Invalidations due to Remote Station's Certificate Revocation.	Controlling and Controlled	1		
Cryptographic Keys Invalidations due to Local Station's Certificate Revocation;	Controlling and Controlled	1		
Successful Data Authentications	Controlling and Controlled	100		
Reply Timeouts	Controlling	3		
Request Timeouts	Controlled	1		
Total Messages Sent	Controlling and Controlled	500		
Total Messages Received	Controlling and Controlled	500		
Discarded Messages	Controlling and Controlled	10		
NOTE 1 On the controlled station, if the threshold is reached the security statistic will be reported to the controlling station using ASDU Type 37: Integrated totals with time tag CP56Time2a as described in 5.4.2.3. NOTE 2 Consider the implications of clock synchronization discussed in Annex B.				

9.8 Security profile support

☐ A-Profile (mandatory to protect IEC 60870-5-101 communication, see Clause 5)

☐ A-Profile (optional to protect IEC 60870-5-104 communication, see Clause 5)

☐ T-Profile (mandatory to protect IEC 60870-5-104 communication, see Clause 6)

Annex A
(informative)

Implementation of A-Profile security with IEC 60870-5-101

This informative Annex A describes a high-level view on the implementation of the A-Profile security for balanced and unbalanced transmission procedures between controlling (primary) and controlled (secondary) stations according to IEC 60870-5-101.

In unbalanced transmission systems, controlled stations are always secondary and controlling stations are always primary. For unbalanced transmission procedures, the primary station contains only a primary link layer and the secondary station contains only a secondary link layer (see Figure A.1).

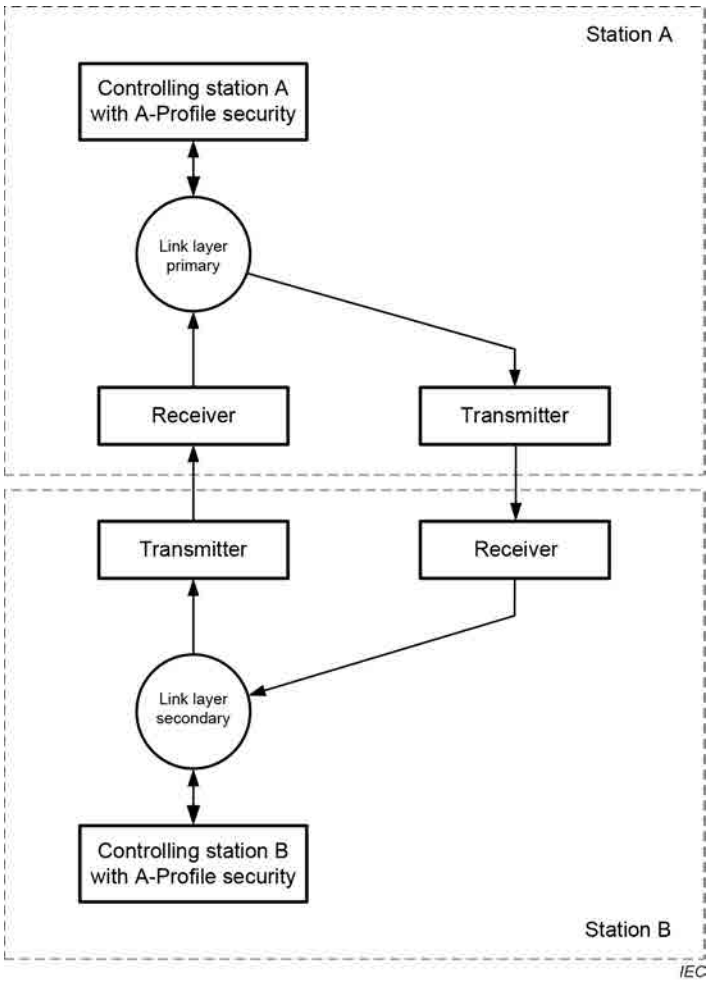


Figure A.1 – Unbalanced transmission system

NOTE 1 Currently A-Profile security does not cover security for broadcast transmission to the secondary stations in the unbalanced point-to-multipoint transmission procedures.

NOTE 2 The secondary stations are not able to solicit the primary station to initiate a session key change by sending the session initiation request message.

The link layers for balanced transmission procedures consist of two decoupled logical processes, one logical process represents station A as the primary station and station B as the secondary station and the other logical process represents station B as the primary station and station A as the secondary station (each station is a combined station with separate controlling and controlled parts with its own independent A-Profiles). Thus, two independent processes exist in each station to control the link layer in the logical primary and in the secondary direction. Figure A.2 shows the typical arrangement of the link layer using balanced transmission procedures.

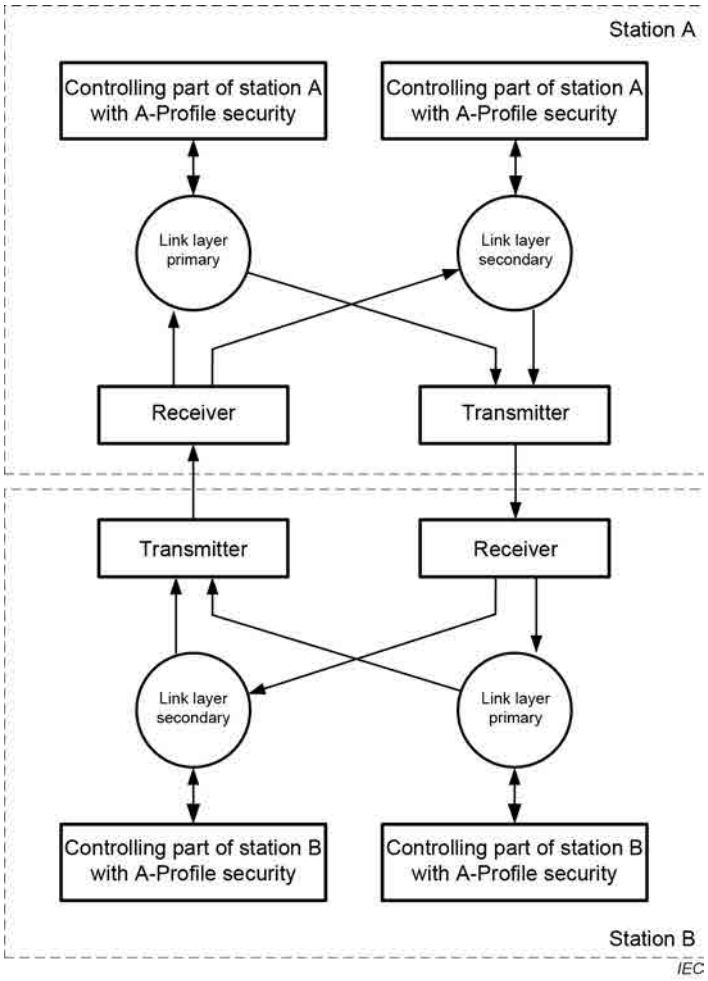


Figure A.2 – Balanced transmission system

Annex B
(informative)

Devices with inaccurate clocks

Certificates have a validity period (a time/date before which it is not valid and a time/date after which it is not valid).

The security mechanisms described in this document depend on certificates and devices implementing this document are required to verify the validity of these certificates.

Some automation devices, especially controlled stations, may have limited capability to maintain a local clock that is accurately synchronized in a secure manner to the correct time. In extreme cases, devices that have no need to report time tagged data might have no clock.

Where a device is unable to ensure that it has an accurate local clock, it may ignore the validity period of a certificate as part of determining if a certificate should be considered valid. Please also note (as stated in IEC 62351-5:2023) that certificate expiry will not invalidate the update key. All other validation of certificates should be performed as normal.

Bibliography

IEC TS 62351-2, *Power systems management and associated information exchange – Data and communications security – Part 2: Glossary of terms*

IEC 62351-8:—[2] (Edition 2), *Power systems management and associated information exchange – Data and communications security – Part 8: Role-based access control for power system management*

_____

[2] Under preparation. Stage at the time of publication: IEC/ACDV 62351-8:2024.

This page deliberately left blank