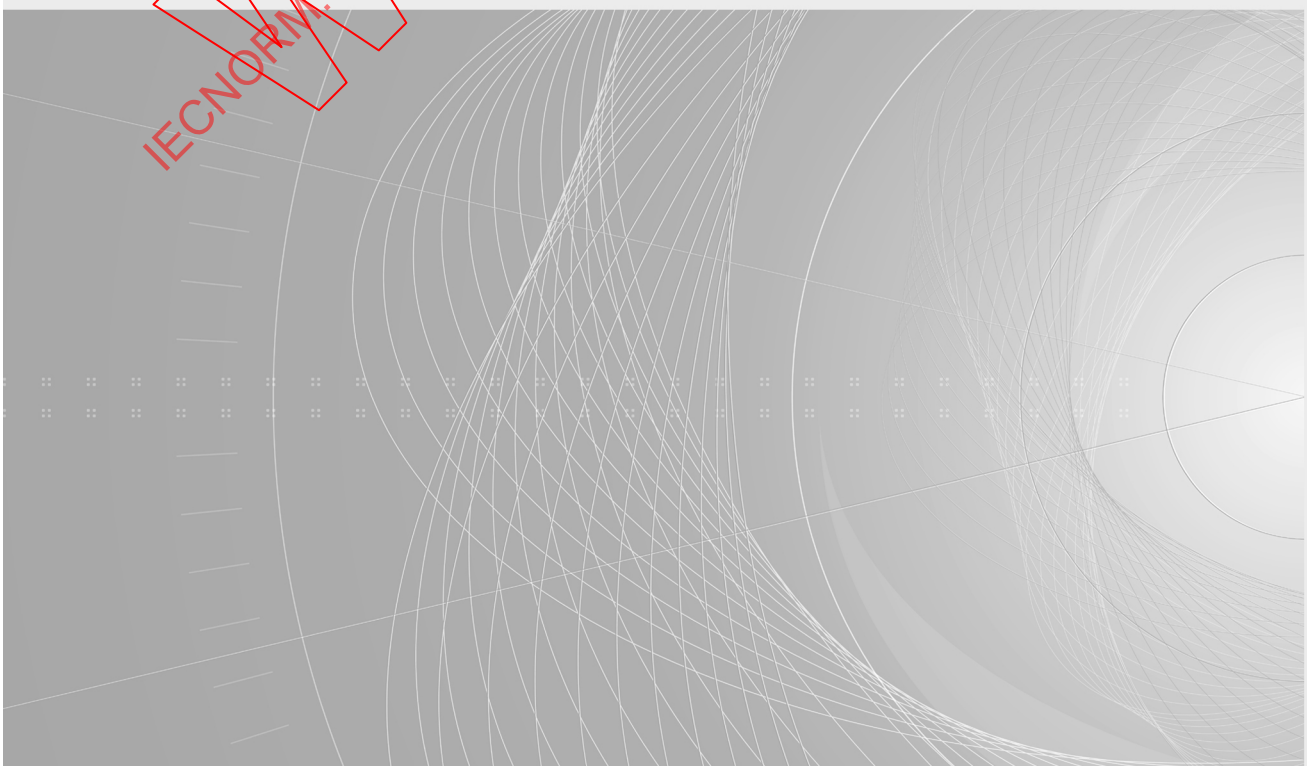
IEC/TS 62351-5

Edition 1.0 2009-08

TECHNICAL SPECIFICATION

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



IEC/TS 62351-5:2009(E)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: www.iec.ch

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

- Catalogue of IEC publications: www.iec.ch/searchpub
The IEC on-line Catalogue enables you to search by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, withdrawn and replaced publications.

- IEC Just Published: www.iec.ch/online_news/justpub
Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.

- Electropedia: www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing more than 20 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary online.

- Customer Service Centre: www.iec.ch/webstore/custserv
If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:

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

IEC/TS 62351-5

Edition 1.0 2009-08

TECHNICAL SPECIFICATION

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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

PRICE CODE XA

ICS 33.200

ISBN 978-2-88910-681-3

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

POWER SYSTEMS MANAGEMENT AND ASSOCIATED INFORMATION EXCHANGE – DATA AND COMMUNICATIONS SECURITY –

Part 5: Security for IEC 60870-5 and derivatives

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.

The main task of IEC technical committees is to prepare International Standards. In exceptional circumstances, a technical committee may propose the publication of a technical specification when

- the required support cannot be obtained for the publication of an International Standard, despite repeated efforts, or
- The subject is still under technical development or where, for any other reason, there is the future but no immediate possibility of an agreement on an International Standard.

Technical specifications are subject to review within three years of publication to decide whether they can be transformed into International Standards.

IEC 62351-5, which is a technical specification, has been prepared by IEC technical committee 57: Power systems management and associated information exchange.

The text of this technical specification is based on the following documents:

Enquiry draft	Report on voting
57/861/DTS	57/921A/RVC

Full information on the voting for the approval of this technical specification 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.

A list of all parts of the IEC 62351 series, under the general title: *Power systems management and associated information exchange – Data and communications security*, can be found on the IEC website.

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.

A bilingual version of this publication may be issued at a later date.

IMPORTANT – The "colour inside" logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this publication using a colour printer.

POWER SYSTEMS MANAGEMENT AND ASSOCIATED INFORMATION EXCHANGE – DATA AND COMMUNICATIONS SECURITY –

Part 5: Security for IEC 60870-5 and derivatives

1 Scope and object

1.1 Scope

This part of IEC 62351 specifies messages, procedures and algorithms for securing the operation of all protocols based on or derived from the standard IEC 60870-5: Telecontrol equipment and systems – Part 5: Transmission protocols. This specification applies to at least those protocols listed in Table 1.

Table 1 – Scope of application to standards

Number	Name
IEC 60870-5-101	Companion standard for basic telecontrol tasks
IEC 60870-5-102	Companion standard for the transmission of integrated totals in electric power systems
IEC 60870-5-103	Companions standard for the informative interface of protection equipment
IEC 60870-5-104	Network access for IEC 60870-5-101 using standard transport profiles
DNP3	Distributed Network Protocol (based on IEC 60870-1 through IEC 60870-5 and controlled by the DNP Users Group)

1.2 Intended audience and use

The initial audience for this specification is intended to be the members of the working groups developing the protocols listed in Table 1. For the measures described in this specification to take effect, they must be accepted and referenced by the specifications for the protocols themselves. This document is written to enable that process.

The subsequent audience for this specification is intended to be the developers of products that implement these protocols.

Portions of this specification may also be of use to managers and executives in order to understand the purpose and requirements of the work.

1.3 Items outside of scope

This part of IEC 62351 focuses only on application layer authentication and security issues arising from such authentication, per directions from IEC Technical Committee 57 Working Group 3. Other security concerns – in particular, protection from eavesdropping or man-in-the-middle attacks through the use of encryption – are considered to be outside the scope. Encryption may be added through the use of this specification with other specifications.

1.4 Use with other standards

The working groups developing the protocols listed in Table 1 may issue standards to be applied in conjunction with this specification. It is expected that these standards will describe a mapping of this authentication mechanism to the messages and procedures of each specific protocol.

Such documents shall not override any of the security measures described in this specification as mandatory and normative.

When applied to IEC 60870-5-104, this specification shall be applied in conjunction with IEC/TS 62351-3: Power systems management and associated information exchange – Data and communications security – Part 3: Communication network and system security – Profiles including TCP/IP.

1.5 Document organization and approach

This document is organized working from the general to the specific, as follows.

- Clauses 2 through 4 provide background terms, definitions, and references.
- Clause 5 describes the problems this specification is intended to address.
- Clause 6 describes the mechanism generically without reference to a specific protocol.
- Clauses 7 and 8 describe the mechanism more precisely and are the primary normative part of this specification.
- Clause 9 describes a few particular implementation issues that are special cases.
- Clause 10 describes the requirements for other standards referencing this specification
- Clause 11 describes the protocol implementation conformance statement (PICS) for this mechanism.

1.6 Compliance

Unless specifically labelled as informative or optional, all clauses of this specification are normative.

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

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

IEC 60870-5-103, *Telecontrol equipment and systems – Part 5-103: Transmission protocols - Companion standard for the informative interface of protection equipment*

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

IEC/TS 62351-1, *Power systems management and associated information exchange – Data and communications security – Part 1: Communication network and system security – Introduction to security issues*

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

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

ISO/IEC 9798-4, *Information technology – Security techniques – Entity authentication – Part 4: Mechanisms using a cryptographic check function*

FIPS 186-2, *Digital Signature Standard (DSS)*

FIPS 197, *Advanced Encryption Standard (AES)*

FIPS 198-1, *The Keyed-Hash Message Authentication Code*

RFC 2104, HMAC: *Keyed-Hashing for Message Authentication*

RFC 3174, *Secure Hash Algorithm (SHA-1)*

RFC 3394, *Advanced Encryption Standard (AES) Key Wrap Algorithm*

RFC 3629, UTF-8, *a transformation format of ISO 10646*

3 Terms and definitions

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

They are described here because they are specific to the IEC 60870-5 standards and may be useful for reading this specification as an independent document.

Refer to IEC/TS 62351-2 for a list of applicable terms and definitions.

3.1
controlling station
the device or application that initiates most of the communications and issues commands

It is commonly called a "master" in some protocol specifications.

3.2
controlled station
the remote device that transmits data gathered in the field to the controlling station

It is commonly called the "outstation" or "slave" in some protocols.

3.3
control direction
data transmitted by the controlling station to the controlled station(s)

3.4
monitoring direction
data transmitted by the controlled station to the controlling stations

The following terms are described here because they are specific to this protocol:

3.5
challenger
station that issues authentication challenges

It may be either a controlled or controlling station.

3.6
responder
station that responds or reacts to authentication challenges

It may be either a controlled or controlling station.

4 Abbreviated terms

Refer to IEC/TS 62351-2 for a list of applicable abbreviated terms. The following term is included here because it is specifically used in the affected protocols and used in the discussion of this authentication mechanism.

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

5 Problem description

5.1 Overview of clause

This clause is informative only. It describes:

- the security threats that this specification is intended to address;
- the unique design problems in implementing authentication for IEC 60870-5 and derived protocols;
- the resulting design principles behind the mechanism.

5.2 Specific threats addressed

This specification shall address only the following security threats, as defined in IEC/TS 62351-2:

- spoofing;
- modification;
- replay;
- non-repudiation – to the extent of identifying individual users of the system.

5.3 Design issues

5.3.1 Overview of subclause

This subclause describes the challenges faced in developing an authentication proposal that can be applied to all the IEC 60870-5 and derivative protocols. This subclause is supplied for the benefit of security experts reviewing this document who may not be familiar with the electrical utility protocol environment.

5.3.2 Asymmetric communications

All the protocols affected by this specification share the concept of inequality between the communication stations. In each of these protocols, there is a designated controlling station and a designated controlled station, each having different roles, responsibilities, procedures and message formats. In particular, the controlling station is in many cases responsible for flow control and media access control.

The existence of a definite controlled/controlling station designation has two impacts on the design of this authentication mechanism:

- the format of messages in each direction will differ, even if the functions are the same;
- key distribution is simplified because they will always be issued by the controlling station.

5.3.3 Message-oriented

All of the affected protocols are message-oriented. This means that authentication must be performed on a message-by-message basis, rather than authenticating only at the beginning of a data stream and occasionally thereafter, as some connection-oriented protocols do.

5.3.4 Poor sequence numbers or no sequence numbers

A common security technique to address the threat of replay is to include in the message a sequence number. Combined with tests for message integrity, the sequence number makes it harder for an attacker to simulate a legitimate user by just copying an existing message, because the messages must be transmitted in a particular order.

Unfortunately, none of the affected protocols includes a sequence number that would provide adequate protection. Those sequence numbers that do exist have very low maximum values, permitting an attacker to attempt a replay after gathering only a small number of messages.

Therefore, the design of this specification must include its own sequence numbers and other time-varying data to protect against replay.

5.3.5 Limited processing power

The lack of processing power available on many power utility devices has been a major design concern for the affected protocols since their creation. This design requirement necessarily affects the authentication mechanism also. The concern is heightened by the fact that many of these devices are single-processor machines; a denial-of-service attack would affect not only the communications capability of such devices but their function as an electrical control, protection, or monitoring device also.

Therefore, the use of security measures requiring extremely high processing power, such as public-key encryption and very large key sizes, has been avoided as much as possible.

5.3.6 Limited bandwidth

The limited amount of bandwidth available in utility networks has been the prime design concern (after message integrity) of the affected protocols. Links of 1 200 bits per second and lower are still a reality for many applications of these protocols. Some communications links also charge costs per octet transmitted.

Therefore, the authentication mechanism must not add very much overhead (i.e. few octets) to the affected protocols. The size of the challenge and authentication data has therefore been limited and truncated as much as possible while retaining an adequate level of security. Other measures may be taken in the implementations in each protocol.

5.3.7 No access to authentication server

The nature of the utility networks in which the affected protocols are deployed is that the controlling station is often the only device with which the controlled station can communicate. If there is any access to other networks, it is often achieved through the device implementing the controlling station.

The impact of this fact on the authentication mechanism is that any system requiring on-line verification of the controlling station's security credentials by a third party is not practical.

5.3.8 Limited frame length

Because of the restrictions on bandwidth and message integrity, the affected protocols are designed to send data in small frames of 255 octets or less. Some derivative protocols permit “chaining” frames together to create larger application layer messages.

However, in general, the authentication mechanism cannot assume the transmission of large data units between the stations.

5.3.9 Limited checksum

Message integrity was a high priority in the design of the affected protocols. However, the integrity measures chosen for these protocols were designed to protect against random noise, and not a concerted attack, as discussed below.

- The serial IEC 60870-5 protocols use frame type FT1.2, which uses parity bits and a single-octet checksum to protect against bit errors. A single octet is not large enough to provide a secure message authentication code (MAC).
- The IEC 60870-5-104 protocol depends on the integrity measures of lower layers. Because this specification discusses an application layer mechanism only, it cannot depend on such measures. In any case, doing so would provide a solution for only one of the affected protocols.
- The DNP3 protocol uses the IEC 60870-5 FT3 frame, with a two-octet cyclic redundancy check every 16 octets or fewer. This provides considerable integrity for security purposes, except that there is no check for the entire frame.

Therefore, the authentication mechanism described in this specification cannot make use of the existing protocol integrity mechanisms to provide message integrity for security purposes.

5.3.10 Radio systems

The affected protocols are often used over radio systems which may or may not provide security measures of their own. Many existing utility radio networks provide no security at all.

Therefore, the mechanism described in this specification must assume a hostile and physically insecure transmission environment.

5.3.11 Dial-up systems

The affected protocols are often used over dial-up telephone networks which require several seconds to re-establish communications before each frame transmitted. Similarly, many radio systems require long “keying” times before each frame.

Therefore, the authentication mechanism provides an option, known as “aggressive mode” that reduces the number of extra frames of data to be transmitted.

5.3.12 Variety of protocols affected

The IEC 60870-5 family of protocols share many common functions and an underlying design philosophy. However, the various companion standards and derivative protocols have been implemented using a variety of message formats and procedures.

Therefore, this specification describes a generic authentication mechanism that must be mapped to each specific affected protocol within specifications that are specific to that protocol.

5.3.13 Differing data link layers

As discussed in 5.3.9, the affected protocols use a variety of transport mechanisms and procedures. Although IEC 60870-5 describes a common data link layer, it permits multiple frame formats and other options. Several of the affected protocols use the FT1.2 frame, one uses FT3, and one does not use that frame format at all. Some of them use only an unbalanced media access control procedure, some use a balanced method, and some optionally use both.

Therefore, the authentication mechanism cannot be based on the data link layer. However, it can assume that there is addressing information available from lower layers that can be used for authentication.

5.3.14 Long upgrade intervals

Utilities depreciate changes to their networks over long periods, and may deploy several different generations of network systems simultaneously.

Therefore, this authentication mechanism follows the principles described in 5.4.8.

5.3.15 Remote sites

The devices that implement the affected protocols are often located at sites that are very remote and expensive to access.

Therefore, as much as possible, this mechanism includes methods of updating security credentials remotely.

5.3.16 Multiple users

A common topology for the affected protocols is for multiple users (such as control consoles, or operators) to access the controlled station through a single controlling station. For non-repudiation purposes, it is important to know which of these users sent a particular command of the controlled station.

Therefore, this mechanism includes methods to authenticate individual users separately from the controlling station itself.

5.3.17 Unreliable media

The affected protocols are often used over unreliable media. This mechanism attempts to take this unreliability into account when addressing error conditions. For instance, it does not assume that the loss of a single security message necessarily means that an attack is underway.

5.4 General principles

5.4.1 Overview of subclause

This subclause describes the guiding principles behind this specification, based on the identified threats and design issues discussed in the previous two clauses.

5.4.2 Authentication only

As discussed in Clause 1, this specification addresses authentication only, not encryption or other security measures. It does not rule out the possibility of such measures being added to the affected protocols by other standards.

5.4.3 Application layer only

This specification describes authentication at the application layer. Refer to IEC/TS 62351-1 for a discussion of why application layer authentication is necessary in the utility environment, in addition to any transport layer security that may be implemented.

5.4.4 Generic definition mapped onto different protocols

This specification describes a common method of authentication that can be used by any of the affected protocols. The implementation of this method in each protocol shall be defined by separate standards. Such standards shall reference this specification according to the rules defined in Clause 10.

5.4.5 Bi-directional

This specification describes a mechanism that can be used in either transmission direction, despite the asymmetry of communications traffic defined by the affected protocols and discussed in 5.3.2.

5.4.6 Challenge-response

The mechanism described in this specification is based on the concept of challenge and reply. This principle has been applied for the following reasons.

- It places the responsibility for security on the device that requires authentication, which is more practical in a diverse network such as those found in the utility industry.
- It permits some communication to be left unsecured if desired, reducing bandwidth and processing requirements.
- It works effectively in a non-connection-oriented environment.

Because “response” is a keyword in the affected protocols, the term used in this specification is “reply”.

5.4.7 Pre-shared keys as default option

This specification permits pre-shared keys to be used by default. This principle recognizes the fact that many utilities are not prepared to manage security credentials in a more sophisticated manner but nevertheless require some level of protection.

This specification does not prevent the use of public-key cryptography or other key distribution mechanisms to be used to change or distribute the pre-shared keys described here. Future specifications may standardize such methods, but they are currently out of the scope of this specification.

5.4.8 Backwards tolerance

This specification recommends that the following conditions be satisfied when a secure device (one implementing this authentication mechanism) communicates with a non-secure device.

- The secure device should be able to detect that the non-secure device does not support the authentication mechanism.
- The non-secure device should continue to operate normally after being contacted by the secure device. In other words, the authentication message cannot cause the non-secure device to fail.
- The two devices should be able to continue to exchange information that is not considered critical.

However, the mechanism’s ability to meet these conditions is largely dependent on the protocol it is mapped to and on the quality of the implementation on any particular device.

This specification therefore recommends that secure devices avoid sending security messages if it is not known whether the remote device supports security. Remote configuration of security or non-security is beyond the scope of this document.

5.4.9 Upgradeable

This specification permits system administrators to change algorithms, key lengths, and other security parameters to deal with future requirements. In keeping with the principle of backward tolerance, it also permits one end of a link to be upgraded at a time.

5.4.10 Perfect forward secrecy

This specification follows the security principle of perfect forward secrecy, as defined in IEC/TS 62351-2. If a session key is compromised, this mechanism only puts data from that particular session at risk, and does not permit an attacker to authenticate data in future sessions.

5.4.11 Multiple users

This specification assumes that there may be multiple users of the system located at the site of the controlling station. It provides a method to authenticate each of the users separately from each other and from the controlling station itself.

The intent of this principle is to permit the controlled station to conclusively identify the individual user (not just the station) that transmits any protocol message. This information could be used in audit logs for non-repudiation purposes, although such use is out of the scope of this specification.

This specification allows for the possibility that controlled stations may limit access to certain functions, either based on the individual identities of users, or based on the “roles” the users perform. The user number discussed in this document can be considered to represent not just a user, but a user acting in a particular role. However, this document does not specify a mechanism for such user-based or role-based access control.

6 Theory of operation (informative)

6.1 Overview of clause

This clause describes the operation of the authentication mechanism in general terms for the benefit of first-time readers. This clause is informative only; in the case of disagreements between this clause and Clause 7, Clause 7 shall be taken as correct.

6.2 Narrative description

6.2.1 Basic concepts

The authentication mechanism is based on two concepts:

- a challenge and response protocol, as discussed in 5.4.6. The general mechanism is illustrated in Figure 1. Because “response” is a keyword in the affected protocols, the term used here is “reply”;
- the concept of a keyed-hash message authentication code (HMAC) that both the controlled and controlling stations calculate based on each application service data unit (ASDU, or protocol message) that is to be authenticated.

An HMAC algorithm is a mathematical calculation that takes a protocol message as input, produces a smaller piece of data as output, and has the following characteristics.

- The value of the output is sensitive to small changes in the input message, so the output of the HMAC can be used to detect if the message was modified.
- The calculation makes intrinsic use of a secret key that is shared by both ends of the communication.
- It is extremely difficult to determine the secret key by viewing the HMAC output.
- It is nearly impossible to determine the original message from the HMAC.
- It is difficult to find two messages that produce the same HMAC.

This challenge-reply mechanism using an HMAC is a “unilateral, two-pass authentication” mechanism as described in ISO/IEC 9798-4.

6.2.2 Initiating the challenge

The challenge may be initiated either by the controlling station or the controlled station. Since the IEC 60870-5 protocols are generally asymmetric, this means that the actual format of the challenge and reply messages will be somewhat different in the control and monitoring directions.

Stations shall issue challenges to protect specific ASDUs that the device considers to be critical. The challenger issues the challenge immediately after receiving the critical ASDU, before taking any action on it.

Controlled stations shall consider all output operations (controls, setpoint adjustments, parameter settings, etc.) to be critical. Other mandatory critical operations are described in 7.3.2.2. Each affected protocol may define additional mandatory critical operations.

To protect against replay attacks, the challenge message contains data that changes randomly each time a challenge is issued.

The challenger specifies in the challenge message the cryptographic keyed-hash message authentication code (HMAC) algorithm for the responder to use when building the reply.

6.2.3 Replying to the challenge

The station (either controlling or controlled) that receives the challenge must respond before communications can continue.

The responder performs the HMAC algorithm specified in the challenge message to produce the reply. A shared session key known to both stations is an integral part of the computation. The following types of information are included in the computation.

- Some addressing information, specific to each protocol, is included in order to authenticate the responder as a valid application layer user.
- The challenge data is included, to protect against replay attacks.
- If the challenger is protecting a specific critical ASDU, data from that ASDU is also included in the computation. This protects against modification of the ASDU by an attacker.

The reply includes the resulting HMAC value.

6.2.4 Authenticating

Upon receiving the reply, the challenger performs the same calculation on the same data used by the responder. If the results match, the challenger permits communications to continue. If the challenger was protecting a particular ASDU, it processes the ASDU.

6.2.5 Authentication failure

If the authentication fails, the challenger shall not perform the requested operation. The challenger may then choose to transmit an error message. To help protect against denial-of-service attacks, the challenger shall cease to transmit error messages after a fixed number of failures. The controlling station must reset the session keys before the error condition can be cleared.

6.2.6 Aggressive mode

To reduce bandwidth usage, a responder attempting a critical operation may optionally "anticipate" the challenge and send the HMAC value in the same ASDU being protected. This eliminates the challenge and reply messages. Aggressive mode provides a lower level of security, because not as much data is changing in each message.

Stations are required to implement aggressive mode, but shall provide a mode of operation in which it can be configured as disabled.

Aggressive mode is a "unilateral, one-pass authentication" mechanism as described in ISO/IEC 9798-4. However, it is somewhat more secure against replay attacks because the aggressive mode request includes information from the most recently received challenge in addition to the sequence number required by ISO/IEC 9798-4.

6.2.7 Changing keys

6.2.7.1 General

Table 2 summarizes how cryptographic keys are used and updated in this authentication mechanism. The session keys that each station uses to hash the challenge data are the most frequently used keys. A different session key is used in each direction, so that if the key for one direction is compromised, it does not compromise communications in the other direction.

Table 2 – Summary of keys used

Type	Use	Change mechanism	Range of expected change interval
Monitoring direction session key	Used to authenticate data transmitted in the monitoring direction by the controlled station.	The controlling station shall encrypt the session key in a key change message using the update key.	Minutes to weeks (for infrequent communications)
Control direction session key	Used to authenticate data transmitted in the control direction by the controlling station.	The controlling station shall encrypt the session key in a key change message using the update key.	Minutes to weeks
Update key	The controlling station shall use the update key to periodically change the session keys.	The update key shall be pre-shared by the two devices and is changed only by means external to the protocol.	Months or years

6.2.7.2 Managing session keys

The session keys that each station uses to hash the challenge data are the most frequently used keys. A different session key is used in each direction, so that if the key for one direction is compromised, it does not compromise communications in the other direction.

The controlling station initializes the session keys immediately after communication is established and regularly changes the session keys thereafter. This practice of periodically changing the session keys protects them from being compromised through analysis of the communications link.

The controlling station uses a second key, called the update key, to encrypt the new session keys, together with the challenge data, inside a key change message. The use of a second key permits the controlling station to change the session key even if the original session key was compromised. Both the session keys and the update key are symmetric keys.

The sequence for changing the session keys is shown in Figure 5 and Figure 6. Like the normal authentication mechanism, it is also based on challenge and reply:

- The controlling station sends a key status request message, which contains no data but serves to initiate the process.
- The controlled station replies with a key status message containing the current status of the keys and some challenge data.
- The controlling station updates the session keys with a key change message. Besides changing the keys, the key change message also constitutes a reply to the challenge and permits the controlled station to authenticate that the correct entity is attempting to change the session keys.
- The controlled station replies with a new key status message. This key status message indicates whether the key change was successful (i.e. properly received and authentic) and includes freshly generated challenge data.
- Thereafter, the controlling station can send another key change message at any time, replying to the most recent challenge data it received.

The algorithm used to encrypt both the session keys together with the challenge data is known as a “key wrap” algorithm. The minimum required key wrap algorithms are specified in 8.2.3.

If either station determines that the communication has failed, it shall assume the most recent set of session keys have been compromised and shall refuse to use them to authenticate any further challenge or aggressive mode request messages. The controlling station shall send a key status request at the earliest opportunity after detecting the communications failure, and re-initialize the session keys.

6.2.7.3 Managing update keys

As discussed in 5.4.11, this authentication mechanism permits multiple users of the system to be authenticated separately from the controlling station itself. Each user is identified by its own user number and has its own update key and set of session keys.

Each user’s update key is rarely changed. The reason for such a change is dependent on the security policy of the organization, but may include the update key being compromised, or a user leaving the organization. In such cases, the update key must be changed through a mechanism external to the protocol. This mechanism is outside the scope of this specification, but it must ensure that the update key is kept secret and cannot be eavesdropped upon nor modified in transit.

6.3 Example message sequences

6.3.1 Overview of subclause

This subclause contains diagrams illustrating examples of how the authentication mechanism shall behave. This subclause is informative only. Refer to Clause 7 for a formal description of the mechanism. Bold arrows in these diagrams represent authentication-specific messages.

6.3.2 Challenge of a critical ASDU

Figure 1 and Figure 2 illustrate the challenge and reply to a critical ASDU.

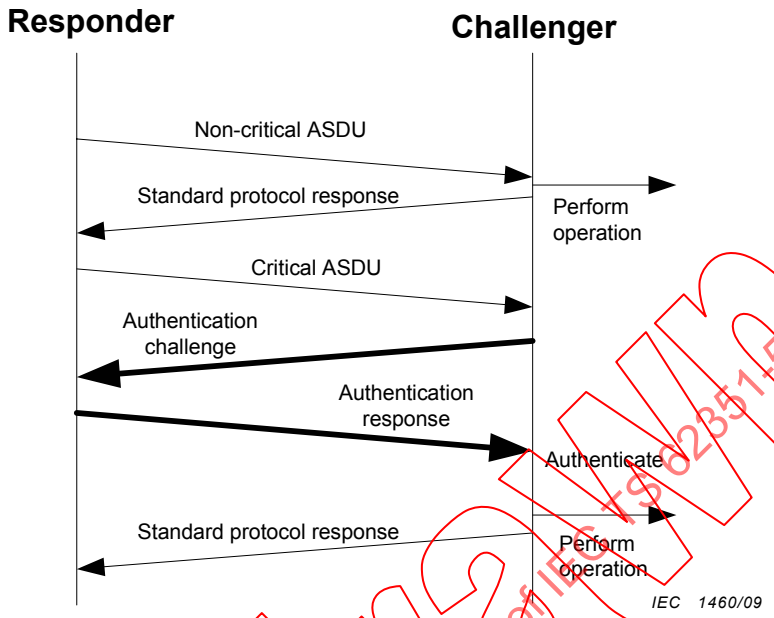


Figure 1 – Example of successful challenge of critical ASDU

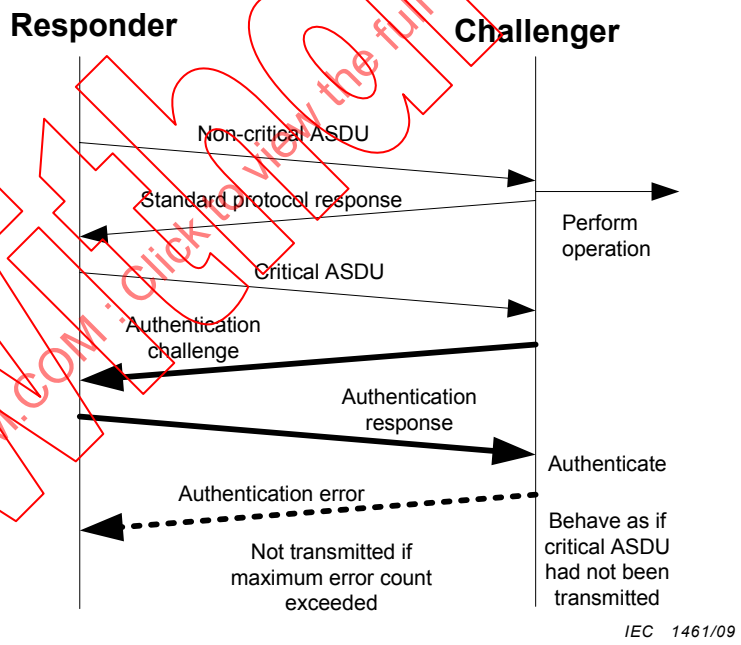


Figure 2 – Example of failed challenge of critical ASDU

6.3.3 Aggressive mode

Figure 3 and Figure 4 illustrate authentication of a critical ASDU using aggressive mode.

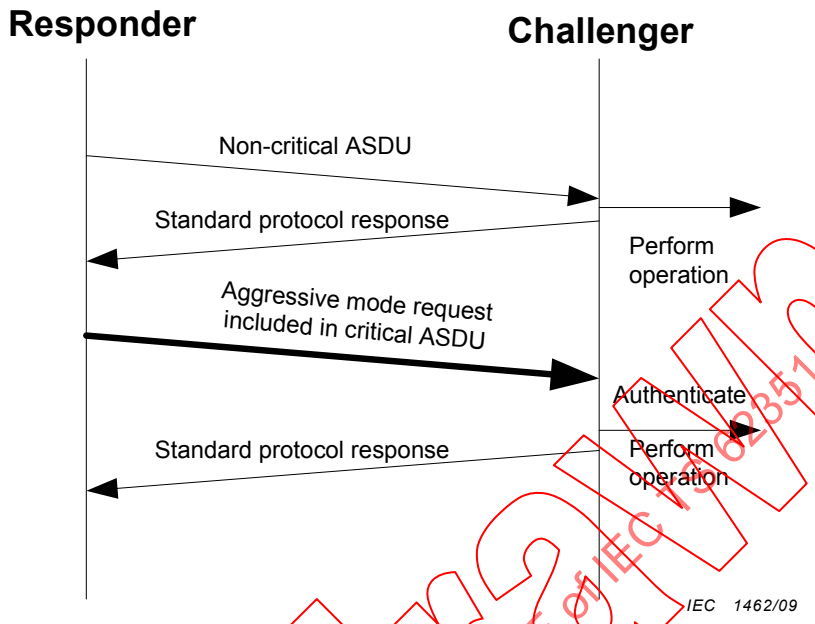


Figure 3 – Example of a successful aggressive mode request

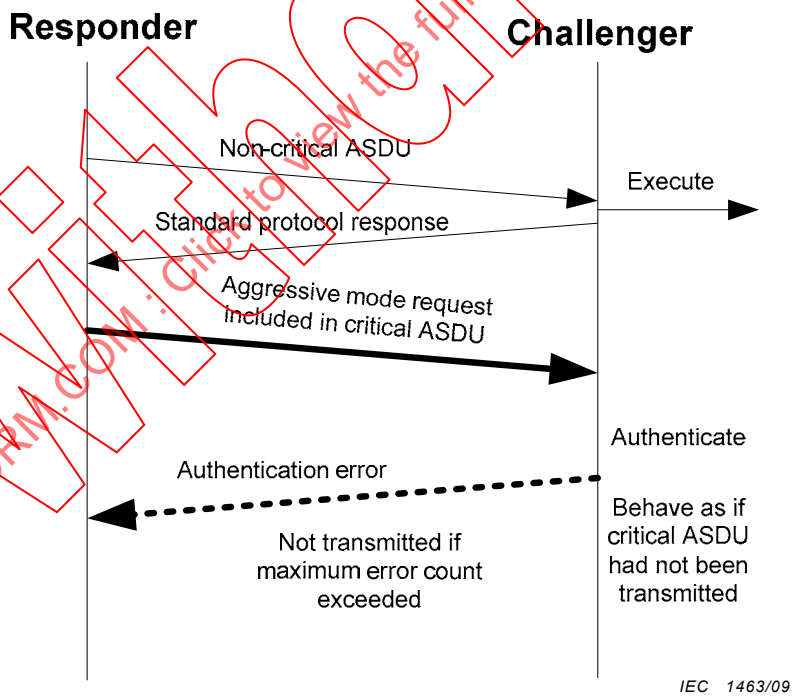


Figure 4 – Example of a failed aggressive mode request

6.3.4 Initializing and changing session keys

Figure 5 and Figure 6 illustrate how the controlling station initializes and changes the session keys on startup, periodically, and after a communications failure.

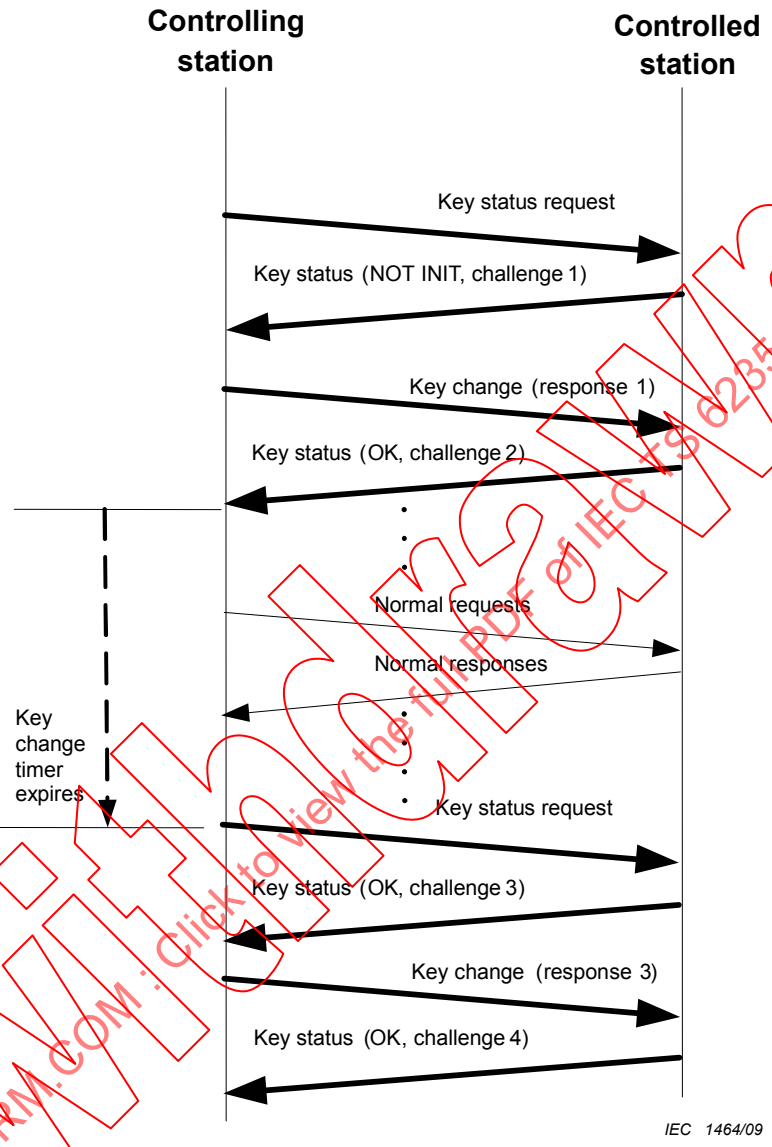


Figure 5 – Example of session key initialization and periodic update

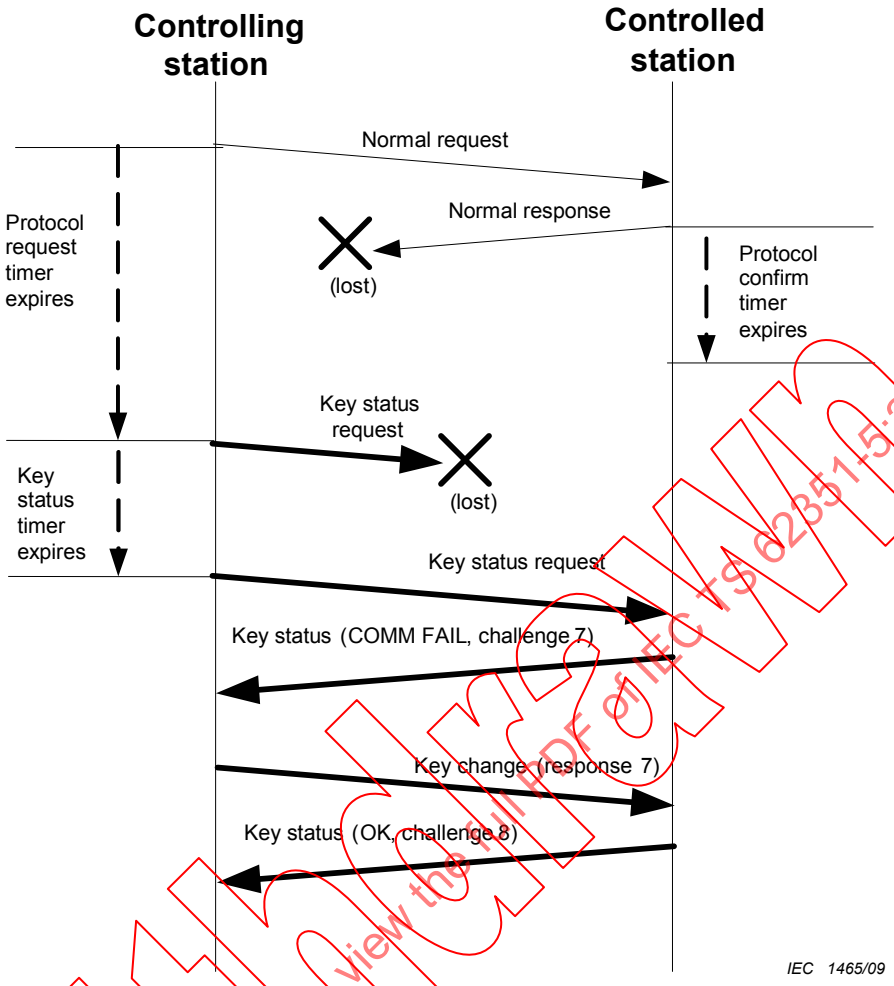


Figure 6 – Example of communications failure followed by session key change

6.4 State machine overview

Figure 7 and Figure 8 show the major state transitions for the protocol. These diagrams are not normative, nor are they comprehensive. The details of the state machines are specified in Clause 7. If these diagrams differ from Clause 7, that clause shall be considered to be correct.

However, these figures are intended to show the general operation of the authentication protocol. In each of the state machine overview diagrams, a state is represented by a circle and state transitions are represented by arrows. The text before the slash ("/") on each state transition arrow is the name of the event. The italicized text after the slash describes action to be taken by the station before the transition to the next state.

The security idle and wait for reply states are common to both controlling and controlled stations. The other states are specific to each type of station.

For simplicity, these figures show a transition to the wait for reply state upon receiving an aggressive mode request. In reality, as described in Table 18, this transition would be only momentary and the station would immediately return to security idle state after taking the appropriate action.

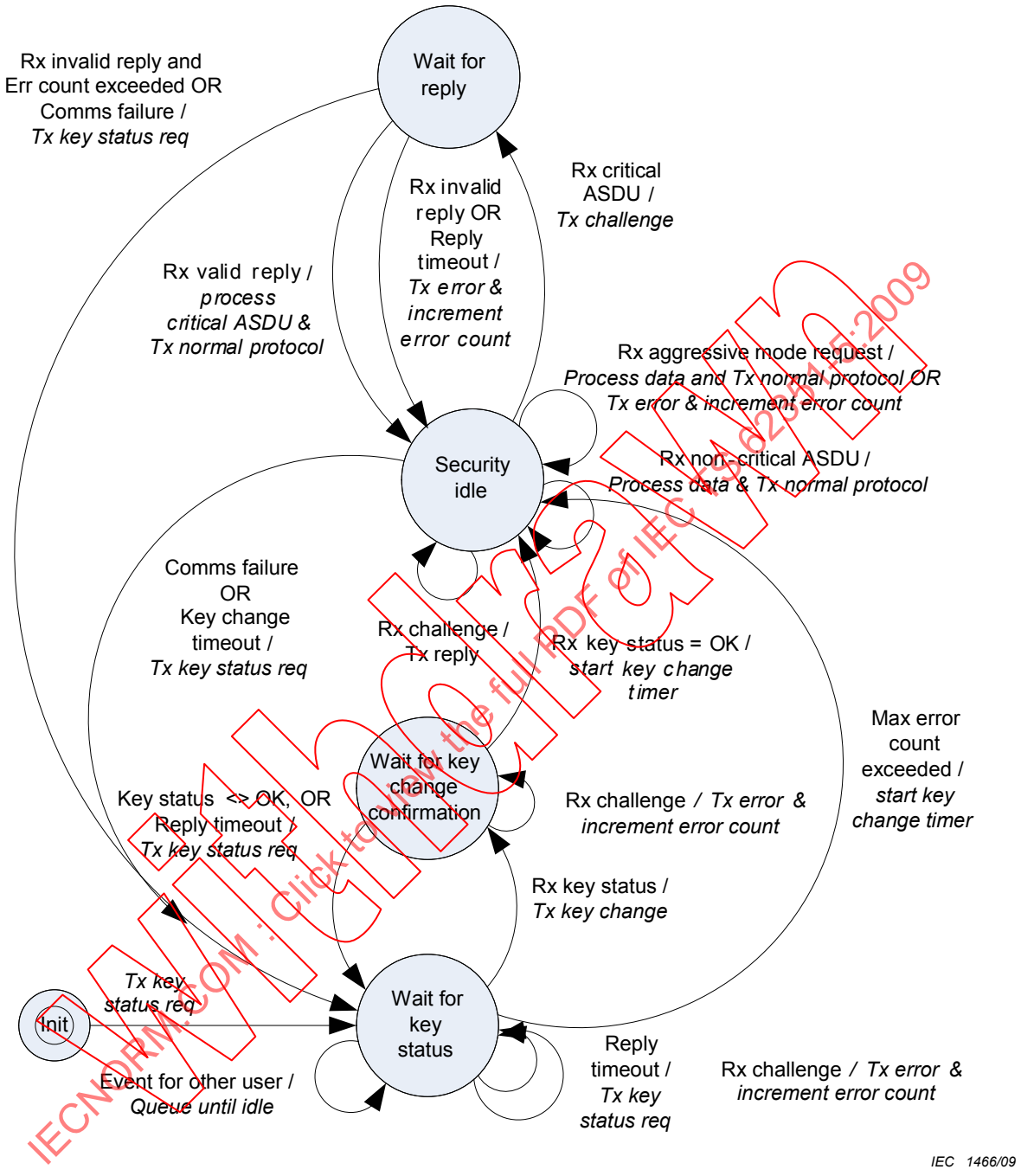


Figure 7 – Major state transitions for controlling station

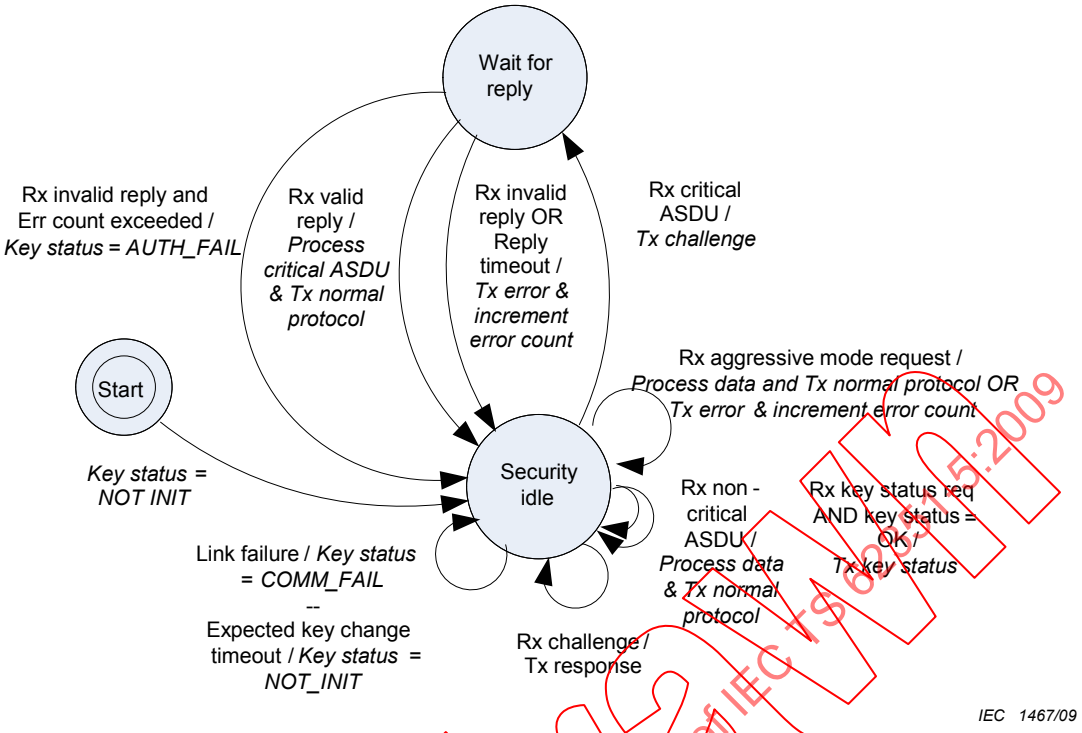


Figure 8 – Major state transitions for controlled station

7 Formal specification

7.1 Overview of clause

This clause formally describes the protocol used for this authentication mechanism. If this clause differs from Clause 6, this clause shall be considered to be definitive.

7.2 Message definitions

7.2.1 Distinction between messages and ASDUs

This subclause describes the data in each security message. A security message is not a complete ASDU. The list of data and the format of this data shall remain the same between protocols, but the ASDUs surrounding the message and the mechanisms used to deliver them shall differ per protocol. This mapping to the affected protocol shall be described in the specification for the affected protocol, as discussed in Clause 10. Note that all of the affected protocols transmit integer values with the least significant octet transmitted first; therefore that same convention shall be used for all the security messages.

7.2.2 Challenge message

7.2.2.1 Structure

Each challenge message shall contain the information described in this subclause and summarized in Table 3. A challenge message shall be a request that the responder authenticate itself to the challenger.

Table 3 – Challenge message

Value Value Value Value	CSQ = Challenge sequence number, defined in 7.2.2.2
Value Value	USR = User number, defined in 7.2.2.3
Enumerated value	HAL = HMAC algorithm, defined in 7.2.2.4
Enumerated value	RSC = Reason for challenge, defined in 7.2.2.5
Value Value	CLN = Challenge data length, defined in 7.2.2.6
Number of octets specified in CLN	Pseudo-random challenge data, defined in 7.2.2.7

7.2.2.2 Challenge sequence number

Stations shall use this value to match replies with challenges. Each station shall maintain its own separate challenge sequence number. Each station shall set this value to zero on startup, and increment this value each time it transmits a challenge message. If the value reaches 4294967295, the next CSQ the challenger transmits shall be zero.

Challenge sequence numbers shall be independent of user number. In other words, each station need only store a single value of CSQ locally regardless of how many users or devices it is communicating with.

CSQ := UI[1..32]<0.. 4294967295>

7.2.2.3 User number

The controlling station shall use this value to identify which set of session keys is to be used in this challenge-reply sequence.

USR := UI[1..8]<0..65535>

<0> := Unknown. The challenge-reply sequence is being initiated by a controlled station. Therefore, the appropriate USR is not yet known. The controlling station will supply the appropriate USR in the reply message.

<1> := Default: The challenge-reply sequence is being initiated by a controlling station on behalf of more than one user, and the set of session keys used will therefore be the default set of keys for this pair of stations. Refer to 7.2.5.2 for more details.

<2..65535> := Chosen by the controlling station to be associated with a particular user and corresponding set of session keys.

7.2.2.4 HMAC algorithm

Using this value, the challenger shall specify the algorithm that the responder shall use to calculate the HMAC Value, as described in 7.2.3.5, and shall also specify the resulting length of the HMAC value, as described in 7.2.3.4. Refer to the normative references listed in Clause 2 for details of these algorithms. Each station shall support at least the minimum subset of algorithms listed in 8.2.2.

HAL := UI[1..8]<0..255>
- <0> := not used
- <1> := HMAC SHA-1 truncated to 4 octets (serial)
- <2> := HMAC SHA-1 truncated to 10 octets (networked)
- <3> := reserved for future SHA algorithms
- <4> := reserved for future SHA algorithms
- <5..127> := reserved for future use
- <128..255> := reserved for vendor-specific choices. Not guaranteed to be interoperable.

IMPORTANT: Refer to the note in 8.2.5.3 regarding the dependency between the use of truncated HMAC algorithms and the need for frequent session key changes. In any case, the longest practical HMAC should be used whenever possible.

7.2.2.5 Reason for challenge

This value explains the challenger's reason for making the challenge. The responder shall use this value to determine what extra data to include when calculating the HMAC value.

RSC := UI[1..8]<0..255>
- <0> := not used
- <1> := CRITICAL. Challenging a critical function. The responder shall include the entire *previous* ASDU transmitted by the responder when calculating the HMAC value, as well as any further protocol-specific information.
- <2..255> := reserved for future use

7.2.2.6 Challenge data length

This value shall specify the length in octets of the challenge data that follows. The minimum length of the challenge data shall be four octets.

CLN := UI[1..16]<4..65535>

7.2.2.7 Pseudo-random challenge data

Stations shall include pseudo-random data in the challenge message to ensure that the contents of the challenge message are not predictable. The pseudo-random data shall be generated using the algorithm specified in the FIPS 186-2 digital signature standard.

7.2.3 Reply message

7.2.3.1 Structure

Each reply message shall contain the information described in this subclause and summarized in Table 4. A reply message shall be a reply to a challenge message.

Table 4 – Reply message

Value	CSQ = Challenge sequence number, defined in 7.2.3.2
Value	
Value	
Value	
Value	USR = User number, defined in 7.2.3.3
Value	
Value	HLN = HMAC length, defined in 7.2.3.4
Value	
Number of octets specified in HLN	HMAC value, defined in 7.2.3.5

7.2.3.2 Challenge sequence number

This value shall be as described in 7.2.2.2. The value transmitted by the responder in the reply message shall be the same value transmitted by the challenger in the previous challenge message.

7.2.3.3 User number

The controlling station shall use this value to identify which set of session keys is to be used to authenticate this reply. If the responder is the controlled station, this value shall be the same as the USR value transmitted by the challenger in the previous challenge message. If the responder is the controlling station, it shall set the USR value according to which user is being authenticated. Refer to 7.2.5.2 for more details.

USR := UI[1..8]<0..65535>

7.2.3.4 HMAC length

HLN := UI[1..16]<2..65535>

The HMAC length shall specify the length of the HMAC value in octets. The HMAC length shall be correct for the HMAC algorithm specified by the challenger, as described in 7.2.2.4.

7.2.3.5 HMAC value

The responder shall calculate the HMAC value according to the HMAC algorithm specified by the challenger, as described in 7.2.2.4. The responder shall include in the HMAC value calculation the data listed in Table 5, in the order listed.

Table 5 – Data included in the HMAC value calculation

Data	Description	Described in	Included
Challenge message	The entire challenge message transmitted by the challenger.	Subclause 7.2.2	Always.
Addressing information	Addressing information identifying the challenger and responder, specific to the protocol and found in the lower layers of the protocol.	Protocol specification	Always.
Challenged ASDU	The entire previous ASDU transmitted by the responder, not including data link layer or APCI information.	Protocol specification	If the reason for challenging is <2>, challenging a critical function.
Padding data	Any padding data required.	Hash specification	As required by the HMAC algorithm.

Controlled stations acting as the responder shall use the current monitoring direction session key to calculate the HMAC value.

Controlling stations acting as the responder shall use the current control direction session key to calculate the HMAC value.

7.2.4 Aggressive mode request

7.2.4.1 Structure

In aggressive mode, a station shall supply authentication information in the same ASDU as the data it is authenticating. Aggressive mode shall be mandatory, but can be disabled by configuration. Aggressive mode is slightly less secure than normal mode operation, but uses considerably less bandwidth, especially if many critical functions must be authenticated.

Each aggressive mode request message shall contain the information described in this subclause and summarized in Table 6.

Table 6 – Aggressive mode request message

Value	CSQ = Challenge sequence number, defined in 7.2.4.3.
Value	
Value	
Value	
Value	USR = User number, defined in 7.2.4.4
Value	
Number of octets specified in HLN	HMAC value, defined in 7.2.4.5.

7.2.4.2 Aggressive mode must be preceded by challenge/reply

The responder shall not transmit an aggressive mode request until the responder has received and responded to at least one challenge message from the challenger. Refer to the procedures in 7.3.3 for more details.

The responder shall use the data from the most recently received challenge message to calculate the challenge sequence number and HMAC value in the aggressive mode request, as described in 7.2.4.3 and 7.2.4.5.

7.2.4.3 Challenge sequence number

The challenge sequence number (CSQ) shall have the value described in 7.2.2.2. The effect of the rules described in that subclause is that the CSQ of a given aggressive mode request shall be the CSQ from the most recently received challenge message, plus the number of aggressive mode requests the responder has transmitted since receiving that challenge message, plus one.

7.2.4.4 User number

The responder shall use this value to identify which set of session keys is to be used to authenticate this aggressive mode request.

USR := UI[1..8]<0..65535>

<0> := Unknown. Not used for this message.

<1> := Default: One of two cases is occurring:

- This message is being sent by a controlling station on behalf of more than one user.
- This message is being sent by a controlled station and there is no corresponding user.

In either case, the set of session keys used will be the default set for this pair of stations. Refer to 7.2.5.2 for more details.

<2..65535> := Chosen by the controlling station to be associated with a particular user and corresponding set of session keys.

7.2.4.5 HMAC value

In aggressive mode, the HMAC value shall be calculated in the same manner as in normal mode, but shall be calculated based on the same ASDU as the aggressive mode request, rather than the previous ASDU. Table 7 describes this difference.

Table 7 – Data included in the HMAC value calculation in aggressive mode

Data	Description	Described in	Included
Challenge message	All the data from the most recently received challenge message, including the CSQ at the time of that message.	Subclause 7.2.2	Always.
New CSQ	The new value of CSQ.	Subclause 7.2.4.3	Always.
Addressing information	Addressing information identifying the challenger and responder, specific to the protocol and found in the lower layers of the protocol.	Protocol specification	Always.
Authenticated data	The entire ASDU transmitted by the responder, not including data link layer or APCI information.	Protocol specification	Always.
Padding data	Any padding data required.	Hash specification	As required by the HMAC algorithm.

The length of the HMAC value shall be determined by the HMAC algorithm (HAL) of the most recent challenge received by the responder, as described in 7.2.2.4.

Controlled stations acting as the responder shall use the current monitoring direction session key to calculate the HMAC value.

Controlling stations acting as the responder shall use the current control direction session key to calculate the HMAC value.

7.2.5 Key status request message

7.2.5.1 Structure

Each key status request message shall contain the information described in this subclause and summarized in Table 8.

Only the controlling station shall send key status request messages. The key status request message shall elicit a key status message from the controlled station.

Table 8 – Key status request message

Value	USR = User number, defined in 7.2.4.4
Value	

7.2.5.2 User number

The controlling station uses this value to identify the set of session keys for which it is requesting the current status.

USR := UI[1..8]<0..65535>

<0> := Unknown. Not used for this message.

<1> := Default. The default set of session keys used by this pair of stations, to be used as illustrated in Table 9.

<2..65535> := Chosen by the controlling station to be associated with a particular user and corresponding set of session keys.

Table 9 – Use of default session keys

Case	User number
Controlled station sends challenge	Unknown <0>
Controlled station sends aggressive mode request	Default <1>
Controlling station challenges response or unsolicited response from controlled station	Default <1>
Controlling station sends request for data to be processed by multiple users	Default <1>
Any other case	<2..65535>

7.2.6 Key status message

7.2.6.1 Structure

Each key status message shall contain the information described in this subclause and summarized in Table 10.

Only the controlled station shall send key status messages. A key status message shall indicate to the controlling station the current status of the session keys and provide challenge data that the controlling station must use to authenticate itself when sending the next key change message.

If the key status = OK, meaning that the controlled station considers the session keys to be valid, the key status message is authenticated with an HMAC.

Table 10 – Key status message

Value	KSQ = Key change sequence number, defined in 7.2.6.2
Value	
Value	
Value	
Value	USR = User number, defined in 7.2.6.3
Value	
Enumerated value	KWA = Key wrap algorithm, defined in 7.2.6.4
Enumerated value	KST = Key status, defined in 7.2.6.5
Enumerated value	HAL = HMAC algorithm, defined in 7.2.6.6
Value	CLN = Challenge data length, defined in 7.2.6.7
Value	
Number of octets specified in CLN	Pseudo-random challenge data, defined in 7.2.6.8
Number of octets specified in HAL	HMAC value, defined in 7.2.6.9

7.2.6.2 Key change sequence number

Each controlled station shall maintain a key change sequence number, which it shall use to match key status messages with subsequent key change messages. This value shall be initialised to zero on start-up of the controlled station. The controlled station shall increment the KSQ each time it receives a key change or key status request message. (The first KSQ transmitted shall therefore always be 1). If the value reaches 4294967295, the next KSQ the controlled station transmits shall be zero.

The controlling station shall not process the KSQ except to include it in subsequent key change messages.

KSQ := UI[1..32]<0.. 4294967295>

7.2.6.3 User number

The controlled station shall use this value to identify the set of session keys for which it is reporting the current status. This value shall match the value supplied in the previous key status request message, as described in 7.2.5.2.

7.2.6.4 Key wrap algorithm

Using this value, the controlled station shall indicate to the controlling station the algorithm it will use to decrypt the data in subsequent key change messages. Refer to the normative references listed in Clause 2 for details of these algorithms. Each station shall support at least the minimum subset of algorithms listed in 8.2.3.

KWA := UI[1..8]<0..255>
<0> := not used
<1> := AES-128 key wrap algorithm, as described in 8.2.3.2.
<2..127> := reserved for future use
<128..255> := reserved for vendor-specific choices. Not guaranteed to be interoperable.

7.2.6.5 Key status

This value describes the status of the two session keys as known by the controlled station.

KST := UI[1..8]<0..255>
<0> := not used
<1> := OK. There have been no communications failures or restarts since the last time the controlled station received an authentic key change message. The session keys are valid.
<2> := NOT INIT. The controlled station has not received an authentic key change message since it last started up. The session keys are not valid.
<3> := COMM FAIL. The controlled station has detected a communications failure in either the control or monitoring direction. The session keys are not valid.
<4> := AUTH FAIL. The controlled station has received a non-authentic challenge or aggressive mode request. The session keys are not valid.
<5..255> := reserved for future use

7.2.6.6 HMAC algorithm

Using this value, the controlled station shall specify the algorithm that the controlling station shall use to calculate the HMAC value in this message, as described in 7.2.6.9, and shall also specify the resulting length of the HMAC value.

The enumerated values used to specify the HMAC algorithm are defined in 7.2.3.5, except for the following:

<0> := No HMAC value in this message. The controlled station shall use this value in all cases except when the key status = OK.

7.2.6.7 Challenge data length

This value shall specify the length in octets of the challenge data that follows. The minimum length of the challenge data shall be eight octets.

CLN := UI[1..16]<8..65535>

7.2.6.8 Pseudo-random challenge data

The controlled station shall include this pseudo-random data in the key status message to ensure that the contents of the key status message are not predictable. The pseudo-random data shall be generated using the algorithm specified in the FIPS 186-2 digital signature standard.

7.2.6.9 HMAC value

If the key status = OK, the controlled station shall calculate the HMAC value according to the HMAC algorithm HAL, as described in 7.2.6.6. The controlled station shall include in the HMAC value calculation the data listed in Table 11, in the order listed. It shall use the

monitoring direction session key from the key change message most recently received from the controlling station. If the key status is not = OK, there is no HMAC value included in this object and HAL = 0.

Table 11 – Data included in the HMAC value calculation for key status

Data	Description	Included
Challenge message	The entire ASDU containing the key change message most recently received by the controlled station.	Always.
Padding data	Any padding data required.	As required by the HMAC algorithm.

7.2.7 Session key change message

7.2.7.1 Structure

Each key change message shall contain the information described in this subclause and summarized in Table 12. A key change message shall be a notice from the controlling station of a change in the session keys.

Table 12 – Key change message

Value Value Value Value	KSQ = Key change sequence number, defined in 7.2.7.2
Value Value	USR = User number, defined in 7.2.7.3
Value Value	WKL = Wrapped key data length, defined in 7.2.7.4
Number of octets specified in KLN	Wrapped key data, defined in 7.2.7.5

7.2.7.2 Key change sequence number

This value shall match the KSQ transmitted in the key status message most recently received by the controlling station, as described in 7.2.6.2.

KSQ := UI[1..24]<0.. 4294967295>

7.2.7.3 User number

The controlling station shall use this value to specify which set of session keys is to be changed. It shall match the USR in the key status message most recently received by the controlling station, as described in 7.2.6.3.

7.2.7.4 Wrapped key data length

This value shall be the length of the data produced by the key wrap algorithm, as described in 7.2.7.5.

WKL := UI[1..16]<8 ..65535>

7.2.7.5 Wrapped key data

This value shall be the result of passing the session keys and the most recent key status message through the key wrap algorithm defined in the key status message. The controlling station shall pass the data through the key wrap algorithm in the order described in Table 13.

Table 13 – Data included in the key wrap (in order)

Data	Description	Described in	Included
Session key length	The size of one of the session keys. Both keys are the same length. This value is two octets long.	Subclause 8.2.4.2	Always
Control direction session key	The key used to authenticate data from the controlling station.	Subclause 7.2.3.5 and 7.2.4.5	Always
Monitoring direction session key	The key used to authenticate data from the controlled station.	Subclause 7.2.3.5 and 7.2.4.5	Always
Key status message	All data in the key status message most recently received from the controlled station, KSQ first.	Subclause 7.2.6	Always
Padding data	As required by the key wrap algorithm.	Subclause 8.2.3 and the algorithm specification.	As required.

The session keys shall be treated as arrays of octets and transmitted with the lowest index octet first. For example, Appendix A of the AES specification provides the example of a 128-bit cipher key shown in Table 14. The byte with index 0, having value 2b, shall be transmitted first.

Table 14 – Example of key order

Value	2b	7e	15	16	28	ae	d2	a6	ab	f7	15	88	09	cf	4f	3c
Index	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Note that the output from the key wrap algorithm may be longer than the input. For instance, the AES key wrap algorithm produces output that is exactly 8 octets longer than its input. Table 15 shows a typical example of the wrapped key data using this algorithm.

Table 15 – Example of wrapped key data

Data	Description	Size (in octets)
Session key length	So the controlled station will know what follows.	2
Control direction session key	Using the minimum size 128-bit keys	16
Monitoring direction session key		16
Key status message	Using the minimum size of challenge data, i.e. 4 octets	15
Padding data	Required to make the input data a multiple of 8 octets.	7
Additional output	For the AES key wrap algorithm	8
TOTAL		**64**

7.2.8 Error message

7.2.8.1 Structure

Each Error message shall contain the information described in this subclause and summarized in Table 16. An error message shall indicate that the station did not accept the previous message from the other station. To avoid denial of service attacks, error messages shall be optional; any station may choose not to send them at any time.

It is recommended that error messages also be transmitted on communications links other than the one on which the error occurred, in order to alert other controlling stations to possible attacks. It is also recommended that error messages be logged by both the sender and receiver.

Table 16 – Error message

Value Value Value Value	CSQ = Challenge sequence number, defined in 7.2.2.2
Value Value	USR = User number, defined in 7.2.8.3
Value Value	AID = Association ID, defined in 7.2.8.4
Enumerated value	ERR = Error code, defined in 7.2.8.5
As defined in the affected protocol	ETM = Error time stamp, defined in the affected protocol. This shall be an absolute and unambiguous timestamp of the time when the error was detected.
Value Value	ELN = Error length, defined in 7.2.8.6.
Number of octets specified in ELN	Error text, defined in 7.2.8.7

7.2.8.2 Sequence number

This value shall be the CSQ, of the operation that the error message is replying to.

7.2.8.3 User number

This value shall be the USR of the operation that the error message is replying to.

7.2.8.4 Association ID

This value shall uniquely identify the association between controlled and controlling station on which the error occurred, in case the USR is not unique within the controlled station. The combination of USR and AID shall be unique within the controlled station.

AID := UI[1..16]<0 ..65535>

7.2.8.5 Error code

This value shall specify the reason the error message is being transmitted.

ERR := UI[1..8]<0..255>

- <0> := not used
- <1> := Authentication failed. The authentication information supplied by the other station was incorrect, or the data it was authenticating was corrupted in transit.
- <2> := Unexpected reply. The other station transmitted a message that did not follow the procedures as described in 7.3.
- <3> := No reply. The other station either did not respond to the challenge message or did not follow an aggressive mode request with data for authentication.
- <4> := Aggressive mode not permitted. The station sending this error code does not permit the use of aggressive mode on this link.
- <5> := HMAC algorithm not permitted. The station sending this error code does not permit the use of the specified HMAC algorithm on this link. Mandatory HMAC algorithms are specified in 8.2.2.
- <6> := Key wrap algorithm not permitted. The station sending this error code does not permit the use of the specified key wrap algorithm on this link. Mandatory key wrap algorithms are specified in 8.2.3.
- <7> := Authorization failed. The authentication information supplied by the other device was correct, but the authenticated user is not permitted to perform the requested operation.
- <8..127> := reserved for future standardization
- <128..255> := private range for definition by each vendor. A station using this range shall use a different error code for each possible error reason, and shall supply an error text to explain each error code.

7.2.8.6 Error text length

This value shall specify the length of the error text that follows.

ELN := UI[1..16]<0 ..65535>

7.2.8.7 Error text

This value shall be a string of text suitable for display on a user interface or in a security log, encoded in unicode UTF-8 as described in RFC 3629 (note that all characters encoded in 7-bit ASCII comply with UTF-8). The error text shall explain the error code. For standardized error codes, the error text is optional and ELN may be zero. For private range error codes, the error text shall be mandatory. It is recommended that the error text contain a unique description of the user represented by the USR.

7.3 Formal procedures

7.3.1 Overview of subclause

This subclause formally describes the procedures used by stations implementing this authentication mechanism as a part of each protocol. If this subclause differs from Clause 6, this subclause shall be considered definitive.

Table 17 describes the states used by the state machines in these procedures, in the general order in which they might be expected to occur. Refer to Figure 7 and Figure 8 for an overview of how the state machines work together.

Table 17 – States used in the state machine descriptions

State	Implemented in		Description	Refer to table
	Controlling station	Controlled station		
Wait for key status	YES	No	The master has either just initialized, or its session keys have expired. It has just transmitted a request key status message and is waiting for the outstation to transmit a key status message.	Table 19
Wait for key change confirmation	YES	No	The master has transmitted a key change message and is waiting for the outstation to send confirmation that the key change has been accepted, by transmitting a key status message with the key status = <1> OK.	Table 19
Wait for reply	YES	YES	The session keys have been initialized and an authentication is in progress. One of the devices has transmitted a challenge message and is waiting for the other end to transmit a reply message.	Table 18
Security idle	YES	YES	There is no authentication in progress. The device is executing the standard protocol. The session keys may or may not be initialized.	Table 18

In each of these states except security idle, the station is waiting for a reply concerning a particular user. Stations shall keep a separate set of timers and states for each user. However, only one user may be in a state other than security idle at a time.

If an event occurs in a state other than security idle, and the event concerns a user other than the one which entered that state, the device shall either queue the event or treat it as an error, as described in the state machines.

If the maximum error count is exceeded in any of the non-idle states, the station shall return to the security idle state and may process events associated with different users. Stations may not process standard protocol request or response messages associated with the user whose error count exceeded the maximum until the controlling station re-initializes the session keys for that user. This requirement is important because it helps to prevent an attacker from denying service by forcing the device to process a particular user continuously.

7.3.2 Challenger procedures

7.3.2.1 Challenger role

A station, either controlling or controlled, that requires authentication from the other station in order to communicate, shall be called a challenger. Challengers shall issue challenge messages in reply to critical ASDUs, according to the state machine described in Table 18.

Challengers shall never intentionally retransmit the same challenge message. Any time a challenge is issued, it shall be created using new challenge data and a new challenge sequence number.

7.3.2.2 Critical functions

Each challenger shall distinguish between critical ASDUs and non-critical ASDUs. A critical ASDU shall be a message implementing a critical function. A critical function is any function that the challenger requires to be authenticated.

Controlled stations shall consider all output operations (controls, setpoint adjustments, parameter settings, etc.) to be critical.

Changing any security parameters such as algorithms, key sizes, timeouts or intervals through the affected protocols shall be considered critical functions.

An additional minimum subset of critical functions for each affected protocol shall be defined in each protocol specification as specified in 10.3.

Challengers may optionally consider additional functions beyond this minimum subset to be critical.

7.3.2.3 Authentication procedures

If the challenger is in any of the states “wait for key status”, or “wait for key change confirmation”, when it receives a reply message, it shall consider the reply message to be an Rx invalid reply event because the session keys are not valid. Similarly, if the challenger receives an aggressive mode request in any of these states, the challenger shall consider it to be an Rx invalid aggressive mode request event.

Upon receiving a reply message, the challenger shall calculate the HMAC value from the information it transmitted in the challenge message, as described in 7.2.3.5.

If the HMAC value from the reply matches the calculated HMAC value, and the challenge sequence numbers from the challenge and reply messages also match, the challenger shall consider the reply message to be a Rx valid reply event.

Otherwise, the challenger shall consider the reply message to be an Rx invalid reply event.

Upon receiving an ASDU containing an aggressive mode request, the challenger shall calculate the HMAC value from the information in the ASDU as described in 7.2.4.5. If the HMAC value in the aggressive mode request matches the calculated HMAC value and the challenge sequence number in the aggressive mode request is correct as described in 7.2.4.3, the challenger shall consider the ASDU to be a Rx valid aggressive mode request event.

Otherwise, the challenger shall consider the aggressive mode request message to be an Rx invalid aggressive mode request event.

In particular, the challenger shall consider any aggressive mode request to be an Rx invalid aggressive mode request event if the challenger has not previously received at least one Rx valid reply event from the responder. This rule follows from the definition of the aggressive mode request, because the challenge sequence number in an aggressive mode request is derived from the challenge sequence number found in the challenge most recently received by the responder.

7.3.2.4 Challenger state machine

Challengers (either controlling station or controlled station) shall implement the state machine described in Table 18. Portions of this state machine that are only implemented by a particular type of station are labelled in capitals, i.e. either CONTROLLING STATION or CONTROLLED STATION.

Note that whenever the controlled station sets the key status to a value other than OK, the set of session keys for the identified user shall be considered invalid and all authentication attempts for that user shall fail until the key status is OK again.

Table 18 – Challenger state machine

Event	Event description	State				
		Security idle		Wait for reply		
		The station is executing the standard protocol.		The station is waiting for the other station to authenticate itself.		
		Action	Next state	Action	Next state	
A	B	C	D	E	F	
Rx Non-critical ASDU	The other station has transmitted an ASDU that does not require authentication.	Process the non-critical ASDU and transmit any appropriate reply required by the standard protocol.	Security idle	Discard the ASDU that is pending authentication. Increment the error count. Cancel the reply timer. If the error count is less than the maximum error count: Process the non-critical ASDU and transmit any appropriate reply required by the standard protocol. If the error count equals the maximum error count: Ttransmit an error message with reason <2> unexpected reply. If the maximum error count has been exceeded, behave according to the “Max invalid replies” event below.	Security idle	1

Event	Event description	State				
		Security idle		Wait for reply		
		The station is executing the standard protocol.		The station is waiting for the other station to authenticate itself.		
		Action	Next state	Action	Next state	
A	B	C	D	E	F	
Rx critical ASDU	The other station has transmitted an ASDU that requires authentication.	If CONTROLLING STATION and session keys are valid or if CONTROLLED STATION: Increment the challenge sequence number (CSQ). Create and transmit a challenge message calculated from the critical ASDU. Start the reply timer. Queue the critical ASDU for execution later.	Wait for reply	Discard the previous critical ASDU pending authentication. Increment the error count. If the error count is less than the maximum error count: Increment the challenge sequence number (CSQ) Create and transmit a challenge message calculated from the critical ASDU. Start the reply timer. Queue the critical ASDU for execution later. If the error count equals the maximum error count, transmit an error message with reason <2> unexpected reply. If the maximum error count has been exceeded, behave according to the “Max invalid replies” event below.	Wait for reply	2
		If CONTROLLING STATION and session keys are invalid: Transmit a key status request message. Start the reply timer.	Wait for key status (Table 19)		Wait for reply	3
Rx valid reply	The other station has transmitted a reply message that correctly authenticates the other station based on a previous challenge.	Discard the message.	Security idle	Perform the operations specified in the queued critical ASDU, if any, and transmit any appropriate reply required by the standard protocol. Cancel the reply timer. Reset the error count to zero.	Security idle	4

Event	Event description	State				
		Security idle		Wait for reply		
		The station is executing the standard protocol.		The station is waiting for the other station to authenticate itself.		
		Action	Next state	Action	Next state	
A	B	C	D	E	F	
Rx invalid reply	The other station has transmitted a reply message that does not correctly authenticate the other station.	Discard the message.	Security idle	Increment the error count. Cancel the reply timer. Discard the critical ASDU that was queued pending authentication. If the maximum error count has not been exceeded, transmit an error message with reason <1> authentication failed. Cancel the reply timer. If the maximum error count has been exceeded, behave according to the “Max invalid replies” event below.	Security idle	5
Reply timeout	The reply timer started when entering wait for reply state has expired. This may be the standard response timer for the protocol. Refer to 8.2.5.2 for details regarding the reply timer.	Should not occur.	Security idle	Increment the error count. Cancel the reply timer. Discard the critical ASDU that was queued pending authentication. If the maximum error count has not been exceeded, transmit an error message with reason <3> no reply. If the maximum error count has been exceeded, behave according to the “Max invalid replies” event below.	Security idle	6

Event	Event description	State				
		Security idle		Wait for reply		
		The station is executing the standard protocol.		The station is waiting for the other station to authenticate itself.		
		Action	Next state	Action	Next state	
A	B	C	D	E	F	
Max invalid replies or Comm. failure detected	One of two conditions has occurred: • The maximum error count has been exceeded. • The standard protocol has detected a communications failure for some other reason.	CONTROLLING STATION: Transmit a key status request message. Start the reply timer.	Wait for key status	CONTROLLING STATION: Discard the critical ASDU that was queued pending authentication. Transmit a key status request message. Start the reply timer.	Wait for key status	7
		CONTROLLED STATION: Set the current key status to COMM FAIL if communications failed or NOT INIT otherwise.	Security idle	CONTROLLED STATION: Discard the critical ASDU that was queued pending authentication. Cancel the reply timer Set the current key status to AUTH FAIL	Security idle	8
Rx error message	The other station has transmitted an error message.	Log the error message, noting that the message was unexpected.	Security idle	Log the error message. If the error code is <5> HMAC algorithm not permitted, use a different HMAC algorithm to send the next challenge. Do not send another challenge immediately, but wait for an appropriate event to cause the challenge. Discard the pending ASDU and cancel the reply timer.	Security idle	9
Key change timeout	For CONTROLLING STATION only. Either the key change timer has expired, or the key change count has been exceeded. Refer to 8.2.5.	Transmit a key status request message. Start the reply timer.	Wait for key status	Queue the event and process it after returning to security idle state.	Wait for reply	10

Event	Event description	State				
		Security idle		Wait for reply		
		The station is executing the standard protocol.		The station is waiting for the other station to authenticate itself.		
		Action	Next state	Action	Next state	
A	B	C	D	E	F	
Expected key change timeout	For CONTROLLED STATION only. The controlled station has not received a valid key change message within the session key change interval or the session key change count configured at the controlling station. Refer to 8.2.5.	Set key status = NOT INIT Invalidate current session keys.	Security idle	If the timeout is for the waiting user: Set key status = NOT INIT. Invalidate current session keys. Discard the pending ASDU. Cancel the reply timer.	Security idle	**11**
				If the timeout is not for the waiting user: Set key status for the user specified in the timeout to NOT INIT.	Wait for reply	**12**
Rx key status request	For CONTROLLED STATION only. The controlling station has transmitted a key status request message.	Transmit a key status message Containing the current key status.	Security idle	Discard the critical ASDU that was queued pending authentication. Transmit a key status message containing the current key status. Cancel the reply timer.	Security idle	**13**

Event	Event description	State				
		Security idle		Wait for reply		
		The station is executing the standard protocol.		The station is waiting for the other station to authenticate itself.		
		Action	Next state	Action	Next state	
A	B	C	D	E	F	
Rx valid aggressive mode request	The other station transmits an ASDU containing an aggressive mode request message that correctly authenticates the other station.	If aggressive mode is enabled, Perform the operations specified in the ASDU containing the aggressive mode request and transmit any appropriate reply required by the standard protocol.	Security idle	If aggressive mode is enabled, Discard the critical ASDU that was queued pending authentication. Perform the operations specified in the ASDU containing the aggressive mode request and transmit any appropriate reply required by the standard protocol. Cancel the reply timer.	Security idle	14
		If aggressive mode is disabled, discard the request and increment the error count. If the maximum error count has not been exceeded, transmit an error message with reason <4> aggressive mode not supported.	Security idle	If aggressive mode is disabled, Discard the critical ASDU that was queued pending authentication and discard the aggressive mode request. Increment the error count. If the maximum error count has not been exceeded, transmit an error message with reason <4> aggressive mode not supported. Cancel the reply timer	Security idle	15
Rx invalid aggressive mode request	The other station has transmitted an ASDU containing an aggressive mode request that does not correctly authenticate the other station. Note that all aggressive mode requests are invalid until at least one valid challenge reply has been received.	Increment the error count. If the maximum error count has not been exceeded, transmit an error message with reason <1> authentication failed if aggressive mode is enabled, or with reason <4> aggressive mode not supported otherwise.	Security idle	Discard the critical ASDU that was queued pending authentication. Increment the error count. If the maximum error count has not been exceeded, transmit an error message with reason <2> unexpected reply if aggressive mode is enabled, or with reason <4> aggressive mode not supported otherwise. Cancel the reply timer.	Security idle	16

Event	Event description	State				
		Security idle		Wait for reply		
		The station is executing the standard protocol.		The station is waiting for the other station to authenticate itself.		
		Action	Next state	Action	Next state	
A	B	C	D	E	F	
Rx valid key change	For CONTROLLED STATION only The other station has transmitted a correctly authenticated key change message.	Store new keys. Set key status = OK. Transmit key status message. Reset error count to zero.	Security idle	Discard the previously pending critical ASDU. Store new keys. Set key status = OK. Transmit key status message. Cancel the reply timer. Reset error count to zero.	Security idle	17
Rx invalid key change	For CONTROLLED STATION only. The other station has transmitted an improperly authenticated key change message.	Set key status = AUTH_FAIL. Transmit key status message.	Security idle	Discard the invalid key change message.	Wait for reply	18
Rx challenge	The station has received a challenge message.	Reply as described in 7.3.3 responder procedures	Security idle	Increment the error count. Cancel the reply timer. If the maximum error count has not been exceeded, transmit an error message with reason <2> unexpected reply. Cancel the reply timer. If the maximum error count has been exceeded, behave according to the “Max invalid replies” event.	Security idle	19

7.3.2.5 Error messages

As described more formally in Table 18, stations may initially respond to error conditions by transmitting error messages. To help protect against denial-of-service attacks, all stations shall stop transmitting error messages after they have counted a number of errors that exceeds a preset maximum error count, described in 8.2.4.4. Any station may also choose not to send error messages at any time regardless of error count.

Note that error messages may be transmitted on communication links other than the one on which the error occurred. This may be extremely useful for detecting attacks and is therefore recommended. It is also recommended that all errors be logged. Note that following these recommendations requires user numbers to be unique across all connections to a particular controlled station.

7.3.3 Responder procedures

7.3.3.1 Responder role

A station, either controlling or controlled, that supplies authentication data shall be called a responder. Each responder shall follow the procedures described in this subclause.

7.3.3.2 Responding to challenges

A responder shall respond to a challenge message with a correctly-formed reply message within an acceptable reply timeout defined per system as described in 8.2.5.2.

A responder shall not proceed with further communications until it has successfully responded to the challenge message. This rule includes not responding to any subsequent challenge messages until the current challenge is completed.

7.3.3.3 Aggressive mode

Aggressive mode, in which a station supplies authentication information in the same ASDU as the data it is authenticating, shall be mandatory, but each station shall also provide a mode of operation in which aggressive mode can be configured as disabled.

A responder that uses aggressive mode shall place a correctly-formed aggressive mode request within the ASDU being authenticated. The location and the formatting of the aggressive mode request within the ASDU shall be specific to the protocol and described in the specifications of the affected protocol.

A responder shall not transmit an aggressive mode request until it has successfully responded to at least one challenge message.

7.3.4 Controlling station procedures

7.3.4.1 Controlling station role

In addition to acting as a challenger and a responder, controlling stations shall follow the procedures described in this subclause in order to initialize and change keys at the controlled station.

7.3.4.2 Changing session keys

There shall be two session keys, one used for authenticating data in the monitoring direction, and one for authenticating data transmitted in the control direction, as described in Table 2. The controlled and controlling stations shall maintain a unique set of session keys for each user of the controlled station and a default set of session keys used for cases when the master acts for multiple users (as in the case of a poll, for instance), or when the outstation initiates the security message sequence).

Each controlling station shall initialize the session keys upon establishing communications, and periodically change the session keys as described in Table 19. The change interval shall be set using a configurable parameter as discussed in 8.2.5.3.

The controlling station shall use a symmetric update key to encrypt the session keys and transmit it to the controlled station in a key change message. There shall be a separate update key for each user of the controlled station and a default update key for the default set of session keys.

7.3.4.3 Controlling station state machine

The controlling station shall execute the state machine in Table 19.