IEC 62351-6

Edition 1.0 2020-10

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Power systems management and associated information exchange – Data and communication security – Part 6: Security for IEC 61850

Gestion des systèmes de puissance et échanges d'informations associés – Sécurité des communications et des données – Partie 6: Sécurité pour l'IEC 61850

IEC 62351-6:2020-10(en-fr)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

About the IEC
The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

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 corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
67 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

A propos de l'IEC
La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications IEC
Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Recherche de publications IEC - webstore.iec.ch/advsearchform
La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études,…). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished
Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et une fois par mois par email.

Service Clients - webstore.iec.ch/csc
Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: sales@iec.ch.

Electropedia - www.electropedia.org
Le premier dictionnaire d'électrotechnologie en ligne au monde, avec plus de 22 000 articles terminologiques en anglais et en français, ainsi que les termes équivalents dans 16 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Glossaire IEC - std.iec.ch/glossary
67 000 entrées terminologiques électrotechniques, en anglais et en français, extraites des articles Termes et Définitions des publications IEC parues depuis 2002. Plus certaines entrées antérieures extraites des publications des CE 37, 77, 86 et CISPR de l'IEC.

IEC 62351-6

Edition 1.0 2020-10

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Power systems management and associated information exchange – Data and communication security – Part 6: Security for IEC 61850

Gestion des systèmes de puissance et échanges d'informations associés – Sécurité des communications et des données – Partie 6: Sécurité pour l'IEC 61850

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

ICS 33.200

ISBN 978-2-8322-9166-5

Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

____

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

Part 6: Security for IEC 61850

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) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 62351-6 has been prepared by IEC technical committee 57: Power systems management and associated information exchange.

The text of this International Standard is based on the following documents:

FDIS	Report on voting
57/2234/FDIS	57/2258/RVD

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

This document has been drafted in accordance with the ISO/IEC Directives, Part 2.

A list of all parts of the IEC 62351 series, published 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 document will remain unchanged until the stability date indicated on the IEC website under "http://webstore.iec.ch" in the data related to the specific document. At this date, the document will be

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

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 document using a colour printer.

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

Part 6: Security for IEC 61850

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 IEC 61850 series. This document applies to at least those protocols listed in Table 1.

Table 1 – Scope of application to standards

Number	Name
IEC 61850-8-1	Communication networks and systems for power utility automation – Part 8-1: Specific communication service mapping (SCSM) – Mappings to MMS (ISO/IEC 9506-1 and ISO/IEC 9506-2) and to ISO/IEC 8802-3
IEC 61850-8-2	Communication networks and systems for power utility automation – Part 8-2: Specific communication service mapping (SCSM) – Mapping to Extensible Messaging Presence Protocol (XMPP)
IEC 61850-9-2	Communication networks and systems for power utility automation – Part 9-2: Specific communication service mapping (SCSM) – Sampled values over ISO/IEC 8802-3
IEC 61850-6	Communication networks and systems for power utility automation – Part 6: Configuration description language for communication in power utility automation systems related to IEDs

The initial audience for this document is intended to be the members of the working groups developing or making use of 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 document is intended to be the developers of products that implement these protocols.

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

1.2 Namespace name and version

This new clause is mandatory for any IEC 61850 namespace (as defined by part 7-1 of IEC 61850 Edition 2).

The parameters which identify this new release of this namespace are:

- Namespace version: 2020
- Namespace revision: A
- Namespace name: “IEC 62351-6:2020A”
- Namespace release: 1

The table below provides an overview of all published versions of this namespace.

Edition	Publication date	Webstore	Namespace
Edition 1.0	2020-?	IEC 62351-6:2020	IEC 62351-6:2020

1.3 Code Component distribution

There is currently no code component scheduled for the code component downloading area.

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 61850-6, *Communication networks and systems for power utility automation – Part 6: Configuration description language for communication in electrical substations related to IEDs*

IEC 61850-7-3, *Communication networks and systems for power utility automation – Part 7-3: Basic communication structure – Common data classes*

IEC 61850-8-1, *Communication networks and systems for power utility automation – Part 8-1: Specific communication service mapping (SCSM) – Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3*

IEC 61850-8-2, *Communication networks and systems for power utility automation – Part 8-2: Specific communication service mapping (SCSM) – Mapping to Extensible Messaging Presence Protocol (XMPP)*

IEC 61850-9-2, *Communication networks and systems for power utility automation – Part 9-2: Specific communication service mapping (SCSM) – Sampled values over ISO/IEC 8802-3*

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 62351-4:2020, *Power systems management and associated information exchange – Data and communications security – Part 4: Profiles including MMS and derivatives*

IEC 62351-9, *Power systems management and associated information exchange – Data and communications security – Part 9: Cyber security key management for power system equipment*

ISO/IEC 13239, *Information technology – Telecommunications and information exchange between systems – High-level data link control (HDLC) procedures*

ISO/IEC 9594-8 | Rec. ITU-T X.509: *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*

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

RFC 5905, *Network Time Protocol Version 4: Protocol and Algorithms Specification*[1]

RFC 8052, *Group Domain of Interpretation (GDOI) Protocol Support for IEC 62351 Security Services*

NIST Special Publication 800-38D, *Recommendation for Block Cipher Modes of Operation Galois/Counter Mode (GCM and GMAC)*

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC TS 62351-2 and IEC 61850-2 apply.

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

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

3.1.1
electronic security perimeter
logical border surrounding a network interconnecting critical cyber assets

3.1.2
client
functional unit that establishes an association and issues requests and receives services from a server.

3.1.3
server
functional unit that receives an association from a Client and provides services requested by the Client

3.2 Abbreviated terms

ACSE	Association Control Service Element
APDU	Application Protocol Data Unit
ASDU	Application Service Data Unit
ASN.1	Abstract Syntax Notation One
ESP	Electronic Security Perimeter
GDOI	Group Domain of Interpretation
GMAC	Galois Message Authentication Code
GOOSE	Generic Object Oriented Substation Event
GSE	Generic Substation Events
HMAC	Hashed Message Authentication Code
ICT	IED Configuration Tool
IED	Intelligent Electronic Device
KFA	Key Delivery Assurance

[1] Restricted to SNTP profile only.

KDC Key Distribution Centre
MAC Message Authentication Code
SMV Sampled Measured Values
SCL Substation Configuration Language
SV Sampled Value

4 Security issues addressed by this document

4.1 Operational issues affecting choice of security options

For applications using Layer 2 IEC 61850-8-1 GOOSE and Layer 2 IEC 61850-9-2 Sampled Value and requiring 3 ms response times, multicast configurations and low CPU overhead, encryption is not recommended. Instead, the communication path selection process (e.g. the fact that Layer 2 GOOSE and SV are supposed to be restricted to a logical substation LAN) shall be used to provide confidentiality for information exchanges. However, this document does define a mechanism for allowing confidentiality for applications where the 3 ms delivery criterion is not a concern.

NOTE The actual performance characteristics of an implementation claiming conformance to this technical specification is outside the scope of this document.

With the exception of confidentiality, this document sets forth a mechanism that allows co-existence of secure and non-secure PDUs.

4.2 Security threats countered

See IEC TS 62351-1 for a discussion of security threats and attack methods.

If encryption is not employed, then the specific threats countered in this clause include:

- unauthorized modification (tampering) of information through message level authentication of the messages.

If encryption is employed, then the specific threats countered in this clause include:

- unauthorized access to information through message level authentication and encryption of the messages;
- unauthorized modification (tampering) or theft of information through message level authentication and encryption of the messages.
- information disclosure is countered.

4.3 Attack methods countered

The following security attack methods are intended to be countered through the appropriate implementation of the specifications/recommendations found within this document:

- man-in-the-middle: this threat will be countered through the use of a Message Authentication Code mechanism specified within this document;
- tamper detection/message integrity: These threats will be countered through the algorithm used to create the authentication mechanism as specified within this document;
- replay: this threat will be countered through the use of specialized processing state machines specified within IEC 62351-4 and this document.

5 Correlation of IEC 61850 parts and IEC 62351 parts

5.1 General

There are four levels of interaction between the parts of the IEC 62351 series and parts of the IEC 61850 series. This part is concerned with the:

- Communication profile security regarding:
  - IEC 61850-8-1 Application Profile for Client/Server communications.
  - IEC 61850-8-2 Application Profile for Client/Server communications.
  - IEC 61850-8-1 Layer 2 T-Profile for GOOSE/GSE
  - IEC 61850-8-1 Layer 2 T-Profile for Multicast Sampled Values
  - IEC 61850-8-1 Layer 3 Routable GOOSE and Sampled Values
- Configuration extensions required for configuration of the Application and Transport communication profiles of concern. These extensions would impact IEC 61850-6.
- Object definitions, regarding security and identification, that are exposed at run-time as part of the IEC 61850-8-1 and IEC 61850-8-2 object mappings.
- The binding of Originator ID values to authenticated peers for Client/Server services.

The scope of this document provides security specifications for use within an Electronic Security Perimeter (ESP) and between ESPs.

5.2 IEC 61850-8-1 Profile for Client/Server communications

5.2.1 General

IEC 61850 implementations claiming conformance to this specification and declaring support for the IEC 61850-8-1 profile utilizing TCP/IP and ISO 9506 (MMS) shall implement Clauses 5 and 6 of IEC 62351-4:2020.

IEC 61850-8-1 specifies the use of MMS within a substation. However, the scope of this specification provides security specifications for use within the substation and external to the substation (e.g. Control Centre to Substation).

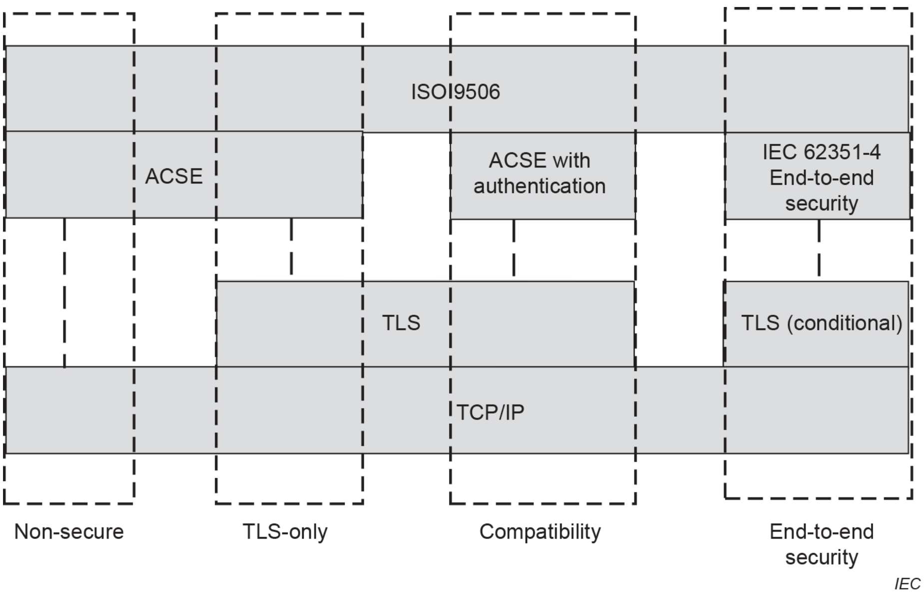

Figure 1 – MMS Security Profiles

Figure 1 shows the security profiles for IEC 61850 Client/Server associations based upon ISO/IEC 9506:

- Non-Secure: Implementations claiming conformance to this clause and Client/Server capability shall support the ability to be configured without securing connections per IEC 62351-4.
- TLS-Only: The use of TLS only is out-of-scope of this document. This profile may not provide the ability to provide user level Role Based Access Control (RBAC) for all use cases.
- Compatibility (per IEC 62351-4): Client implementations claiming conformance shall support the configuration and exchange of information utilizing ACSE Authentication per IEC 62351-4 and TLS. The use of TLS is mandatory.
- End-to-End: The support for this security profile is optional. However, in future editions of this standard, it is intended to make the support of this profile mandatory.

See Table 6 for a formal conformance statement.

5.2.2 Control centre to substation

IEC 62351-4 shall be used without any other additions.

5.2.3 Substation communications

The mandatory cipher suites are found in IEC 62351-4.

5.3 IEC 61850 security for profiles using VLAN IDs

For the IEC 61850 profiles specified that make use of VLAN IDs (e.g. IEC 61850-8-1 GOOSE, and IEC 61850-9-2) profile security shall be provided as specified in Clause 8.

5.4 IEC 61850-8-2 for Client/Server communications

IEC 61850 implementations claiming conformance to this document and declaring support for the IEC 61850-8-2 A-Profile for Client/Server communications shall implement the End-to-End security mechanism as specified by IEC 62351-4.

IEC 61850-8-2 does not support ACSE therefore, the IEC 62351-4 security mechanism of ACSE authentication (A-Profile) are not implemented or supported.

Additionally, IEC 61850-8-2 utilizes a T-Profile consisting of XMPP, which in turn controls TLS. Therefore, the TLS security mechanisms, and cipher suites, specified in IEC 62351-4 are out-of-scope for IEC 61850-8-2.

5.5 Using OriginatorID for Client/Server Services

There are several Common Data Classes (CDCs) defined in IEC 61850-7-3 and service tracking functions that explicitly define the ability to provide information about the originator of the control or service. The actual value representing the initiating entity in both IEC 61850-8-1 and IEC 61850-8-2 is originatorID and is a 64-octet octetstring.

The use of certificate-based authentication and security provides a mechanism for providing authoritative information regarding the originator. However, the size restriction of originatorID is not large enough to provide exposure of the Issuer and Serial Number. Therefore, implementations claiming conformance to this standard shall implement the optional DataAttribute certIssuer in the instance to the IEC 61850-7-3 CDCs of: CST, BTS, UTS, LTS, GTS, MTS, NTS, and STS.

The use of the value of the certIssuer Data Attribute follows:

- The value shall be a concatenation of the sequence of name values that may be present in the Issuer field. If there is more than one name in the sequence, the concatenation token shall be the "\" character, i.e. have a zero(0) length value if the client association is not authenticated.
- Have the value of the X.509 Issuer Name for a client association that is authenticated.
- If the concatenated value is greater than 255 characters, the value shall be truncated to 255 characters.
- If the client association was not authenticated through the use of certificates, the length of the certIssuer shall be zero(0) and therefore the value shall be NULL. All octets in the value shall be initialized to 0.

Implementations claiming conformance to this standard shall also utilize the originatorID Data Attribute as follows:

- If the certIssuer value is not NULL, the value of the X.509 certificate serial number shall be used for the value for clients associations that have been authenticated by use of a certificate. A certificate serial number is an encoded positive integer value. The encoded value shall be copied into the originatorID value, not including the tag or length.
- If the certIssuer value is NULL, the value of the originatorID may be "unknown" with "u" being the most significant octet of the value. Other values are a local issue.

6 Multicast Association Protocols

6.1 General

IEC 61850-8-1 and IEC 61850-9-2 specify two different application protocols that utilize the IEC 61850 Multicast Association model. These are GSE (e.g. GOOSE) and Multicast Sampled Values. These application protocols are mapped over two different T-Profile mappings.

The T-Profiles specified provide a Layer 2 and a Routable mapping of the application protocol. The combination of the A-Profiles and T-Profiles are commonly referred to as as Layer 2 or Routable (e.g. Layer 2 GOOSE or Routable GOOSE). This document specifies security behaviours that are common regardless of the T-Profile and specific security protocol extensions for the Layer 2 T-Profiles.

This clause specifies the expected behaviours for replay protection for both GOOSE and Multicast Sampled Values regardless of the T-Profile utilized.

6.2 Replay Protection

Replay protection can be implemented for GOOSE and Sampled Value A-Profiles with or without security extensions. The replay protection algorithms specified in the following clauses are for subscribers claiming conformance to this part and therefore replay protection is to be implemented regardless if the published GOOSE or Sampled Value APDU has security. The replay protection algorithm is implemented by the subscriber

6.2.1 GOOSE replay protection

6.2.1.1 General

The normal GOOSE subscriber state machine in IEC 61850-8-1 does not detail how to transition out-of-order state numbers (stNum) or sequence numbers (sqNum) should be received.

Implementations claiming conformance to this standard shall implement the state machine shown in Figure 2. Additional security and replay checks may be implemented. For this clause, the Application is defined as the GOOSE Subscriber function and not the actual process that utilizes GOOSEData (per IEC 61850-7-2) in order to perform protection, etc.

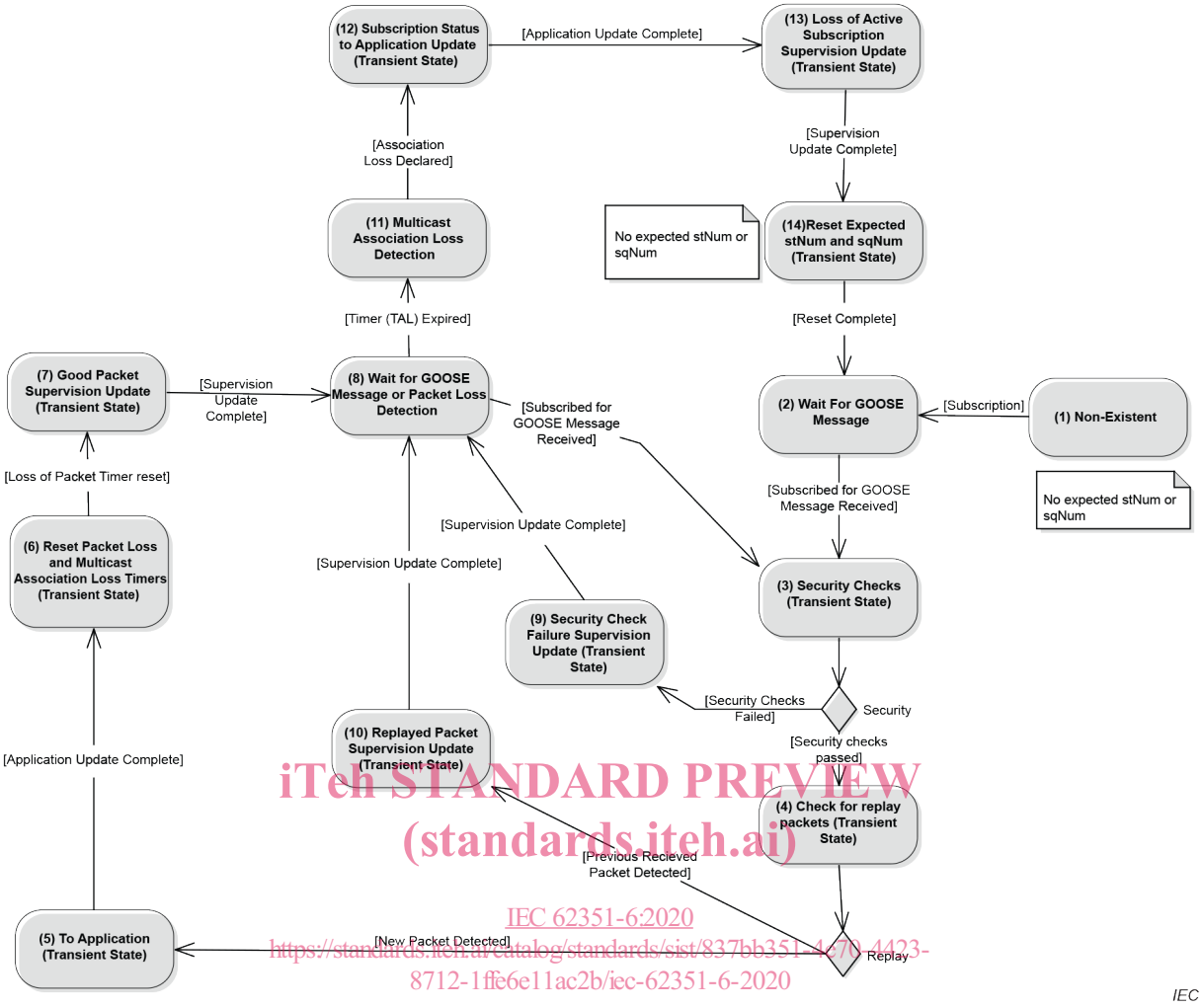

Figure 2 – Replay Protection State Machine for GOOSE

Figure 2 is relevant for GOOSE messages for which the subscriber has an active subscription shall be configured through the use of SCL and an ICT. Other configuration mechanisms are out-of-scope. Implementations claiming conformance to this clause shall maintain at least the following internal state machine variables: last received stNum (lastRcvStNum); last received sqNum (lastRcvSqNum); last received state change timestamp (lastRcvT); and an internal Time Allowed to Live (intTAL) value. The states and their transitions are defined as follows:

1) The Non-Existent state represents the state when there is no GOOSE subscription.
2) Upon activating the subscription (e.g. power-up or subscription configuration), the state machine will internally set the lastRcvStNum , lastRcvSqNum, lastRcvT, and intTAL to invalid since no GOOSE message has been received and the state machine transitions to the Wait for GOOSE Message state.

   Upon receiving the subscribed GOOSE message, the subscriber shall transition to the Security Checks state (State 3).
3) The processing in the Security Checks state is described in 6.2.1.2.

   If the Subscriber has never received a key from the KDC, it shall pass the security check for non-encrypted packets and perform a GROUP-PULL as defined by IEC 62351-9. Subscribers receiving an encrypted GOOSE messages, and not having the key for the ID conveyed in the GOOSE message shall transition to Security Check Failure and shall perform a GROUP-PULL as defined by IEC 62351-9.

   If the subscriber has been unable to receive keys prior to the expiration of the last key delivered, it shall report an alarm indicating that key delivery has failed and that expired keys are being assumed. It shall process packets whose keyID is the last key delivered.