



INTERNATIONAL STANDARD

NORME INTERNATIONALE



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

**Gestion des systèmes de puissance et échanges d'informations associés –
Sécurité des communications et des données –
Partie 5: Aspects de sécurité pour l'IEC 60870-5 et ses dérivés**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 33.200

ISBN 978-2-8322-6017-3

**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

FOREWORD.....	6
1 Scope.....	8
2 Normative references	9
3 Terms and definitions	10
4 Abbreviated terms	11
5 Problem description.....	12
5.1 Overview of clause	12
5.2 Specific threats addressed.....	12
5.3 Design issues	12
5.3.1 Overview of subclause.....	12
5.3.2 Asymmetric communications.....	12
5.3.3 Message-oriented	12
5.3.4 Poor sequence numbers or no sequence numbers.....	13
5.3.5 Limited processing power	13
5.3.6 Limited bandwidth.....	13
5.3.7 No access to authentication server	13
5.3.8 Limited frame length	13
5.3.9 Limited checksum	14
5.3.10 Radio systems	14
5.3.11 Dial-up systems	14
5.3.12 Variety of protocols affected	14
5.3.13 Differing data link layers	14
5.3.14 Long upgrade intervals	15
5.3.15 Remote sites	15
5.3.16 Unreliable media	15
5.4 General principles.....	15
5.4.1 Overview of subclause.....	15
5.4.2 Application layer only	15
5.4.3 Generic definition mapped onto different protocols	15
5.4.4 Bi-directional	15
5.4.5 Management of cryptographic keys.....	15
5.4.6 Backwards tolerance	16
5.4.7 Upgradeable.....	16
5.4.8 Multiple connections	16
6 Theory of operation	16
6.1 Overview of clause	16
6.2 The secure communication	16
6.2.1 Basic concepts	16
6.2.2 Association ID	17
6.2.3 Authenticating	18
6.2.4 Central Authority.....	18
6.2.5 Role Based Access Control (RBAC).....	18
6.2.6 Cryptographic keys	18
6.2.7 Security statistics	22
6.2.8 Security events.....	22
7 Functional requirements	22

7.1	Overview of clause	22
7.2	Procedures Overview	22
7.3	State machine overview	23
7.4	Timers and counters	25
7.5	Security statistics and events	25
7.5.1	General	25
7.5.2	Special security thresholds	29
7.5.3	Security statistics reporting	29
7.5.4	Security events monitoring and logging	29
8	Formal procedures	30
8.1	Overview of subclause	30
8.2	Distinction between messages and ASDUs	30
8.2.1	General	30
8.2.2	Messages datatypes and notations	30
8.3	Station Association procedure	30
8.3.1	General	30
8.3.2	Public key certificates	31
8.3.3	Configuration of authorized remote stations	33
8.3.4	Pre-requisites to initiate the Station Association procedure	33
8.3.5	Messages definition	33
8.3.6	Controlling station state machine	42
8.3.7	Controlled station state machine	52
8.3.8	Verification of remote station's certificate	61
8.3.9	Verification of certificates during normal operations	61
8.3.10	Update Keys derivation	62
8.3.11	Controlling station directives for Station Association and Update Keys management	63
8.3.12	Controlled station directives for Station Association and Update Keys management	63
8.3.13	Initializing and updating Stations Association and Update Keys	65
8.4	Session Key Change procedure	66
8.4.1	General	66
8.4.2	Messages definition	67
8.4.3	Controlling station state machine	76
8.4.4	Controlled station state machine	85
8.4.5	Controlling station directives for Session Keys management	93
8.4.6	Controlled station directives for Session Keys management	93
8.4.7	Initializing and changing Session Keys	94
8.5	Secure Data Exchange	95
8.5.1	General	95
8.5.2	Messages definition	96
8.5.3	Controlling station state machine	100
8.5.4	Controlled station state machine	105
8.5.5	Controlling station directives for Secure Data Exchange	109
8.5.6	Controlled station directives for Secure Data Exchange	109
8.5.7	Example of Secure Data exchange during Station Association	110
8.5.8	Example of Secure Data Exchange during Session Key Change	111
9	Interoperability requirements	113
9.1	Overview of clause	113

9.2	Minimum requirements	113
9.2.1	Overview of subclause	113
9.2.2	Authentication algorithms	113
9.2.3	Key wrap / transport algorithms	113
9.2.4	Cryptographic keys	114
9.2.5	Cryptographic curves	114
9.2.6	Configurable values	114
9.2.7	Cryptographic information	116
9.3	Options	116
9.3.1	Overview of subclause	116
9.3.2	MAC/AEAD algorithms	117
9.3.3	Key wrap / transport algorithms	117
9.3.4	Cryptographic curves	117
9.4	Use with TCP/IP	117
9.5	Use with redundant channels	117
10	Requirements for referencing this standard	118
10.1	Overview of clause	118
10.2	Selected options	118
10.3	Message format mapping	118
10.4	Reference to procedures	118
10.5	Protocol information	118
10.6	Controlled station response to unauthorized operations requests	119
10.7	Transmission of security statistics	119
10.8	Configurable values	119
10.9	Protocol implementation conformance statement	119
Annex A (informative)	Security Event mapping to IEC 62351-14	120
A.1	General	120
A.2	Mapping of IEC 62351-5 events specified in this document	120
Bibliography	122
Figure 1	– Overview of interaction between Central Authority and stations	21
Figure 2	– Sequence of procedures	23
Figure 3	– Station Association procedure	34
Figure 4	– Station Association – Controlling station state machine	43
Figure 5	– Station Association – Controlled station state machine	53
Figure 6	– Example of Association ID, Update Keys and Session Keys initialization	66
Figure 7	– Session Key Change procedure	67
Figure 8	– Session Key Change – Controlling station state machine	77
Figure 9	– Session Key Change – Controlled station state machine	86
Figure 10	– Example of Session Key initialization and periodic update	95
Figure 11	– Secure Data Exchange	96
Figure 12	– Secure Data Exchange – Controlling station state machine	101
Figure 13	– Secure Data Exchange – Controlled station state machine	106
Figure 14	– Example of Secure Data Exchange during Station Association	111
Figure 15	– Example of Secure Data messages exchanged during Session Key Change	112

Table 1 – Scope of application to standards.....	8
Table 2 – Summary of symmetric keys used	19
Table 3 – Summary of asymmetric keys used	19
Table 4 – States used in the controlling station state machine	24
Table 5 – States used in the controlled station state machine	24
Table 6 – Summary of timers and counters used.....	25
Table 7 – Security statistics and associated events	26
Table 8 – Elliptic curves.....	31
Table 9 – Association Request message.....	35
Table 10 – Association Response message	36
Table 11 – Update Key Change Request message.....	38
Table 12 – Data Included in MAC calculation (in order).....	40
Table 13 – Update Key Change Response message.....	40
Table 14 – Data Included in MAC calculation (in order).....	41
Table 15 – Controlling station state machine: Station Association	44
Table 16 – Controlled station state machine: Station Association.....	54
Table 17 – List of pre-defined role-to-permission assignment.....	64
Table 18 – Session Request message	68
Table 19 – Session Response message.....	70
Table 20 – Data Included in MAC calculation (in order).....	71
Table 20 – Session Key Change Request message	72
Table 21 – Data Included in WKD (in order).....	73
Table 22 – Example of Session Key order.....	74
Table 23 – Data Included in the MAC calculation (in order).....	74
Table 25 – Session Key Change Response message.....	75
Table 26 – Data Included in the MAC calculation (in order).....	75
Table 27 – Controlling station state machine: Session Key Change	78
Table 28 – Controlled station state machine: Session Key Change	87
Table 29 – Secure Data message	97
Table 29 – Secure Data Payload using MAC algorithm	98
Table 31 – Data included in the MAC calculation in Secure Data Payload (in order).....	99
Table 32 – AEAD algorithm parameters to generate the Secure Data Payload (in order).....	99
Table 33 – Controlling station state machine: Secure Data Exchange	102
Table 34 – Controlled station state machine: Secure Data Exchange	107
Table 35 – Configuration of cryptographic information	116
Table 36 – Legend for configuration of cryptographic information.....	116
Table A.1 – Security event logs defined in IEC 62351-5 Ed.1 mapped to IEC 62351-14	120

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 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.

IEC 62351-5 has been prepared by IEC technical committee 57: Power systems management and associated information exchange. It is an International Standard.

This International Standard cancels and replaces IEC TS 62351-5 published in 2013. It constitutes a technical revision. The primary changes in this International Standard are:

- a) The secure communication mechanism is performed on per controlling station/controlled station association.
- b) User management to add, change or delete a User, was removed.
- c) Symmetric method to change the Update Key was removed.
- d) Asymmetric method to the change Update Key was reviewed.
- e) Challenge/Reply procedure and concepts were removed.
- f) Aggressive Mode concept was replaced with the Secure Data message exchange mechanism.
- g) Authenticated encryption of application data was added.

- h) The list of permitted security algorithms has been updated.
- i) The rules for calculating messages sequence numbers have been updated
- j) Events monitoring and logging was added.

NOTE The following print types are used:

CAPITALIZATION has been used in the text of this document to formally identify the most important components of the described security mechanism. These components include: 1) data items e.g. Update Keys, Session Keys; 2) procedure names, e.g. Station Association, Session Key Change; message names, e.g. Association Request, Session Request; 3) state names, e.g. Session Established, Wait for Session Response; 4) statistics e.g. Authentication Errors, Unexpected Messages and 5) event names e.g. Reply Timeout, Rx Invalid Session Key Change.

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

Draft	Report on voting
57/2516/FDIS	57/2555/RVD

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

The language used for the development of this International Standard is English.

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

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

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

IMPORTANT – The "colour inside" logo on the cover page of this document 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 COMMUNICATIONS SECURITY –

Part 5: Security for IEC 60870-5 and derivatives

1 Scope

This part of IEC 62351 defines the application profile (A-profile) secure communication mechanism specifying messages, procedures and algorithms for securing the operation of all protocols based on or derived from IEC 60870-5, *Telecontrol Equipment and Systems – Transmission Protocols*. This document 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	Companion 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 (defined in IEEE Std 1815, based on IEC 60870-1 through IEC 60870-5 and maintained jointly by the DNP Users Group and the IEEE)

The initial audience for this document is intended to be the members of the working groups developing the protocols listed in Table 1.

For the measures described in this document 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 working groups in charge of taking this document to the specific protocols listed in Table 1 may choose not to do so.

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.

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 define the interoperability requirements for this secure communication mechanism, including the relationship of this standard to IEC 62351-3 for transport layer security..
- Clause 10 describes the requirements for other standards referencing this document.

The actions of an organization in response to events and error conditions described in this document are expected to be defined by the organization's security policy and they are beyond the scope of this document.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 60870-5 (all parts), *Telecontrol equipment and systems – Part 5: Transmission protocols*

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

IEC 62351-7, *Power systems management and associated information exchange – Data and communications security – Part 7: Network and System Management (NSM) data object models*

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

IEC 62351-14, *Power systems management and associated information exchange – Data and communications security – Part 14: Cyber security event logging¹*

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

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

IETF RFC 5116, *An Interface and Algorithms for Authenticated Encryption*

IETF RFC 5869, *HMAC-based Extract-and-Expand Key Derivation Function (HKDF)*

IETF RFC 7693, *The BLAKE2 Cryptographic Hash and Message Authentication Code (MAC)*

IETF RFC 7748, *Elliptic Curve for Security*

SEC2-V2, *Standards for Efficient Cryptography SEC2: Recommended Elliptic Curve Domain Parameters – Version 2.0*

¹ Under preparation. Stage at the time of publication: IEC ACDV 62351-14:2021.

SOMMAIRE

AVANT-PROPOS	128
1 Domaine d'application	130
2 Références normatives	131
3 Termes et définitions	132
4 Abréviations	133
5 Description de problème	134
5.1 Vue d'ensemble de l'article	134
5.2 Menaces spécifiques traitées	134
5.3 Problèmes de conception	134
5.3.1 Vue d'ensemble du paragraphe	134
5.3.2 Communications asymétriques	134
5.3.3 Orientés message	135
5.3.4 Numéros de séquence faibles ou absence de numéros de séquence	135
5.3.5 Puissance de traitement limitée	135
5.3.6 Largeur de bande limitée	135
5.3.7 Pas d'accès au serveur d'authentification	136
5.3.8 Longueur de trame limitée	136
5.3.9 Somme de contrôle limitée	136
5.3.10 Systèmes radio	136
5.3.11 Systèmes commutés	136
5.3.12 Diversité des protocoles concernés	137
5.3.13 Couches liaison de données différentes	137
5.3.14 Intervalles d'amélioration longs	137
5.3.15 Sites à distance	137
5.3.16 Supports peu fiables	137
5.4 Principes généraux	137
5.4.1 Vue d'ensemble du paragraphe	137
5.4.2 Couche application seulement	138
5.4.3 Définition générique mise en correspondance avec différents protocoles	138
5.4.4 Bidirectionnel	138
5.4.5 Gestion des clés cryptographiques	138
5.4.6 Rétrotolérance	138
5.4.7 Possibilité de mise à jour	138
5.4.8 Connexions multiples	139
6 Théorie de fonctionnement	139
6.1 Vue d'ensemble de l'article	139
6.2 Communication sécurisée	139
6.2.1 Concepts fondamentaux	139
6.2.2 ID d'Association	140
6.2.3 Authentification	140
6.2.4 Autorité Centrale	141
6.2.5 Contrôle d'Accès Basé sur les Rôles (RBAC)	141
6.2.6 Clés cryptographiques	141
6.2.7 Statistiques de sécurité	145
6.2.8 Événements de sécurité	145
7 Exigences fonctionnelles	145

7.1	Vue d'ensemble de l'article	145
7.2	Vue d'ensemble des procédures	145
7.3	Vue d'ensemble des diagrammes d'états	146
7.4	Horloges et compteurs	148
7.5	Statistiques de sécurité et événements	149
7.5.1	Généralités	149
7.5.2	Seuils de sécurité spéciaux	153
7.5.3	Rapport des statistiques de sécurité	153
7.5.4	Surveillance et enregistrement des événements de sécurité	154
8	Procédures formelles	154
8.1	Vue d'ensemble du paragraphe	154
8.2	Distinction entre messages et ASDU	154
8.2.1	Généralités	154
8.2.2	Types des données et notations des messages	155
8.3	Procédure d'Association de Poste	155
8.3.1	Généralités	155
8.3.2	Certificats de clés publiques	155
8.3.3	Configuration des postes distants autorisés	158
8.3.4	Conditions préalables pour initier la procédure d'Association de Poste	158
8.3.5	Définition des messages	158
8.3.6	Diagramme d'état du poste de conduite	167
8.3.7	Diagramme d'état du poste téléconduit	180
8.3.8	Vérification du certificat du poste distant	190
8.3.9	Vérification des certificats pendant les opérations normales	191
8.3.10	Dérivation des Clés de Mise à Jour	191
8.3.11	Directives du poste de conduite pour la gestion de l'Association de Poste et des Clés de Mise à Jour	192
8.3.12	Directives du poste téléconduit pour la gestion de l'Association de Poste et des Clés de Mise à Jour	192
8.3.13	Initialisation et mise à jour d'Associations de Postes et de Clés de Mise à Jour	195
8.4	Procédure de Modification de Clé de Session	196
8.4.1	Généralités	196
8.4.2	Définition des messages	197
8.4.3	Diagramme d'état du poste de conduite	206
8.4.4	Diagramme d'état du poste téléconduit	219
8.4.5	Directives du poste de conduite pour la gestion des Clés de Session	229
8.4.6	Directives du poste téléconduit pour la gestion des Clés de Session	229
8.4.7	Initialisation et modification des Clés de Session	230
8.5	Échange de Données Sécurisées	231
8.5.1	Généralités	231
8.5.2	Définition des messages	232
8.5.3	Diagramme d'état du poste de conduite	236
8.5.4	Diagramme d'état du poste téléconduit	243
8.5.5	Directives du poste de conduite pour l'Échange de Données Sécurisées	249
8.5.6	Directives du poste téléconduit pour l'Échange de Données Sécurisées	250
8.5.7	Exemple d'Échange de Données Sécurisées pendant l'Association de Poste	250
8.5.8	Exemple d'Échange de Données Sécurisées pendant la Modification de Clé de Session	252

9	Exigences d'interopérabilité	254
9.1	Vue d'ensemble de l'article	254
9.2	Exigences minimales	254
9.2.1	Vue d'ensemble du paragraphe	254
9.2.2	Algorithmes d'authentification	254
9.2.3	Algorithmes d'enveloppement/transport de clé	254
9.2.4	Clés cryptographiques	255
9.2.5	Courbes cryptographiques	255
9.2.6	Valeurs configurables	255
9.2.7	Informations cryptographiques	257
9.3	Options	258
9.3.1	Vue d'ensemble du paragraphe	258
9.3.2	Algorithmes de MAC/AEAD	258
9.3.3	Algorithmes d'enveloppement/transport de clé	258
9.3.4	Courbes cryptographiques	259
9.4	Utilisation avec TCP/IP	259
9.5	Utilisation avec canaux redondants	259
10	Exigences de référencement de la présente norme	259
10.1	Vue d'ensemble de l'article	259
10.2	Options choisies	259
10.3	Mise en correspondance du format de message	259
10.4	Références aux procédures	260
10.5	Information de protocole	260
10.6	Réponse du poste téléconduit aux requêtes d'opérations non autorisées	260
10.7	Transmission des statistiques de sécurité	260
10.8	Valeurs configurables	260
10.9	Déclaration de conformité de la mise en œuvre d'un protocole	260
Annex A (informative)	Mise en correspondance des Événements de Sécurité avec l'IEC 62351-14	261
A.1	Généralités	261
A.2	Mise en correspondance des événements définis dans l'IEC 62351-5, spécifiés dans le présent document	261
Bibliographie	263
Figure 1	– Vue d'ensemble de l'interaction entre l'Autorité Centrale et les postes	144
Figure 2	– Séquence des procédures	146
Figure 3	– Procédure d'Association de Poste	159
Figure 4	– Association de Poste – Diagramme d'état du poste de conduite	170
Figure 5	– Association de Poste – Diagramme d'état du poste téléconduit	182
Figure 6	– Exemple d'initialisation d'ID d'Association, de Clés de Mise à Jour et de Clés de Session	196
Figure 7	– Procédure de Modification de Clé de Session	197
Figure 8	– Modification de Clé de Session – Diagramme d'état du poste de conduite	209
Figure 9	– Modification de Clé de Session – Diagramme d'état du poste téléconduit	222
Figure 10	– Exemple d'initialisation et de mise à jour périodique de Clé de Session	231
Figure 11	– Échange de Données Sécurisées	232
Figure 12	– Échange de Données Sécurisées – Diagramme d'état du poste de conduite	238
Figure 13	– Échange de Données Sécurisées – Diagramme d'état du poste téléconduit	245

Figure 14 – Exemple d’Échange de Données Sécurisées pendant l’Association de Poste	251
Figure 15 – Exemple de messages de Données Sécurisées échangés pendant la Modification de Clé de Session	253
Tableau 1 – Domaine d'application aux normes	130
Tableau 2 – Résumé des clés symétriques utilisées	141
Tableau 3 – Résumé des clés asymétriques utilisées.....	142
Tableau 4 – États utilisés dans le diagramme d’état du poste de conduite	147
Tableau 5 – États utilisés dans le diagramme d’état du poste téléconduit	148
Tableau 6 – Résumé des horloges et compteurs utilisés.....	149
Tableau 7 – Statistiques de sécurité et événements associés	150
Tableau 8 – Courbes cryptographiques elliptiques	156
Tableau 9 – Message de Requête d’Association	160
Tableau 10 – Message de Réponse d’Association	161
Tableau 11 – Message de Requête de Modification de Clé de Mise à Jour	163
Tableau 12 – Données incluses dans le calcul de MAC (dans cet ordre).....	165
Tableau 13 – Message de Réponse de Modification de Clé de Mise à Jour.....	166
Tableau 14 – Données incluses dans le calcul de MAC (dans cet ordre).....	167
Tableau 15 – Diagramme d’état du poste de conduite: Association de Poste	171
Tableau 16 – Diagramme d’état du poste téléconduit: Association de Poste	183
Tableau 17 – Liste d’affectations rôle-permission prédéfinies	194
Tableau 18 – Message de Requête de Session.....	198
Tableau 19 – Message de Réponse de Session	200
Tableau 20 – Données incluses dans le calcul MAC (dans l'ordre).....	201
Tableau 20 – Message de Requête de Modification de Clé de Session	202
Tableau 21 – Données incluses dans les WKD (dans cet ordre).....	204
Tableau 22 – Exemple d’ordre de Clé de Session	204
Tableau 23 – Données incluses dans le calcul de MAC (dans cet ordre).....	205
Tableau 24 – Message de Réponse de Modification de Clé de Session	205
Tableau 26 – Données incluses dans le calcul de MAC (dans cet ordre).....	206
Tableau 27 – Diagramme d’état du poste de conduite: Modification de Clé de Session	209
Tableau 27 – Diagramme d’état du poste téléconduit: Modification de Clé de Session	222
Tableau 28 – Message de Données Sécurisées	233
Tableau 29 – Données Utiles des Données Sécurisées utilisant un algorithme de MAC	234
Tableau 31 – Données incluses dans le calcul de MAC dans les Données Utiles des Données Sécurisées (dans cet ordre)	235
Tableau 32 – Paramètres d'algorithme de AEAD pour générer les Données Utiles des Données Sécurisées (dans cet ordre)	236
Tableau 33 – Diagramme d’état du poste de conduite: Échange de Données Sécurisées.....	239
Tableau 33 – Diagramme d’état du poste téléconduit: Échange de Données Sécurisées.....	246
Tableau 34 – Configuration des informations cryptographiques.....	257
Tableau 35 – Légende pour la configuration des informations cryptographiques	258
Tableau A.1 – Journaux des événements d’enregistrement de sécurité définis dans l’IEC 62351-5 Éd. 1, mis en correspondance avec l’IEC 62351-14	261

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

GESTION DES SYSTÈMES DE PUISSANCE ET ÉCHANGES D'INFORMATIONS ASSOCIÉS – SÉCURITÉ DES COMMUNICATIONS ET DES DONNÉES –

Partie 5: Aspects de sécurité pour l'IEC 60870-5 et ses dérivés

AVANT-PROPOS

- 1) La Commission Électrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. À cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
- 2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
- 3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
- 4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
- 5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
- 6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
- 7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
- 8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
- 9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets.

L'IEC 62351-5 a été établie par le comité d'études 57 de l'IEC: Gestion des systèmes de puissance et échanges d'informations associés. Il s'agit d'une Norme internationale.

Cette Norme internationale annule et remplace l'IEC TS 62351-5 parue en 2013. Elle constitue une révision technique. Les modifications principales présentées dans la présente Norme internationale sont les suivantes:

- a) le mécanisme de communication sécurisée est réalisé par une association poste de conduite/poste téléconduit;
- b) la gestion des Utilisateurs, qui sert à ajouter, modifier ou supprimer un Utilisateur, a été supprimée;
- c) la méthode symétrique, qui sert à modifier la Clé de Mise à Jour, a été supprimée;

- d) la méthode asymétrique, qui sert à modifier la Clé de Mise à Jour, a été révisée;
- e) la procédure et les concepts de Stimulation/Réponse ont été supprimés;
- f) le concept de Mode Agressif a été remplacé par le mécanisme d'échange de messages de Données Sécurisées;
- g) un chiffrement authentifié des données d'application a été ajouté;
- h) la liste des algorithmes de sécurité admis a été mise à jour;
- i) les règles de calcul des numéros de séquence des messages ont été mises à jour;
- j) la surveillance et l'enregistrement des événements ont été ajoutés.

NOTE Les caractères d'imprimerie suivants sont utilisés:

Les MAJUSCULES sont utilisées dans le texte du présent document pour identifier formellement les composantes les plus importantes du mécanisme de sécurité décrit. Ces composantes incluent: 1) les éléments relatifs aux données (par exemple, les Clés de Mise à Jour, les Clés de Session); 2) les noms de procédures (par exemple, Association de Postes, Modification de Clé de Session); les noms de message (par exemple, Requête d'Association, Requête de Session); 3) les noms d'états (par exemple, Session Établie, Attendre la Réponse de la Session); 5) les statistiques (par exemple, Erreurs d'Authentification, Messages Inattendus) et 5) les noms d'événements (par exemple, Temporisation de Réponse, Modification de Clé de Session Non Valide Rx).

Le texte de cette Norme internationale est issu des documents suivants:

Projet	Rapport de vote
57/2516/FDIS	57/2555/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à son approbation.

La langue employée pour l'élaboration de cette Norme internationale est l'anglais.

Ce document a été rédigé selon les Directives ISO/IEC, Partie 2, il a été développé selon les Directives ISO/IEC, Partie 1 et les Directives ISO/IEC, Supplément IEC, disponibles sous www.iec.ch/members_experts/refdocs. Les principaux types de documents développés par l'IEC sont décrits plus en détail sous www.iec.ch/standardsdev/publications.

Le comité a décidé que le contenu de ce document ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous webstore.iec.ch dans les données relatives au document recherché. À cette date, le document sera

- reconduit,
- supprimé,
- remplacé par une édition révisée, ou
- amendé.

IMPORTANT – Le logo "colour inside" qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

GESTION DES SYSTÈMES DE PUISSANCE ET ÉCHANGES D'INFORMATIONS ASSOCIÉS – SÉCURITÉ DES COMMUNICATIONS ET DES DONNÉES –

Partie 5: Aspects de sécurité pour l'IEC 60870-5 et ses dérivés

1 Domaine d'application

La présente partie de l'IEC 62351 définit le mécanisme de communication sécurisée du profil d'application (profil A) qui spécifie les messages, les procédures et les algorithmes pour sécuriser le fonctionnement de tous les protocoles fondés sur ou dérivés de l'IEC 60870-5, *Matériels et systèmes de téléconduite – Protocoles de transmission*. Le présent document s'applique au moins aux protocoles énumérés dans le Tableau 1.

Tableau 1 – Domaine d'application aux normes

Numéro	Nom
IEC 60870-5-101	Norme d'accompagnement pour les tâches élémentaires de téléconduite
IEC 60870-5-102	Norme d'accompagnement pour la transmission de totaux intégrés dans un système électrique de puissance
IEC 60870-5-103	Norme d'accompagnement pour l'interface de communication d'information des équipements de protection
IEC 60870-5-104	Accès aux réseaux utilisant des profils de transport normalisés pour l'IEC 60870-5-101
DNP3	Protocole de Réseau Distribué (défini dans la norme IEEE 1815, fondé sur les normes IEC 60870-1 à IEC 60870-5 et maintenu conjointement par le Groupe d'utilisateurs du DNP et l'IEEE)

Il est prévu que les premiers lecteurs du présent document soient les membres des groupes de travail qui élaborent les protocoles énumérés dans le Tableau 1.

Pour que les mesures décrites dans le présent document entrent en application, elles doivent être acceptées et référencées par les spécifications des protocoles eux-mêmes. Le présent document est rédigé dans le but de permettre ce processus. Les groupes de travail chargés d'associer le présent document aux protocoles spécifiques énumérés dans le Tableau 1 peuvent choisir de ne pas le faire.

Il est prévu que les lecteurs suivants du présent document soient les personnes chargées d'élaborer les produits qui mettent en œuvre ces protocoles.

Certaines parties du présent document peuvent également être utiles aux gestionnaires et aux cadres dirigeants pour comprendre le but et les exigences du travail.

Ce document est organisé du plus général au plus spécifique, comme suit:

- les Articles 2 à 4 fournissent des termes, des définitions et des références de contexte;
- l'Article 5 décrit les problèmes que la présente spécification est destinée à traiter;
- l'Article 6 décrit le mécanisme de manière générale, sans référence à un protocole spécifique;
- les Articles 7 et 8 décrivent le mécanisme plus précisément. Ils constituent la partie normative principale de la présente spécification;

- l'Article 9 définit les exigences d'interopérabilité pour ce mécanisme de communication sécurisée y compris la relation entre cette norme et la CEI 62351-3 pour la sécurité de la couche transport;
- l'Article 10 décrit les exigences des autres normes qui font référence au présent document.

Il est attendu que les actions d'une organisation en réponse aux événements et conditions d'erreurs décrits dans le présent document soient définies par la politique de sécurité de l'organisme. Elles ne relèvent pas du domaine d'application du présent document.

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

IEC 60870-5 (toutes les parties), *Matériels et systèmes de téléconduite – Partie 5: Protocoles de transmission*

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* (disponible en anglais seulement)

IEC TS 62351-2, *Power systems management and associated information exchange – Data and communications security – Part 2: Glossary of terms* (disponible en anglais seulement)

IEC 62351-3, *Gestion des systèmes de puissance et échanges d'informations associés – Sécurité des communications et des données – Partie 3: Sécurité des réseaux et des systèmes de communication – Profils comprenant TCP/IP*

IEC 62351-7, *Gestion des systèmes de puissance et échanges d'informations associés – Sécurité des communications et des données – Partie 7: Modèles d'objets de données de gestion de réseaux et de systèmes (NSM)*

IEC 62351-8, *Gestion des systèmes de puissance et échanges d'informations associés – Sécurité des communications et des données – Partie 8: Contrôle d'accès basé sur les rôles pour la gestion de systèmes de puissance*

IEC 62351-14, *Power systems management and associated information exchange – Data and communications security – Part 14: Cyber security event logging* (disponible en anglais seulement)¹

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

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

IETF RFC 5116, *An Interface and Algorithms for Authenticated Encryption*

IETF RFC 5869, *HMAC-based Extract-and-Expand Key Derivation Function (HKDF)*

IETF RFC 7693, *The BLAKE2 Cryptographic Hash and Message Authentication Code (MAC)*

¹ En cours d'élaboration. Stade au moment de la publication: IEC ACDV 62351-14:2021.

IETF RFC 7748, *Elliptic Curve for Security*

SEC2-V2, *Standards for Efficient Cryptography SEC2: Recommended Elliptic Curve Domain Parameters – Version 2.0*