
Upravljanje elektroenergetskih sistemov in z njim povezana izmenjava informacij - Varnost podatkov in komunikacij - 14. del: Beleženje dogodkov kibernetске varnosti

Power systems management and associated information exchange - Data and communications security - Part 14: Cyber security event logging

iTeh Standards

Gestion des systèmes de puissance et échanges d'informations associés - Sécurité des communications et des données - Partie 14: Journalisation des événements de cyber sécurité

Ta slovenski standard je istoveten z: prEN IEC 62351-14:2025

<https://standards.iteh.ai/catalog/standards/sist/ccbbfaf7-e352-498f-81e4-22737009ae79/osist-pren-iec-62351-14-2026>

ICS:

29.240.30	Krmilna oprema za elektroenergetske sisteme	Control equipment for electric power systems
35.240.50	Uporabniške rešitve IT v industriji	IT applications in industry

oSIST prEN IEC 62351-14:2026

en



57/2849/CDV

COMMITTEE DRAFT FOR VOTE (CDV)

PROJECT NUMBER:

IEC 62351-14 ED1

DATE OF CIRCULATION:

2025-12-05

CLOSING DATE FOR VOTING:

2026-02-27

SUPERSEDES DOCUMENTS:

57/2741/NP, 57/2784A/RVN
IEC TC 57 : POWER SYSTEMS MANAGEMENT AND ASSOCIATED INFORMATION EXCHANGE

SECRETARIAT:

Germany

SECRETARY:

Mr Heiko Englert

OF INTEREST TO THE FOLLOWING COMMITTEES:

HORIZONTAL FUNCTION(S):

ASPECTS CONCERNED:

Electricity transmission and distribution, Information security and data privacy
☒ SUBMITTED FOR CENELEC PARALLEL VOTING

☐ NOT SUBMITTED FOR CENELEC PARALLEL VOTING

Attention IEC-CENELEC parallel voting

The attention of IEC National Committees, members of CENELEC, is drawn to the fact that this Committee Draft for Vote (CDV) is submitted for parallel voting.

The CENELEC members are invited to vote through the CENELEC online voting system.

<https://standards.iteh.ai/catalog/standards/sist/c6b5f7-e352-498f-81e4-22737009ae79/osist-pren-iec-62351-14-2026>

This document is still under study and subject to change. It should not be used for reference purposes.

Recipients of this document are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Recipients of this document are invited to submit, with their comments, notification of any relevant "In Some Countries" clauses to be included should this proposal proceed. Recipients are reminded that the CDV stage is the final stage for submitting ISC clauses. (SEE [AC/22/2007](#) OR [NEW GUIDANCE DOC](#)).

TITLE:

Power systems management and associated information exchange – Data and communications security – Part 14: Cyber security event logging

PROPOSED STABILITY DATE: 2026

NOTE FROM TC/SC OFFICERS:

Copyright © 2025 International Electrotechnical Commission, IEC. All rights reserved. It is permitted to download this electronic file, to make a copy and to print out the content for the sole purpose of preparing National Committee positions. You may not copy or "mirror" the file or printed version of the document, or any part of it, for any other purpose without permission in writing from IEC.

CONTENTS

FOREWORD.....	6
INTRODUCTION.....	8
1 Scope.....	9
2 Normative references	10
3 Terms and definitions	12
3.1 Cyber security event	12
3.2 Cyber security event log	12
3.2.1 Log generation entity	12
3.2.2 Log collection entity	12
3.3 Event.....	12
3.4 Entity	12
3.5 Type	12
3.6 Characters And Character Sets.....	12
3.6.1 Named Characters.....	13
3.6.2 Named Character Sets	14
3.6.3 UTF-8.....	14
3.7 User.....	15
3.8 Abbreviations and acronyms	15
4 Structure for cyber security event	15
4.1 Information structure for describing a cyber security event.....	16
4.2 Information structure for logging a cyber security event	19
4.3 Relation between [Table 1] and [Table 2]	23
4.4 Cyber security event identifier numeric range allocation	23
4.4.1 ID (Composite)	24
4.4.2 Domain ID	24
4.4.3 Event Group	24
4.4.4 Event Number.....	25
4.5 Dynamic parameter insertion	25
5 Using electronic version to describe a cyber security event	26
6 Cyber security event logging using Syslog RFC5424	26
6.1 Mapping to RFC 5424 Syslog HEADER.....	26
6.2 Mapping to RFC 5424 STRUCTURED-DATA	28
6.2.1 Mapping to SD-ELEMENT 62351-14@41912 (Mandatory)	28
6.2.2 Mapping to SD-ELEMENT timeQuality (Optional).....	29
6.3 Mapping to RFC 5424 MSG	30
6.4 Mapping to Syslog RFC 5424 PRI.....	30
6.5 Secure and reliable transport of cyber security events using Syslog	31
6.6 Raw storage of mapped information	32
7 Cyber security event logging using XML	32
7.1 IEC 62351-14 Security Event Definition XSD Schemas	32
7.1.1 Basic Types Definition (SECEVT_BaseTypes.xsd).....	32
7.1.2 Events Definition Types (SECEVT_EventsDefinition.xsd)	36
7.1.3 Events List Types (SECEVT_EventList.xsd)	40
7.2 Rules for creating event definition and event text translations XML files.....	44
8 A French translation of the 1 st version would be named: IEC62351-14_v1_fr.xml Mapping Syslog to SNMP	45

IEC CDV 62351-14 © IEC 2025

9	Mapping SNMP to Syslog	46
10	Storage recommendations of cyber security events	46
11	Conformance	46
	Annex A (informative/normative) Generic cybersecurity events	47
	Annex B (informative/normative) IEC 62351 parts specific cybersecurity events	57
	Annex B.1 IEC 62351 specific cyber security events	57
	Annex B.1.1 IEC 62351-3 cybersecurity event logs	57
	Annex B.1.2 IEC 62351-4 cybersecurity event logs	61
	Annex B.1.3 IEC 62351-5 cybersecurity event logs	73
	Annex B.1.4 IEC 62351-6 cybersecurity event logs	75
	Annex B.1.5 IEC 62351-8 cybersecurity event logs	76
	Annex B.1.6 IEC 62351-9 cybersecurity event logs	79
	Annex B.1.7 IEC 62351-11 cybersecurity event logs	82
	Annex C (informative) Examples – Syslog (RFC 5424) based logging	83
	Annex C.1 Syslog (RFC 5424) based logging of a generic cybersecurity event	83
	Example 1 – Account Creation	84
	Example 2 – Nonzero SqNum Encoding	88
	Example 3 – Custom SD-ELEMENT	91
	Annex D (informative) IEC 62443-4-2 mapping with IEC 62351-14 event definition attributes	92

FIGURES

Figure 1 – Relationship between [Table 1] and [Table 2]	23
---	----

TABLES

Table 1 – Abstract information structure for defining a cyber security event	16
Table 2 – Abstract information structure for logging a cyber security event log	19
Table 3 – Dynamic parameter example	25
Table 4 – Mapping to Syslog [RFC 5424] HEADER	27
Table 5 – Mapping to SD-ELEMENT 62351-14@41912	28
Table 6 – Mapping to SD-ELEMENT timeQuality	30
Table 7 – Mapping of IEC 62351 severity attribute to Syslog RFC 5424 severity	31
Table 9 – General cyber security events	48
Table 10 – (IEC62351-3) TLS handshake cyber security events	58
Table 11 – (IEC 62351-3) TLS certificate cyber security events	59
Table 12 – (IEC 62351-4) E2E HandshakeReq cyber security events	62
Table 13 – (IEC 62351-4) E2E HandshakeAcc cyber security events	63
Table 14 – (IEC 62351-4) E2E ApplicationReject cyber security events	64
Table 15 – (IEC 62351-4) E2E ApplicationSecReject cyber security events	65
Table 16 – (IEC 62351-4) E2E HandshakeSecAbort cyber security events	66
Table 17 – (IEC 62351-4) E2E DtSecAbort cyber security events	67
Table 18 – (IEC 62351-4) E2E ApplAbort cyber security events	68
Table 19 – (IEC 62351-4) E2E ClearTransfer cyber security events	69
Table 20 – (IEC 62351-4) E2E EncrTransfer cyber security events	70

IEC CDV 62351-14 © IEC 2025

Table 21 – (IEC 62351-4) E2E ReleaseReq cyber security events	71
Table 22 – (IEC 62351-4) E2E ReleaseRsp cyber security events.....	71
Table 23 – (IEC 62351-4) OSI operational environment cyber security events	72
Table 24 – (IEC 62351-4) XMPP operational environment cyber security events	73
Table 25 – (IEC 62351-5) secure communication cyber security events	73
Table 26 – (IEC 62351-5) certificate cyber security events.....	74
Table 27 – (IEC 62351-6) GOOSE cyber security events	75
Table 28 – IEC 62351-6 SV cyber security events.....	75
Table 29 – (IEC 62351-8) general access token cyber security events	76
Table 30 – (IEC 62351-8) profile A, B and C cyber security events	77
Table 31 – (IEC 62351-8) security events for backend interaction	77
Table 32 – (IEC 62351-8) security events related to RBAC engineering and maintenance	77
Table 33 – (IEC 62351-9) credential transport and certificate enrolment cyber security events.....	79
Table 34 – (IEC62351-9) public-key certificate cyber security events	80
Table 35 – (IEC62351-9) attribute certificate cyber security events	81
Table 36 – (IEC62351-9) certificate revocation cyber security events.....	81
Table 37 – (IEC62351-9) GDOI cyber security events	81
Table 38 – IEC 62351-11 cyber security events	82
Table 39 – Account creation (Event Field – Value).....	84
Table 40 – Account Creation (Logging Attributes)	84
Table 41 – Account Creation (SYSLOG RFC 5424 HEADER Construction)	85
Table 42 – Account Creation (SD-ELEMENT: 62351-14@41912).....	86
Table 43 – Account Creation (SD-ELEMENT: timeQuality).....	87
Table 44 – Nonzero SqNum Encoding (Event Field – Value).....	88
Table 45 – Nonzero SqNum Encoding (Logging Attributes)	88
Table 46 – Nonzero SqNum Encoding (HEADER Construction)	89
Table 47 – Nonzero SqNum Encoding (SD-ELEMENT: 62351-14@41912).....	90
Table 48 – Nonzero SqNum Encoding (SD-ELEMENT: timeQuality).....	90
Table 49 – Custom SD-ELEMENT.....	91
Table 50 – IEC 62443-4-2 to IEC 62351-14 mapping	92

IEC CDV 62351-14 © IEC 2025

REVISION

Name	Document changes	Date
Arijit Kumar Bose	Drafted based on the feedback from IEC 62351 TC 57 WG15 members and participants.	02 nd August 2024
Arijit Kumar Bose	Based on the resolutions of comments as received from National Committees on the first draft. These resolutions were discussed and approved within WG15.	16 th June 2025
Arijit Kumar Bose	Updated the header based on the input from WG15.	22 nd June 2025
Arijit Kumar Bose	Aligned IEC 62351-8 list of cybersecurity events in accordance with latest FDIS of IEC 62351-8.	21 st July 2025
Jean-Sebastien Gagnon	Formulation of sections 5 and 7.	10 th September 2025
Arijit Kumar Bose	1) Introduced sections 3.2.1 and 3.2.2. 2) Updated section 4.1 with note for "SupersededBy". 3) For section 4.1, introduced the conditional clause and a note for the attribute "Text". 4) For section 4.2, introduced the conditional clause for the attribute "P.label". 5) For section 5, cross-referenced to section 7. 6) Introduced section 6.6 for handling "raw data". 7) Based on 6), accordingly updated Table 8 of section 11. 8) Grouped all generic cybersecurity events inside Annex A. 9) Grouped all IEC 62351 parts specific cybersecurity events inside Annex B. 10) Grouped all examples inside Annex C. 11) Grouped inside Annex D addressing "IEC 62443-4-2 event attributes mapping to IEC 62351-14 event definition attributes".	22 nd September 2025