DEUTSCHE NORM *Entwurf* September 2020

DIN EN IEC 62351-14 (VDE 0112-351-14)

DIN

VDE

Diese Norm ist zugleich eine **VDE-Bestimmung** im Sinne von VDE 0022. Sie ist nach Durchführung des vom VDE-Präsidium beschlossenen Genehmigungsverfahrens unter der oben angeführten Nummer in das VDE-Vorschriftenwerk aufgenommen und in der „etz Elektrotechnik + Automation" bekannt gegeben worden.

ICS 33.200; 35.030; 35.240.50

Einsprüche bis 2020-10-21

Entwurf

Energiemanagementsysteme und zugehöriger Datenaustausch – Daten- und Kommunikationssicherheit – Teil 14: Protokollierung von IT-Sicherheitsvorfällen (IEC 57/2162/CD:2019); Text Deutsch und Englisch

Power systems management and associated information exchange –
Data and communications security –
Part 14: Cyber security event logging
(IEC 57/2162/CD:2019);
Text in German and English

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2020-08-21 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an dke@vde.com möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an die DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE, Stresemannallee 15, 60596 Frankfurt am Main.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 107 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

Documents
Document Sharing Hub

Full document details: E DIN EN IEC 62351-14:2020-09

Anwendungsbeginn

Anwendungsbeginn dieser Norm ist ... .

Nationales Vorwort

Das internationale Dokument IEC 57/2162/CD:2019 „Power systems management and associated information exchange – Data and communications security – Part 14: Cyber security event logging“ (CD, en: Committee Draft) ist unverändert in diesen Norm-Entwurf übernommen worden. Dieser Norm-Entwurf enthält eine noch nicht autorisierte deutsche Übersetzung.

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung des CD entsprechend der diesbezüglich durch die IEC erteilten Erlaubnis beigefügt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen IEC-Text.

Das internationale Dokument wurde vom TC 57 „Power systems management and associated information exchange“ der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet und unterliegt dem Copyright der IEC.

Das Dokument wurde den nationalen Komitees zur Stellungnahme vorgelegt.

Die Internationale Elektrotechnische Kommission (IEC) und das Europäische Komitee für Elektrotechnische Normung (CENELEC) haben vereinbart, dass ein auf IEC-Ebene erarbeiteter Entwurf für eine Internationale Norm zeitgleich (parallel) bei IEC und CENELEC zur Umfrage (CDV-Stadium) und Abstimmung als FDIS (en: Final Draft International Standard) bzw. Schluss-Entwurf für eine Europäische Norm gestellt wird, um eine Beschleunigung und Straffung der Normungsarbeit zu erreichen. Dokumente, die bei CENELEC als Europäische Norm angenommen und ratifiziert werden, sind unverändert als Deutsche Normen zu übernehmen.

Da der Abstimmungszeitraum für einen FDIS bzw. Schluss-Entwurf FprEN nur 6 Wochen beträgt, und dann keine sachlichen Stellungnahmen mehr abgegeben werden können, sondern nur noch eine „JA/NEIN“-Entscheidung möglich ist, wobei eine „NEIN“-Entscheidung fundiert begründet werden muss, wird bereits der CD als DIN-Norm-Entwurf veröffentlicht, um die Stellungnahmen aus der Öffentlichkeit frühzeitig berücksichtigen zu können.

Für dieses Dokument ist das nationale Arbeitsgremium K 952 „Netzleittechnik“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE (www.dke.de) zuständig.

Für den Fall einer undatierten Verweisung im normativen Text (Verweisung auf ein Dokument ohne Angabe des Ausgabedatums und ohne Hinweis auf eine Abschnittsnummer, eine Tabelle, ein Bild usw.) bezieht sich die Verweisung auf die jeweils aktuellste Ausgabe des in Bezug genommenen Dokuments.

Für den Fall einer datierten Verweisung im normativen Text bezieht sich die Verweisung immer auf die in Bezug genommene Ausgabe des Dokuments.

Der Zusammenhang der zitierten Dokumente mit den entsprechenden deutschen Dokumenten ergibt sich, soweit ein Zusammenhang besteht, grundsätzlich über die Nummer der entsprechenden IEC-Publikation. Beispiel: IEC 60068 ist als EN 60068 als Europäische Norm durch CENELEC übernommen und als DIN EN 60068 ins Deutsche Normenwerk aufgenommen.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. IEC ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62351-14:2020-09

Inhalt

Seite

Einleitung 5
1 Anwendungsbereich 6
2 Normative Verweisungen 6
3 Begriffe 8
4 Abkürzungen 8
5 Struktur eines IT-Sicherheitsereignisses 9
5.1 Informationsstruktur zur Beschreibung eines IT-Sicherheitsereignisses 9
5.2 Informationsstruktur zur Protokollierung eines IT-Sicherheitsereignisses 11
5.3 Zuweisung von numerischen Bereichen zu IT-Sicherheitsereignis-Kennungen 15
6 Protokollierung von IT-Sicherheitsereignissen unter Verwendung von Syslog 15
6.1 Protokollierung unter Verwendung des strukturierten Syslog-Formats RFC 5424 15
6.2 Abbildung des Schweregrads von IT-Sicherheitsereignissen nach IEC 62351-14 auf Syslog RFC 5424-Prioritätsstufe 21
6.3 Sichere und zuverlässige Übertragung von IT-Sicherheitsereignissen unter Verwendung von Syslog 22
7 Abbildung von Syslog auf SNMP 22
8 Abbildung von SNMP auf Syslog 22
9 Empfehlungen zur Speicherung von IT-Sicherheitsereignissen 22
Anhang A (informativ) Auflistung von IT-Sicherheitsereignissen 23
A.1 Generische IT-Sicherheitsereignisse 24
A.2 Für IEC 62351 spezifische IT-Sicherheitsereignisse 42
A.2.1 IT-Sicherheitsereignis-Protokolle entsprechend IEC 62351-3 42
A.2.2 IT-Sicherheitsereignisse entsprechend IEC 62351-5 43
A.2.3 Für IEC 60870-5 spezifische Ereignisse 44
A.2.4 IT-Sicherheitsereignisse entsprechend IEC 62351-6 45
A.2.5 IT-Sicherheitsereignisse entsprechend IEC 62351-8 46
A.2.6 IT-Sicherheitsereignisse entsprechend IEC 62351-9 48
A.2.7 IT-Sicherheitsereignisse entsprechend IEC 62351-11 50
A.3 Beispiel für die Protokollierung mit Syslog 50

Tabellen

Tabelle 1 – Abstrakte Informationsstruktur zur Definition eines Protokolls für IT-Sicherheitsereignisse 10
Tabelle 2 – Abstrakte Informationsstruktur zur Protokollierung eines Protokolls für IT-Sicherheitsereignisse 11
Tabelle 3 – Abbildung der Struktur abstrakter Informationen nach IEC 62351 auf die Meldungsfelder von Syslog [RFC 5424] 16
Tabelle 4 – Abbildung des Attributs „Severity“ nach IEC 62351 auf den Schärfegrad von Syslog RFC 5424 21
Tabelle 5 – Allgemeine IT-Sicherheitsereignisse 24
Tabelle 6 – IT-Sicherheitsereignis-Protokolle entsprechend IEC 62351-3 43

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62351-14:2020-09

Seite

Tabelle 7 – IT-Sicherheitsereignis-Protokolle entsprechend IEC 62351-5 44
Tabelle 8 – Für IEC 60870-5 spezifische Ereignisse 45
Tabelle 9 – IT-Sicherheitsereignis-Protokolle entsprechend IEC 62351-6 46
Tabelle 10 – IT-Sicherheitsereignis-Protokolle entsprechend IEC 62351-8 47
Tabelle 11 – IT-Sicherheitsereignis-Protokolle entsprechend IEC 62351-9 49
Tabelle 13 – Generische IT-Sicherheitsereignisse 51
Tabelle 14 – Zuweisung von Werten zu Protokollierungsattributen 51
Tabelle 15 – Für IEC 62351-3 spezifisches IT-Sicherheitsereignis 53
Tabelle 16 – Ein für IEC 62351-3 spezifisches IT-Sicherheitsereignis 53

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62351-14:2020-09

Einleitung

Das Energieversorgungssystem wird immer komplexer und vernetzter. Traditionell wurde ein Elektrizitätsversorgungssystem in einer isolierten Umgebung betrieben, in der der Anlagenbesitzer seine Versorgungseinrichtungen in seinem geografischen Gebiet betrieb. Es gab auch keine Fernverbindung zum Zugriff auf die Daten des Energieversorgungssystems. Dieser traditionelle Trend ändert sich jedoch, da die verschiedenen Energieversorgungsunternehmen immer stärker miteinander verbunden sind. Die Fernverbindung zum Zugriff auf ein Energieversorgungssystem wird auch aus Gründen der Flexibilität immer nützlicher. Diese Digitalisierung des Energieversorgungssystems bietet zwar Vorteile wie Flexibilität beim Zugriff auf und bei der Ausführung von Funktionen im Energieversorgungssystem mit der Möglichkeit, den Zustand des Energieversorgungssystems von entfernten Standorten aus visuell darzustellen, aber sie führt auch zu Bedrohungen für die IT-Sicherheit des Energieversorgungssystems. Solche Bedrohungen können sowohl aus dem internen als auch aus dem externen Kommunikationsnetz eines Energieversorgungsunternehmens hervorgehen. Für einen sicheren und zuverlässigen Betrieb des Energieversorgungssystems ist die IT-Sicherheit daher ein wichtiger Aspekt. Für eine sichere und zuverlässige Verwaltung des Energieversorgungssystems ist es immens wichtig, einen ganzheitlichen Ansatz für die IT-Sicherheit bereitzustellen. Wenn es zu einem Angriff auf die IT-Sicherheit kommt, dann ist es entscheidend, diesen so frühzeitig wie möglich zu erkennen, um proaktive Maßnahmen einleiten zu können. Dies erfordert die Protokollierung und Analyse von IT-Sicherheitsereignissen im gesamten Energieversorgungssystem. Die Protokollierung solcher Ereignisse mit anschließender Analyse ermöglicht einen detaillierten Überblick über die IT-Sicherheitssituation und ihre Grundursachen. Dies ist für die Betreiber von Energieversorgungssystemen äußerst nützlich, damit sie etwaige Präventivmaßnahmen ergreifen können, um die mit möglichen Angriffen auf die IT-Sicherheit verbundenen Risiken zu mindern.

AVA Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62351-14:2020-09

Energiemanagementsysteme und zugehöriger Datenaustausch – Daten- und Kommunikationssicherheit – Teil 14: Protokollierung von IT-Sicherheitsvorfällen

1 Anwendungsbereich

Dieser Teil von IEC 62351 legt die technischen Spezifikationen für die Protokollierung von IT-Sicherheitsvorfällen in Energieversorgungssystemen fest. Der Anwendungsbereich dieser Norm umfasst:

1. eine abstrakte Informationsstruktur, die aus Metadaten besteht, d. h. aus mehreren Attributen zur Definition und Protokollierung eines IT-Sicherheitsereignisses in einem Energieversorgungssystem.
2. Die Norm enthält außerdem eine Liste von IT-Sicherheitsereignissen als Anhang, die mit dieser Abstraktion beschrieben werden. Diese Ereignisse sind nützlich für die Überwachung der IT-Sicherheitslage im gesamten Energieversorgungssystem.
3. Sie beschreibt zudem ein Verfahren zur sicheren Protokollierung solcher IT-Sicherheitsereignisse mit einer sicheren Variante von Syslog.

Die Aspekte, die nicht in den Anwendungsbereich dieser Norm fallen, sind Folgende:

1. Definition des Verfahrens zur Verwendung von anderen Ereignisprotokollen als Syslog für die Protokollierung von IT-Sicherheitsereignissen im Energieversorgungssystem.
2. Sie behandelt nicht die technischen Spezifikationen und Verfahren zur Analyse eines IT-Sicherheitsereignisses und damit zur Ermittlung seiner Ursache.

   Anmerkung: Die Analyse und Ermittlung der Ursachen hinter jedem IT-Sicherheitsereignis und die anschließende Erkennung eines Angriffs auf die IT-Sicherheit erfordert jedoch zwingend die Protokollierung des jeweiligen IT-Sicherheitsereignisses mit nützlichen Informationen aus erster Hand. Diese Norm enthält daher nur technische Spezifikationen für die Protokollierung eines IT-Sicherheitsereignisses für das Energieversorgungssystem.

Der Zweck dieser Norm ist es, eine harmonisierte und standardisierte IT-Sicherheitsspezifikation für die Ereignisprotokollierung über das gesamte Energieversorgungssystem hinweg festzulegen, um Interoperabilität in einer uneinheitlichen Umgebung zu ermöglichen.

2 Normative Verweisungen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

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

IEC 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: Profiles including TCP/IP*

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

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

IEC 62351-6, Power systems management and associated information exchange – Data and communications security – Part 6: Security for IEC 61850

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62351-14:2020-09

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*

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

IEC 62351-10, *Power systems management and associated information exchange – Data and communications security – Part 10: Security architecture guidelines*

IEC 62351-11, *Power systems management and associated information exchange – Data and communications security – Part 11: Security for XML documents*

IEC 62351-12, *Power systems management and associated information exchange – Data and communications security – Part 12: Resilience and security recommendations for power systems with distributed energy resources (DER) cyber-physical systems*

IEC 62351-13, *Power systems management and associated information exchange – Data and communications security – Part 13: Guidelines on what security topics should be covered in standards and specifications*

IEC 60870-5, *Telecontrol equipment and system*

RFC 5424, *The Syslog Protocol*

RFC 3629, *UTF 8, a transformation format for ISO 10646*

RFC 5246, *Transport Layer Security (TLS) Protocol Version 1.2*

RFC 5245, *Transport Layer Security (TLS) Mapping for Syslog*

RFC 1777, *Lightweight Directory Access Protocol*

RFC 1035, *Domain names – Implementation and Specification*

RFC 5675, *Mapping Simple Network Management Protocol (SNMP) Notifications to Syslog messages*

RFC 5676, *Definition of Managed Objects for Mapping Syslog Messages to Simple Network Management Protocol (SNMP) Notifications*

RFC 2527, *Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework*

RFC 3647, *Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework*

IEEE 1686, *IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities*

NERC-CIP, *North American Electric Reliability Corporation Critical Infrastructure Protection Standard*

NERC-CIP-007-5, *Cyber Security – System Security Management*

NERC-CIP-007-6, *Cyber Security – System Security Management*

IEC 62443, *Network and system security for industrial-process measurement and control*

IEC 62443-4-2, *Technical Security Requirements for Industrial Automation and Control System (IACS) components*

ISO 27001, *Information technology – Security Techniques – Information security management systems – Requirements.*

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62351-14:2020-09

RFC 791, *Internet Protocol Darpa Internet Program Protocol Specification*

RFC 6335, *Internet Assigned Numbers Authority (IANA) Procedures for the Management of the Service Name and Transport Protocol Port Number Registry*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

- IEC Electropedia: verfügbar unter http://www.electropedia.org/
- ISO Online Browsing Platform: verfügbar unter http://www.iso.org/obp

3.1
IT-Sicherheitsereignis
Die Ereignisse, die mit den Aspekten der IT-Sicherheit einer Einheit in Zusammenhang stehen.

3.2
IT-Sicherheitsereignis-Protokoll
Wenn das IT-Sicherheitsereignis protokolliert, d. h. in einer Einheit gespeichert wird.

3.3
Ereignis
Eintritt einer Bedingung oder einer Aktion

[QUELLE: IEC 61025:2006, 3.8]

3.4
Einheit
spezifisches Objekt (Ding), wie Person, Ort, Prozess, Objekt, Konzept, Zuordnung oder Ereignis

[QUELLE: IEC 61158-6-14, ed. 3.0 (2014-08)]

3.5
MMS
MMS ist eines der Kommunikationsprotokolle, auf die IEC 61850 angewendet wird.

[QUELLE: IEC 61850-Normenreihe]

3.6
TCP
eines der Kernprotokolle innerhalb der Internet-Protokollreihe

[QUELLE: IEC 80001-2-3, ed. 1.0 (2012-07)]

3.7
TLS
Ein Internet-Protokoll [RFC 2246], das auf SSL Version 3.0 basiert und diesem sehr ähnelt.

[QUELLE: RFC 2828]

4 Abkürzungen

dezentrale Energiequellen	Dezentrale Energieversorgung (en: Distributed Energy Resources)
DNS	Domänennamensystem (en: Domain Name System)
FQDN	vollständiger Domänenname (en: Fully Qualified Domain Name)

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62351-14:2020-09

IP	Internetprotokoll
IEC	International Electrotechnical Commission
LDAP	Leichtgewichtiges Verzeichniszugriffsprotokoll (en: Lightweight Directory Access Protocol)
MMS	Manufacturing Messaging Specification
OSI	Kommunikation offener Systeme (en: Open Systems Interconnection)
SNMP	einfaches Netzwerkverwaltungsprotokoll (en: Simple Network Management Protocol)
TLS	Transportschichtsicherheit (en: Transport Layer Security)
TCP	Übertragungssteuerungsprotokoll (en: Transmission Control Protocol)
TK	Technisches Komitee (en: Technical Committee)
UTF	Universelles Zeichensatz-Umwandlungs-Format (en: Universal Character Set Transformation Format)
UTC	koordinierte Weltzeit (en: Coordinated Universal Time)

Zusätzliche Abkürzungen und Akronyme sind in IEC 62351-2 aufgeführt.

5 Struktur eines IT-Sicherheitsereignisses

Dieser Abschnitt enthält eine Informationsstruktur mit einer Liste von Attributen zur Beschreibung und Protokollierung eines IT-Sicherheitsereignisses für ein Energieversorgungssystem. Diese Informationsstruktur wird agnostisch zu jedem Ereignisprotokollformat und unabhängig von jedem Kommunikationsprotokoll zur Übertragung der IT-Sicherheitsereignisse formuliert. Diese Abstraktion bietet den Endanwendern dieser Norm die Flexibilität, das IT-Sicherheitsereignis unter Verwendung eines beliebigen, einer Industrienorm entsprechenden Ereignisprotokolls zu protokollieren, indem diese abstrakte Informationsstruktur auf die verschiedenen Attribute eines Ereignisprotokolls angewendet wird. Diese Norm stellt eine Abbildung dieser abstrakten Informationsstruktur auf Syslog [RFC 5424] zur Verfügung und bietet damit die Möglichkeit, die Protokollierung mit dem Protokoll Syslog [RFC 5424] durchzuführen.

5.1 Informationsstruktur zur Beschreibung eines IT-Sicherheitsereignisses

Dieser Abschnitt enthält eine abstrakte Informationsstruktur zur Beschreibung eines IT-Sicherheitsereignisses für ein Energieversorgungssystem. Der Vorteil besteht darin, dass diese die Möglichkeit bietet, eine Liste von IT-Sicherheitsereignissen für das Energieversorgungssystem zu beschreiben, um die Interoperabilität in einer heterogenen Umgebung von Energieversorgungssystemen zu ermöglichen. Eine solche Liste von IT-Sicherheitsereignissen wird in Anhang A detaillierter beschrieben. Diese Informationsstruktur besteht aus einer Reihe von Minimalattributen, wie in Tabelle 1 angegeben, die zur Beschreibung eines IT-Sicherheitsereignisses erforderlich sind.

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62351-14:2020-09

Tabelle 1 – Abstrakte Informationsstruktur zur Definition eines Protokolls für IT-Sicherheitsereignisse

Attribute	Definition und Typ
IECversion	**Definition:** Dieses Attribut muss verwendet werden, um die Version dieser Norm, d. h. IEC 62351-14, anzugeben, der das IT-Sicherheitsereignis einer Einheit entspricht. Diese Norm könnte in Zukunft überarbeitet werden, und deshalb ist es wichtig, sich auf die Version dieser Norm zu beziehen, der ein IT-Sicherheitsereignis entspricht. **Typ:** Monoton steigende ganze Zahl von 1 bis 65535. Der Startwert für diese Ausgabe der Norm ist der ganzzahlige Wert 1.
MNEMONIC	**Definition:** Dieses Attribut muss eine schnelle Identifizierung und ein hohes Maß an menschlichem Verständnis eines IT-Sicherheitsereignisses ermöglichen. Mnemonic hilft dabei, die hohe Bedeutung eines IT-Sicherheitsereignisses schnell zu erfassen, ohne dass man sich in die Einzelheiten der Beschreibung einarbeiten muss, wodurch ein schnelles menschliches Verständnis ermöglicht wird. Im Gegensatz zum Attribut „ID“, wie in Tabelle 2 angegeben, ist bei diesem Attribut nicht garantiert, dass es einen eindeutigen Wert besitzt. Es wird jedoch empfohlen, diesem Attribut einen eindeutigen Wert zuzuweisen. **Typ:** Großbuchstaben ohne Größenbeschränkung. Verwendung von Unterstrichen erlaubt. z. B. LOGIN_OK
LogType	**Definition:** Dieses Attribut muss deutlich auf einen Typ von IT-Sicherheitsereignissen nach IEC 62351-14 hinweisen. Das ist nützlich, um ein IT-Sicherheitsereignis nach IEC 62351-14 unter verschiedenen Arten von Ereignissen, die zu einer heterogenen Umgebung von Energieversorgungssystemen gehören, eindeutig und klar zu unterschieden. **Typ:** Kodierte feste Zeichenkette UTF-8 [RFC 3629] mit dem Wert „IEC 62351-14“.
Attribute	**Definition und Typ**
Schärfegrad	**Definition:** Dieses Attribut muss den Schärfegrad des IT-Sicherheitsereignisses angeben. Dieser Standard unterteilt diesen Schärfegrad in vier Kategorien: {alarm, error, notice und warning} **alarm:** IT-Sicherheitsereignis, das auf unbefugte Aktivitäten entsprechend [IEEE 1686] hinweisen kann. . Es wird empfohlen, sofort Maßnahmen zu ergreifen Dies würde jedoch auch von den Endanwendern des lokalen Sicherheitsgrundsatzes dieser Norm abhängen. **error:** Fehlerzustand. Beispielsweise könnte ein solcher Fehlerzustand in einer Einheit aufgrund einer oder mehrerer unvorhergesehener Umweltbedingungen auftreten, in denen die Einheit tätig ist. **notice:** IT-Sicherheitsereignisse, die als autorisierte IT-Sicherheitsaktivitäten klassifiziert sind, die bei der routinemäßigen Nutzung und Wartung einer Einheit erwartet werden können, siehe [IEEE 1686]. Der Schärfegrad „notice“ wird als ein IT-Sicherheitsereignis klassifiziert, aber nicht als eine Verletzung oder einen Angriff auf die IT-Sicherheit oder eine Abweichung vom normalen Betriebszustand einer Einheit. **warning:** Hierbei handelt es sich um ein IT-Sicherheitsereignis, das als anormal klassifiziert wird, d. h. als Abweichung vom normalen Betriebszustand eines Unternehmens, aber nicht zwingend als Cyberangriff. Wenn beispielsweise während des TLS Handshakes der TLS Handshake durch eine TLS-Version festgelegt wird, die für IT-Sicherheitsprobleme anfällig ist, kann dieses Ereignis als „warning“ klassifiziert werden. In diesem Fall ist nicht zwingend gesagt, dass ein Cyberangriff stattfindet, und die Verwendung dieser schwachen TLS-Version könnte auf den lokalen Sicherheitsgrundsatz in der Zielumgebung zurückzuführen sein. **Typ:** UTF-8 [RFC 3629]-kodierte Zeichenkette mit einem der folgenden Werte: {alarm, error, notice und warning}.
ID	**Definition:** Hierbei handelt es sich um eine einmalige und eindeutige numerische Kennung für das IT-Sicherheitsereignis, die dazu beiträgt, dem IT-Sicherheitsereignis eine eindeutige und unverwechselbare numerische Identität zuzuordnen. **Typ:** UTF-8 [RFC 3629]-kodiert mit 128 Zeichen, d. h. innerhalb eines Zeichenbereichs von 0 bis 127, kodiert mit UTF-8.
Text	**Definition:** Dieses Attribut muss einen Informationstext über das IT-Sicherheitsereignis liefern. **Typ:** UTF-8 [RFC 3629]-kodiert mit 128 Zeichen, d. h. innerhalb eines Zeichenbereichs von 0 bis 127, kodiert mit UTF-8.

Die in Tabelle 1 aufgeführten Attribute sind die verbindlichen Minimalattribute zusammen mit ihren jeweiligen Werten, die zur Beschreibung eines IT-Sicherheitsereignisses erforderlich sind.

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62351-14:2020-09

5.2 Informationsstruktur zur Protokollierung eines IT-Sicherheitsereignisses

Dieser Abschnitt stellt eine abstrakte Informationsstruktur zur Verfügung, die sich aus Attributen zusammensetzt, die für ein IT-Sicherheitsereignis bei seinem Auftreten in einer Einheit protokolliert werden müssen. Tabelle 2 enthält diese abstrakte Informationsstruktur, die agnostisch für jedes Ereignisprotokollformat und jedes Kommunikationsprotokoll formuliert wird.

Tabelle 2 – Abstrakte Informationsstruktur zur Protokollierung eines Protokolls für IT-Sicherheitsereignisse (1 von 4)

Feldindex	Protokollierungsattribute	Definition und Typ	Verbindlich/Optional/ Bedingung
1	**IECversion**	**Definition:** Dieses Attribut muss verwendet werden, um die Version dieser Norm, d. h. IEC 62351-14, anzugeben, der das IT-Sicherheitsereignis einer Einheit entspricht. Diese Norm könnte in Zukunft überarbeitet werden, und deshalb ist es wichtig, sich auf die Version dieser Norm zu beziehen, der ein IT-Sicherheitsereignis entspricht. **Typ:** Monoton steigende ganze Zahl von 1 bis 65535. Der Startwert für diese Ausgabe der Norm ist der ganzzahlige Wert 1.	**Verbindlich**
2	**LogType**	**Definition:** Dieses Attribut muss deutlich auf einen Typ von IT-Sicherheitsereignissen nach IEC 62351-14 hinweisen. Das ist nützlich, um ein IT-Sicherheitsereignis nach IEC 62351-14 unter verschiedenen Arten von Ereignissen, die zu einer heterogenen Umgebung von Energieversorgungssystemen gehören, eindeutig und klar zu unterschieden. **Typ:** Kodierte feste Zeichenkette UTF-8 [RFC 3629] mit dem Wert „IEC 62351-14“.	**Verbindlich**
3	**Severity**	**Definition:** Dieses Attribut muss den Schärfegrad des IT-Sicherheitsereignisses angeben. Dieser Standard unterteilt diesen Schärfegrad in vier Kategorien: {alarm, error, notice und warning} **alarm:** IT-Sicherheitsereignis, das auf unbefugte Aktivitäten entsprechend [IEEE 1686] hinweisen kann. Es wird empfohlen, sofort Maßnahmen zu ergreifen Dies würde jedoch auch von den Endanwendern des lokalen Sicherheitsgrundsatzes dieser Norm abhängen. **error:** Fehlerzustand. Beispielsweise könnte ein solcher Fehlerzustand in einer Einheit aufgrund einer oder mehrerer unvorhergesehener Umweltbedingungen auftreten, in denen die Einheit tätig ist. **notice:** IT-Sicherheitsereignisse, die als autorisierte IT-Sicherheitsaktivitäten klassifiziert sind, die bei der routinemäßigen Nutzung und Wartung einer Einheit erwartet werden können, siehe [IEEE 1686]. Der Schärfegrad „notice“ wird als ein IT-Sicherheitsereignis klassifiziert, aber nicht als eine Verletzung oder einen Angriff auf die IT-Sicherheit oder eine Abweichung vom normalen Betriebszustand einer Einheit. **warning:** Hierbei handelt es sich um ein IT-Sicherheitsereignis, das als anormal klassifiziert wird, d. h. als Abweichung vom normalen Betriebszustand eines Unternehmens, aber nicht zwingend als Cyberangriff. Wenn beispielsweise während des TLS Handshakes der TLS Handshake durch eine TLS-Version festgelegt wird, die für IT-Sicherheitsprobleme anfällig ist, kann dieses Ereignis als „warning“ klassifiziert werden. In diesem Fall ist nicht zwingend gesagt, dass ein Cyberangriff stattfindet, und die Verwendung dieser schwachen TLS-Version könnte auf den lokalen Sicherheitsgrundsatz in der Zielumgebung zurückzuführen sein. **Typ:** UTF-8 [RFC 3629]-kodierte Zeichenkette mit einem der folgenden Werte: {alarm, error, notice und warning}.	**Verbindlich**

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62351-14:2020-09

Tabelle 2 (2 von 4)

Feldindex	Protokollierungsattribute	Definition und Typ	Verbindlich/Optional/Bedingung
4	**ID**	**Definition:** Hierbei handelt es sich um eine einmalige und eindeutige numerische Kennung für das IT-Sicherheitsereignis, die dazu beiträgt, dem IT-Sicherheitsereignis eine eindeutige und unverwechselbare numerische Identität zuzuordnen. Siehe Abschnitt 5.3 **Typ:** UTF-8 [RFC 3629]-kodiert mit 128 Zeichen, d. h. innerhalb eines Zeichenbereichs von 0 bis 127, kodiert mit UTF-8.	**Verbindlich**
5	**Text**	**Definition:** Dieses Attribut muss einen Informationstext über das IT-Sicherheitsereignis liefern. **Typ:** UTF-8 [RFC 3629]-kodiert mit 128 Zeichen, d. h. innerhalb eines Zeichenbereichs von 0 bis 127, kodiert mit UTF-8.	**Verbindlich**
6	**ProdName**	Definition: Dieses Attribut muss den Namen der Einheit angeben, aufgrund derer das IT-Sicherheitsereignis-Protokoll erstellt wurde. Typ: UTF-8 [RFC 3629]-kodiert mit 8 Zeichen, d. h. innerhalb eines Zeichenbereichs von 0 bis 7, kodiert mit UTF-8.	**Optional**
7	**Source**	**Definition:** Dieses Attribut muss die eindeutige Kennung der Einheit oder einer Anwendung innerhalb einer Einheit liefern, die das IT-Sicherheitsereignis erzeugt hat. Zwei Einheiten können den gleichen Namen haben, d. h. zwei Geräte vom gleichen Hersteller könnten den gleichen Namen haben. Zur weiteren Unterscheidung zwischen diesen beiden gleichnamigen Geräten und zur eindeutigen Identifizierung des Geräts, das das IT-Sicherheitsereignis erzeugt hat, kann das Attribut „Source“ verwendet werden, wobei dem Attribut „Source“ eine eindeutige Kennung des Geräts oder einer Anwendung innerhalb des Geräts, das das jeweilige IT-Sicherheitsereignis erzeugt hat, entsprechend zugeordnet werden kann. **Typ:** UTF-8 [RFC 3629]-kodiert mit 64 Zeichen, d. h. innerhalb eines Zeichenbereichs von 0 bis 63, kodiert mit UTF-8.	**Verbindlich**
9	**Zeitstempel**	**Definition:** Dieses Attribut gibt den Wert des Zeitpunkts an, zu dem das jeweilige IT-Sicherheitsereignis von der „Source“ erzeugt wurde. Zur Definition von „Source“ siehe entsprechende Definition in Feldindex Nummer 7 dieser Tabelle. **Typ:** UTC-Zeitformat nach [IEC 62351-4]. Anmerkung: Wenn die Einheit nicht in der Lage ist, einen Zeitstempel im UTC-Format zu erstellen, kann ein Zeitversatz verwendet werden. TIME-OFFSET = „Z“ / TIME-NUMOFFSET TIME-NUMOFFSET = („+“ / „-“) TIME-HOUR „:“ TIME-MINUTE	**Verbindlich**
Feldindex	**Protokollierungsattribute**	**Definition und Typ**	**Verbindlich/Optional/Bedingung**
8[N1]	**RemoteIP: Port**	**Definition:** Dieses Attribut muss die IP-Adresse und Port-Nummer der Einheit angeben, von der aus während des Auftretens des jeweiligen IT-Sicherheitsereignisses auf die Einheit zugegriffen wurde, die das IT-Sicherheitsereignis erzeugt hat. Wenn während des Verlaufs eines IT-Sicherheitsereignisses die Ursache für die Erzeugung dieses Ereignisses in einer Handlung lag, die von einer externen Einheit aus auf die Einheit, die das Ereignis erzeugt hat, angewendet wurde, dann ist es sinnvoll, die Koordinaten dieser externen Einheit zu ermitteln **Typ:** IP-Version-4-Adresse [RFC 791]: Port-Nummer [RFC 6335]	**Bedingung** Die Bedingung ist, dass die Einheit IP-fähig ist, d. h. IP-Adressen unterstützt.

[N1] Nationale Fußnote: Nummerierung nicht korrekt

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62351-14:2020-09

Tabelle 2 (3 von 4)

Feldindex	Protokollierungsattribute	Definition und Typ	Verbindlich/Optional/Bedingung
		Anmerkung: Um Spoofing-Angriffe auf „RemoteIP“ zu verhindern, wird empfohlen, eine TLS-Verbindung zwischen der externen Einheit und der jeweiligen Einheit, die das IT-Sicherheitsereignis erzeugt hat, zu verwenden. Die Fälschung der IP-Adresse könnte während der Zertifikatsvalidierungsphase von TLS entdeckt werden. Zusätzlich können Konfigurationen wie DNS verwendet werden, um IP-Spoofing-Angriffe auf „RemoteIP“ zu verhindern.	
10	**ExtraInfo**	**Definition:** Dieses Attribut muss zusätzlichen Informationstext über das IT-Sicherheitsereignis liefern, d. h. zusätzlich zu den Informationen, die das Attribut „Text“ erfasst, kann dieses Attribut dazu verwendet werden, zusätzliche nützliche Informationen über das IT-Sicherheitsereignis während des Protokollierungszeitpunktes zu erfassen. **Typ:** UTF-8 [RFC 3629]-kodiert mit 32 Zeichen, d. h. innerhalb eines Zeichenbereichs von 0 bis 31, kodiert mit UTF-8.	**Bedingung** Die Bedingung ist, dass zusätzliche aussagekräftige Informationen für die Protokollierung zur Verfügung stehen, die bei der Ermittlung der Grundursache eines IT-Sicherheitsproblems helfen können.
11	**SOE**	**Definition:** Dieses Attribut muss die laufende Nummer des IT-Sicherheitsereignisses angeben, das von einer Einheit erzeugt wird. Für jedes einzelne IT-Sicherheitsereignis, das von einer Einheit erzeugt wird, muss der Wert dieses Attributs um eins erhöht werden. **Typ:** Monoton steigende ganzer Zahlenwert von 1 bis 4294967295.	**Bedingung** Die Bedingung ist, dass die Einheit eine Sequenznummer für jedes der aufeinander folgenden IT-Sicherheitsereignisse generieren kann.
12	**UsrID**	**Definition:** Dieses Attribut muss die eindeutige Kennung eines Benutzers liefern, wenn es mit der Erzeugung des IT-Sicherheitsereignisses durch eine Einheit in Verbindung steht. **Typ:** UTF-8 [RFC 3629]-kodiert mit 32 Zeichen, d. h. innerhalb eines Zeichenbereichs von 0 bis 31, kodiert mit UTF-8.	**Bedingung** Die Bedingung ist, dass ein Benutzer mit der Erzeugung eines IT-Sicherheitsereignisses in Verbindung gebracht wird.
13	**RoleID**	**Definition:** Wenn ein Benutzer mit der Erzeugung eines IT-Sicherheitsereignisses in Verbindung gebracht wurde, muss dieses Attribut die Rollenkennung des jeweiligen Benutzers liefern. Dies gilt nur, wenn dem Benutzer entsprechend dem lokalen Sicherheitsgrundsatz eine Rolle zusammen mit einer Kennung für diese Rolle zugewiesen ist. **Typ:** Der Datentyp des Attributs „RoleID“ muss dem Datentyp des Attributs „RoleID“, wie in IEC 62351-8 definiert, entsprechen.	**Bedingung** Die Bedingung ist, dass ein Benutzer

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62351-14:2020-09

Tabelle 2 (4 von 4)

Feldindex	Protokollierungsattribute	Definition und Typ	Verbindlich/Optional/ Bedingung
		Anmerkung: Für Einheiten, die Reihen von Kommunikationsprotokollen nach IEC TC 57 verarbeiten, wird davon ausgegangen, dass diese Einheiten die Liste der Standardrollen, d. h. die Standardliste „RoleDefinition“ nach IEC 62351-8 zusammen mit den entsprechenden „RoleIDs“ nach IEC 62351-8 unterstützen müssen. Für Reihen von Kommunikationsprotokollen, die nicht TC 57 entsprechen, müssen andere Rollendefinitionen zusammen mit einer anderen „RoleID“ (d. h. andere als die von der Standardliste „RoleID“ für die in IEC 62351-8 genannten Standardrollen) unterstützt werden.	hinter der Erzeugung des IT-Sicherheitsereignisses steht / mit diesem assoziiert ist und dass dem Benutzer eine „Rolle“ und eine „Rollenkennung“ zugewiesen wurde.
Feldindex	**Protokollierungs-attribute**	**Definition und Typ**	**Verbindlich/ Optional/ Bedingung**
14	**AccountType**	**Definition:** Wenn ein Benutzer mit der Erzeugung eines IT-Sicherheitsereignisses assoziiert wurde, muss dieses Attribut den Typ des Benutzerkontos, d. h. die Rollendefinition des Benutzers, angeben. **Typ:** Der Datentyp des Attributs „AccountType“ muss dem Datentyp des Attributs „RoleDefinition“, wie in IEC 62351-8 definiert, entsprechen. Anmerkung: Für Einheiten, die Reihen von Kommunikationsprotokollen nach IEC TC 57 verarbeiten, wird davon ausgegangen, dass diese Einheiten die Liste der Standardrollen, d. h. die Standardliste „RoleDefinition“ nach IEC 62351-8 unterstützen müssen. Für Reihen von Kommunikationsprotokollen, die nicht TC 57 entsprechen, müssen andere Rollendefinitionen unterstützt werden.	**Bedingung** Die Bedingung ist, dass ein Benutzer hinter der Erzeugung des IT-Sicherheitsereignisses steht / mit diesem assoziiert ist und dass dem Benutzer eine „Rolle“ zugewiesen wurde.
15	**ParameterName**	**Definition:** Wenn ein Benutzer mit der Erzeugung eines IT-Sicherheitsereignisses assoziiert wurde, muss dieses Attribut den Namen des Parameters oder des Dienstes angeben, auf den der Benutzer während des Auftretens dieses jeweiligen IT-Sicherheitsereignisses zugegriffen hat oder den er ausgeführt hat. **Typ:** UTF-8 [RFC 3629]-kodierte Zeichenkette mit 64 Zeichen, d. h. innerhalb eines Zeichenbereichs von 0 bis 63, kodiert mit UTF-8.	**Bedingung** Die Bedingung ist, dass ein Benutzer hinter der Erzeugung des IT-Sicherheitsereignisses steht / mit der Erzeugung des IT-Sicherheitsereignisses assoziiert ist und ein Parameter oder Dienst von diesem Benutzer für die Einheit (die das IT-Sicherheitsereignis erzeugt) aufgerufen oder ausgeführt wurde.

Tabelle 2 enthält die verbindlichen und an eine Bedingung geknüpften Attribute. Durch „Bedingung“ wird angezeigt, dass die Einheit ein Attribut nur dann protokollieren wird soll, wenn das entsprechende Merkmal

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62351-14:2020-09

und die entsprechende Fähigkeit darin vorhanden ist. Die entsprechenden Bedingungen sind in Tabelle 2 aufgeführt.

Ein Ereignisprotokoll wie Syslog kann von der Einheit verwendet werden, um diese Attribute zu protokollieren. Abschnitt 7 beschreibt, wie eine solche Protokollierung mit Syslog durchgeführt wird.

5.3 Zuweisung von numerischen Bereichen zu IT-Sicherheitsereignis-Kennungen

Um Interoperabilität und Vereinheitlichung sicherzustellen, ist die Zuweisung einer eindeutigen Ereigniskennung für alle IT-Sicherheitsereignisse wichtig, und daher ist ein Zuweisungsschema für das Attribut „ID“ erforderlich, wie in Tabelle 1 und Tabelle 2 angegeben. Mit diesem Zuweisungsschema wird ein globaler Raum für die IT-Sicherheitsereignis-Kennungen auf Grundlage der Kategorisierung und des Typs zugewiesen. Hierbei gilt das folgende Schema:

Domain ID:event number – Der Datentyp ist eine Zeichenkette. Die Obergrenze ist eine Zeichenkette mit 128 Zeichen, kodiert nach UTF-8 [RFC 3629].

Die Beschreibung der beiden oben genannten Unterfelder ist nachfolgend aufgeführt:

- „Domain ID“: Dieses Feld muss die Einheit definieren, die Eigentümer dieser Ereignis-ID ist. Dies kann ein Normungs- oder privater Anbieter sein. Der Datentyp dieses Feldes muss eine ASCII-Zeichenkette [a-zA-Z0-9_\-] (max. 32 Bytes) sein
    - Bei IT-Sicherheitsereignissen im Zusammenhang mit der Normung muss der Wert dieses Feldes der Titel der Norm sein. Die generische Reihe von IT-Sicherheitsereignissen, die in dieser Norm in A.1 aufgeführt ist, muss den Wert „IEC 62351-14“ haben. Für die IT-Sicherheitsereignisse, die für jeden der anderen relevanten Teile von IEC 62351 spezifisch sind, müssen die jeweiligen Normentitel für dieses Fachgebiet angegeben werden. Beispielsweise müssen die IT-Sicherheitsereignisse, die aus IEC 62351-3 stammen, für dieses Feld den Wert IEC 62351-3 haben.
    - Bei IT-Sicherheitsereignissen, die sich auf private Einheiten beziehen, wie z. B. Anbieterangaben, muss der Wert dieses Feldes dem von der IANA zugewiesenen numerischen Wert des jeweiligen Anbieters entsprechen. Daher muss er die Kennung des Anbieters sein, so wie er von der IANA registriert ist https://www.iana.org/assignments/enterprise-numbers/enterprise-numbers.
- „Event Number“: Dieses Feld enthält einen numerischen Wert, der jedem der IT-Sicherheitsereignisse, die zur jeweiligen „Domain ID“ gehören, zugeordnet wird. Dabei muss es sich um eine 32-Bit-Zahl ohne Vorzeichen handeln, die zwischen 1 und 4294967295 liegt, und zwar in Textform. „0“ ist reserviert.

6 Protokollierung von IT-Sicherheitsereignissen unter Verwendung von Syslog

Dieser Abschnitt beschreibt das Verfahren zur Protokollierung von IT-Sicherheitsereignissen mit Syslog. Konkret wird beschrieben, wie die Attribute der abstrakten Informationsstruktur protokolliert werden, wie in Tabelle 2 für die Protokollierung mit Syslog beschrieben. Diese Norm muss sich auf [RFC 5424] für die Protokollierung mit Syslog beziehen. [RFC 5424] ist die neueste Norm für die Protokollierung eines Ereignisses im Syslog-Format. Sie bietet die Möglichkeit, ein Ereignis zu protokollieren, indem sowohl ein strukturiertes als auch ein unstrukturiertes Format verwendet wird.

Zur Protokollierung von IT-Sicherheitsereignissen nach dieser Norm unter Verwendung von Syslog [RFC 5424] ist es zwingend erforderlich, die Attribute der abstrakten Informationsstruktur wie in Tabelle 2 beschrieben mit den entsprechenden äquivalenten Syslog [RFC 5424]-Feldern abzubilden. Diese Abbildung muss die Verwendung von Syslog [RFC 5424] zur Protokollierung der Attribute der abstrakten Informationsstruktur eines IT-Sicherheitsereignisses, wie in Tabelle 2 festgelegt, ermöglichen.

6.1 Protokollierung unter Verwendung des strukturierten Syslog-Formats RFC 5424

Dieser Abschnitt stellt eine Abbildung der abstrakten Informationsstruktur des IT-Sicherheitsereignisses dieser Norm auf die Felder von Syslog [RFC 5424] dar. Tabelle 3 beschreibt diese Abbildung

AVA Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62351-14:2020-09

Tabelle 3 – Abbildung der Struktur abstrakter Informationen nach IEC 62351 auf die Meldungsfelder von Syslog [RFC 5424] (1 von 5)

Protokollierungsattribute nach IEC 62351-14	Meldungsfelder von Syslog RFC 5424
Severity **Typ:** UTF-8 [RFC 3629]-kodierte Zeichenkette mit einem der folgenden Werte: {alarm, error, notice und warning}. Das Attribut „Severity“ in der abstrakten Struktur gibt den Schärfegrad des IT-Sicherheitsereignisses nach IEC 62351-14 an. Daher muss sie auf das Feld „PRI“ der Kopfzeile abgebildet werden.	**Kopfzeilen-Feld: PRI** -- *gibt die Priorität der Syslog-Meldung an, wie in [RFC 5424] definiert* **Wert:** Anmerkung: Der Feldwert „PRI“ für die IT-Sicherheitsereignisse dieser Norm muss quantitativ abgeleitet werden, wie in Abschnitt 6.3 beschrieben.
	Kopfzeilen-Feld: VERSION -- *gibt die Versionsnummer der Syslog-Meldung an, wie in [RFC 5424] definiert* **Wert:** 1 Anmerkung: Die aktuelle Versionsnummer von [RFC 5424] ist „1“, entsprechend [RFC 5424]-Spezifikation.
Zeitstempel **Typ:** UTC-Zeitformat nach [IEC 62351-4] Anmerkung: Wenn die Einheit nicht in der Lage ist, einen Zeitstempel im UTC-Format zu erstellen, kann ein Zeitversatz verwendet werden. TIME-OFFSET = „Z“ / TIME-NUMOFFSET TIME-NUMOFFSET = („+“ / „-“) TIME-HOUR „:“ TIME-MINUTE Dieses Attribut gibt den Wert des Zeitpunkts an, zu dem das jeweilige IT-Sicherheitsereignis von der „Source“ erzeugt wurde.	**Kopfzeilen-Feld:** TIMESTAMP -- *gibt den Zeitstempel der generierten Syslog-Meldung an, wie in [RFC 5424] definiert.* **Wert:** - Anmerkung: Der Zeitstempel sollte in UTC angegeben werden. Wenn die Ortszeit verwendet wird, muss ein Zeitzonenversatz vorgesehen werden.
Protokollierungsattribute nach IEC 62351-14	**Meldungsfelder von Syslog RFC 5424**
	Kopfzeilen-Feld: HOSTNAME -- *gibt den Hostnamen der Einheit an, die die Syslog-Meldung entsprechend der Definition in [RFC 5424] generiert hat. Dies kann ein FQDN, ein Hostname, eine statische oder dynamische IP-Adresse, Version 4, eine statische oder dynamische IP-Adresse, Version 6 oder ein „NIL“-Wert sein, wenn die Einheit nicht in der Lage ist, einen Wert für dieses jeweilige Attribut entsprechend [RFC 5424] zuzuweisen. Die bevorzugte Reihenfolge dieser Optionen muss nach [RFC 5424] festgelegt werden.* **Wert:** Anmerkung: FQDN oder Hostname oder IP-Adresse, Version 4 oder Version 6, oder ein NIL-Wert entsprechend [RFC 5424].

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62351-14:2020-09

Tabelle 3 (2 von 5)

Protokollierungsattribute nach IEC 62351-14	Meldungsfelder von Syslog RFC 5424
ProdName **Typ**: UTF-8 [RFC 3629]-kodiert mit 8 Zeichen, d. h. innerhalb eines Zeichenbereichs von 0 bis 7, kodiert mit UTF-8. Das Attribut „ProdName“ gibt den Namen der Einheit an, die die IT-Sicherheitsereignisse nach IEC 62351-14 erzeugt. Daher ist es sinnvoll, es auf das Syslog-Kopfzeilenfeld „APP-NAME“ abzubilden [RFC 5424].	**Kopfzeilen-Feld: APP-NAME** -- *identifiziert die Einheit, die die Syslog-Meldung erzeugt hat. Ein „NIL“-Wert, wenn die Einheit nicht in der Lage ist, einen Wert für dieses jeweilige Attribut entsprechend [RFC 5424] zuzuweisen. Da außerdem „ProdName“, wie in Tabelle 2 angegeben, optional ist, erfüllt die Zuweisung eines „NIL“-Wertes die Vorgabe, dass sie optional sein muss.* ***Wert:***
	Kopfzeilen-Feld: PROCID -- *gibt die Prozesskennung oder den Prozessnamen an, die bzw. der mit der generierten Syslog-Meldung entsprechend der Definition in [RF 5424] assoziiert ist. Ein „NIL“-Wert, wenn die Einheit nicht in der Lage ist, einen Wert für dieses jeweilige Attribut entsprechend [RFC 5424] zuzuweisen.* **Wert:** Anmerkung: Im Rahmen dieser Norm muss PROCID einen „NIL“-Wert haben, da dies im Zusammenhang mit der mit dieser Norm assoziierten Interoperabilität nicht von Bedeutung ist.
LogType und IECversion **LogType** **Typ:** Kodierte feste Zeichenkette UTF-8 [RFC 3629] mit dem Wert „IEC62351-14“. Das Attribut „LogType“ in abstrakter Struktur zeigt ein IT-Sicherheitsereignis nach IEC 62351-14 an. **IECversion** **Typ:** Monoton steigende ganze Zahl von 1 bis 65535. Der Startwert für diese Ausgabe der Norm ist der ganzzahlige Wert 1. „IECversion“ gibt die Versionsnummer der Norm IEC 62351-14 an. Das entsprechende Feld „MSGID“ in Syslog dient als Kennung der Syslog-Meldung, die den Relais und Firewalls hilft, die Meldungen auf Basis ihres Typs zu filtern. Daher würde die Abbildung des Attributs „LogType“ und „IECversion“ auf das Feld „MSGID“ der Syslog-Kopfzeile den Relais und Firewalls helfen, die mit IEC 62351-14 (einschließlich ihrer Version) assoziierten IT-Sicherheitsereignis-Protokoll zu identifizieren und sie weiterzuleiten.	**Kopfzeilen-Feld: MSGID** -- *gibt den Typ der Syslog-Meldung an, wie in [RFC 5424] definiert.* **Wert:** IEC62351-14:1
Protokollierungsattribute nach IEC 62351-14	**Meldungsfelder von Syslog RFC 5424**

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62351-14:2020-09

Tabelle 3 (3 von 5)

Protokollierungsattribute nach IEC 62351-14	Meldungsfelder von Syslog RFC 5424
ID **Typ:** UTF-8 [RFC 3629]-kodiert mit 128 Zeichen, d. h. innerhalb eines Zeichenbereichs von 0 bis 127, kodiert mit UTF-8. Hierbei handelt es sich um eine einmalige und eindeutige numerische Kennung für das IT-Sicherheitsereignis, die dazu beiträgt, dem IT-Sicherheitsereignis eine eindeutige und unverwechselbare numerische Identität zuzuordnen.	**Feld für strukturierte Daten (SD-Element)** PARAM-NAME = ID PARAM-VALUE= „ ” Der Parameterwert, also PARAM-VALUE, muss über 128 Zeichen verfügen und nach UTF-8 [RFC 3629] kodiert sein, d. h er muss in einem Größenbereich von 0 bis 127 Zeichen mit UTF-8-Kodierung liegen. Zeichen, die als Escape-Zeichen nach [RFC 5424] angezeigt werden, müssen befolgt werden.
Text **Typ:** UTF-8 [RFC 3629]-kodiert mit 128 Zeichen, d. h. innerhalb eines Zeichenbereichs von 0 bis 127, kodiert mit UTF-8. Dieses Attribut muss einen Informationstext über das IT-Sicherheitsereignis liefern.	Feld für strukturierte Daten (SD-Element) PARAM-NAME = Text PARAM-VALUE= „ ” Der Parameterwert, also PARAM-VALUE, muss über 128 Zeichen verfügen und nach UTF-8 [RFC 3629] kodiert sein, d. h er muss in einem Größenbereich von 0 bis 127 Zeichen mit UTF-8-Kodierung liegen. Zeichen, die als Escape-Zeichen nach [RFC 5424] angezeigt werden, müssen befolgt werden.
ExtraInfo **Typ:** UTF-8 [RFC 3629]-kodiert mit 32 Zeichen, d. h. innerhalb eines Zeichenbereichs von 0 bis 31, kodiert mit UTF-8. Dieses Attribut muss zusätzlichen Informationstext über das IT-Sicherheitsereignis liefern, d. h. zusätzlich zu den Informationen, die das Attribut „Text“ erfasst, kann dieses Attribut dazu verwendet werden, zusätzliche nützliche Informationen über das IT-Sicherheitsereignis während der Protokollierung erfassen.	**SD-Elementfeld (mit Bedingung zu protokollieren, wie in Tabelle2 angegeben)** PARAM-NAME = ExtraInfo PARAM-VALUE= „ ” Der Parameterwert, also PARAM-VALUE muss über 32 Zeichen verfügen und nach UTF-8 [RFC 3629] kodiert sein, d. h er muss in einem Größenbereich von 0 bis 31 Zeichen mit UTF-8-Kodierung liegen. Zeichen, die als Escape-Zeichen nach [RFC 5424] angezeigt werden, müssen befolgt werden.
SOE **Typ:** Monoton steigende ganzer Zahlenwert von 1 bis 4294967295. Dieses Attribut muss die laufende Nummer des IT-Sicherheitsereignisses angeben, das von einer Einheit erzeugt wird. Für jedes einzelne IT-Sicherheitsereignis, das von einer Einheit erzeugt wird, muss der Wert dieses Attributs um eins erhöht werden.	**SD-Elementfeld (mit Bedingung zu protokollieren, wie in Tabelle 2 angegeben)** PARAM-NAME = SOE PARAM-VALUE= „ ” Der Parameterwert, also SOE, muss ein monoton ansteigender ganzzahliger Wert von 1 bis 4294967295 sein, der als nach UTF-8 [RFC 3629] kodierte Zeichenkette dargestellt wird. Zeichen, die als Escape-Zeichen nach [RFC 5424] angezeigt werden, müssen befolgt werden.
Protokollierungsattribute nach IEC 62351-14	**Meldungsfelder von Syslog RFC 5424**

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62351-14:2020-09

Tabelle 3 (4 von 5)

Protokollierungsattribute nach IEC 62351-14	Meldungsfelder von Syslog RFC 5424
Source **Typ:** UTF-8 [RFC 3629]-kodiert mit 64 Zeichen, d. h. innerhalb eines Zeichenbereichs von 0 bis 63, kodiert mit UTF-8. Dieses Attribut muss die eindeutige Kennung der Einheit oder einer Anwendung innerhalb einer Einheit liefern, die das IT-Sicherheitsereignis hervorgerufen hat. Zwei Einheiten können den gleichen Namen haben, d. h. zwei Geräte vom gleichen Hersteller könnten den gleichen Namen haben. Zur weiteren Unterscheidung zwischen diesen beiden gleichnamigen Geräten und zur eindeutigen Identifizierung des Geräts, das das IT-Sicherheitsereignis erzeugt hat, kann das Attribut „Source“ verwendet werden, wobei dem Attribut „Source“ eine eindeutige Kennung des Geräts oder einer Anwendung innerhalb des Geräts, das das jeweilige IT-Sicherheitsereignis erzeugt hat, entsprechend zugeordnet werden kann.	**SD-Elementfeld** PARAM-NAME = Source PARAM-VALUE= „ ” Der Parameterwert, also PARAM-VALUE, muss ein über 64 Zeichen verfügen und nach UTF-8 [RFC 3629] kodiert sein, d. h. er muss in einem Größenbereich von 0 bis 63 Zeichen mit UTF-8-Kodierung liegen. Zeichen, die als Escape-Zeichen nach [RFC 5424] angezeigt werden, müssen befolgt werden.
UsrID **Typ:** UTF-8 [RFC 3629]-kodiert mit 32 Zeichen, d. h. innerhalb eines Zeichenbereichs von 0 bis 31, kodiert mit UTF-8. Dieses Attribut muss die eindeutige Kennung eines Benutzers liefern, wenn es mit der Erzeugung des IT-Sicherheitsereignisses durch eine Einheit in Verbindung steht.	**SD-Elementfeld (mit Bedingung zu protokollieren, wie in Tabelle 2 angegeben)** PARAM-NAME = UsrID PARAM-VALUE= „ ” Der Parameterwert, also PARAM-VALUE, muss ein über 32 Zeichen verfügen und nach UTF-8 [RFC 3629] kodiert sein, d. h. er muss in einem Größenbereich von 0 bis 31 Zeichen mit UTF-8-Kodierung liegen. Zeichen, die als Escape-Zeichen nach [RFC 5424] angezeigt werden, müssen befolgt werden.
RemoteIP: Port **Typ:** IP-Adresse, Version 4 [RFC 791]: Port-Nummer [RFC 6335] Dieses Attribut muss die IP-Adresse und Port-Nummer der Einheit angeben, von der aus während des Auftretens des jeweiligen IT-Sicherheitsereignisses auf die Einheit zugegriffen wurde, die das IT-Sicherheitsereignis erzeugt hat.	**SD-Elementfeld (mit Bedingung zu protokollieren, wie in Tabelle 2 angegeben)** PARAM-NAME = RemoteIP:Port PARAM-VALUE= „ ” Der Parameterwert, also PARAM-VALUE, muss ein über 32 Zeichen verfügen und nach UTF-8 [RFC 3629] kodiert sein, d. h. er muss in einem Größenbereich von 0 bis 31 Zeichen mit UTF-8-Kodierung liegen. Zeichen, die als Escape-Zeichen nach [RFC 5424] angezeigt werden, müssen befolgt werden.

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62351-14:2020-09

Tabelle 3 (5 von 5)

Protokollierungsattribute nach IEC 62351-14	Meldungsfelder von Syslog RFC 5424
RoleID **Typ:** Der Datentyp des Attributs „RoleID“ muss dem Datentyp des Attributs „RoleID“ wie in IEC 62351-8 definiert entsprechen. Wenn ein Benutzer mit der Erzeugung eines IT-Sicherheitsereignisses in Verbindung gebracht wurde, muss dieses Attribut die Rollenkennung des jeweiligen Benutzers liefern.	**SD-Elementfeld (mit Bedingung zu protokollieren, wie in Tabelle 2 angegeben)** PARAM-NAME = RoleID PARAM-VALUE= „ ” Der Parameterwert, also PARAM-VALUE, muss ein über 32 Zeichen verfügen und nach UTF-8 [RFC 3629] kodiert sein, d. h. er muss in einem Größenbereich von 0 bis 31 Zeichen mit UTF-8-Kodierung liegen. Zeichen, die als Escape-Zeichen nach [RFC 5424] angezeigt werden, müssen befolgt werden.
Protokollierungsattribute nach IEC 62351-14	**Meldungsfelder von Syslog RFC 5424**
AccountType **Typ**: Der Datentyp des Attributs „AccountType“ muss dem Datentyp des Attributs „RoleDefinition“ wie in IEC 62351-8 definiert entsprechen. Wenn ein Benutzer mit der Erzeugung eines IT-Sicherheitsereignisses assoziiert wurde, muss dieses Attribut den Typ des Benutzerkontos, d. h. die Rollendefinition des Benutzers, angeben.	**SD-Elementfeld (mit Bedingung zu protokollieren, wie in Tabelle 2 angegeben)** PARAM-NAME = AccountType PARAM-VALUE= „ ” Der Parameterwert, also PARAM-VALUE, muss ein über 24 Zeichen verfügen und nach UTF-8 [RFC 3629] kodiert sein, d. h. er muss in einem Größenbereich von 0 bis 23 Zeichen mit UTF-8-Kodierung liegen. Zeichen, die als Escape-Zeichen nach [RFC 5424] angezeigt werden, müssen befolgt werden.
ParameterName Typ: UTF-8 [RFC 3629]-kodierte Zeichenkette mit 64 Zeichen, d. h. innerhalb eines Zeichenbereichs von 0 bis 63, kodiert mit UTF-8. Wenn ein Benutzer mit der Erzeugung eines IT-Sicherheitsereignisses assoziiert wurde, muss dieses Attribut den Namen des Parameters oder des Dienstes angeben, auf den der Benutzer während des Auftretens dieses jeweiligen IT-Sicherheitsereignisses zugegriffen hat oder den er ausgeführt hat.	**SD-Elementfeld (mit Bedingung zu protokollieren, wie in Tabelle 2 angegeben)** PARAM-NAME = AccountType PARAM-VALUE= „ ” Der Parameterwert, also PARAM-VALUE, muss ein über 64 Zeichen verfügen und nach UTF-8 [RFC 3629] kodiert sein, d. h. er muss in einem Größenbereich von 0 bis 63 Zeichen mit UTF-8-Kodierung liegen. Zeichen, die als Escape-Zeichen nach [RFC 5424] angezeigt werden, müssen befolgt werden.

Im Rahmen von IEC 62351-14 muss das Syslog [RFC 5424]-Kopfzeilenfeld „PROCID“ ein „NIL“-Wert sein, da dieses Feld implementierungsabhängig ist und im Zusammenhang mit der IT-Ereignisprotokollierung in einer uneinheitlichen Energieversorgungsumgebung möglicherweise nicht nützlich ist. Für diese Norm muss die SD-Element-Kennung IEC@41912 sein, wobei 41912 die eindeutige Kennung von IEC in IANA ist.

Die strukturierte Syslog-Variante von [RFC 5424] unter Verwendung der strukturierten Datenelemente, wie in Tabelle 3 angegeben, muss verbindlich sein. Die strukturierten Datenelemente, die mit einer Bedingung gekennzeichnet sind, müssen nur dann protokolliert werden, wenn das entsprechende Merkmal und die entsprechende Fähigkeit von der Einheit unterstützt wird. Für diese entsprechenden Bedingungen, siehe Tabelle 2, in der die jeweiligen Bedingungen für die Protokollierungsattribute mit Bedingung angegeben sind. Die Verwendung von unstrukturierten Syslog-Daten unter Verwendung des „MSG“-Feldes [RFC 5424] ist optional. Daher müssen neben den strukturierten Datenelementen, die in Tabelle 2 aufgeführt sind, optional auch unstrukturierte Syslog-Daten unterstützt werden. Dazu unterstützt [RFC 5424] unstrukturierte Ereignis-

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62351-14:2020-09

daten unter Verwendung seines „MSG“-Feldes. Das Feld „MSG“ muss alle zusätzlichen nützlichen Informationen über das IT-Sicherheitsereignis in freier Form enthalten.

Das Feld „MSG“ hat das folgende Format und die folgende Syntax-Definition entsprechend Syslog [RFC 5424].

MSG = MSG-ANY / MSG-UTF8

MSG-ANY = *OCTET; nicht beginnend mit BOM

MSG-UTF8 = BOM UTF-8-STRING

BOM = %xEF.BB.BF

6.2 Abbildung des Schweregrads von IT-Sicherheitsereignissen nach IEC 62351-14 auf Syslog RFC 5424-Prioritätsstufe

Dieser Abschnitt stellt einen Mechanismus zur Verfügung, um das abstrakte Informationsstruktur-Attribut „Severity“, d. h. den Schärfegrad, wie in Tabelle 2 angegeben, auf die Prioritätsstufe in [RFC 5424] abzubilden. Syslog [RFC 5424] definiert die Priorität durch das Attribut „PRI“, das sich aus zwei Teilen zusammensetzt, und zwar „Facility“ und „Severity“. Für diese Norm muss die standardmäßige Einrichtungsebene für ein IT-Sicherheitsereignis „Facility Level – 13“ sein. Dabei handelt es sich um die Syslog-Einrichtungsebene für Auditierung. Der Grund für die Auswahl dieser Einrichtungsebene aus allen derzeit verfügbaren Einrichtungsebenen, die in [RFC 5424] festgelegt sind, liegt in der großen Bedeutung der Auditierung von IT-Sicherheitsereignis-Protokollen und ihrer forensischen Zwecke (ohne darauf beschränkt zu sein) im Rahmen dieser Norm.

Tabelle 4 bietet eine Abbildung des Attributs „Severity“, wie es in der abstrakten Informationsstruktur in Tabelle 2 angegeben ist, mit den entsprechenden numerischen [RFC 5424]-Codes für den Schärfegrad.

Tabelle 4 – Abbildung des Attributs „Severity“ nach IEC 62351 auf den Schärfegrad von Syslog RFC 5424

Schärfegrad des IT-Sicherheitsereignis-Attributs entsprechend IEC 62351-14 – „Severity“		**Attribut „Severity“ von Syslog RFC 5424**	
Bezeichnung: Severity **Typ:** UTF-8 [RFC 3629]-kodierte Zeichenkette mit einem der folgenden Werte – {alarm, error, notice und warning}.		**Nummerncode**	**Schärfegrad**
	Alarm	1	**Alarm:** Es müssen umgehend Maßnahmen ergriffen werden
	Error	3	**Error:** Fehlerbedingungen
	Warning	4	**Warning:** Warnbedingungen
	Notice	5	**Notice:** normale aber wichtige Bedingung

Für diese Norm müssen nur die oben aufgeführten Schärfegrade (0–5) berücksichtigt werden. Der Schärfegrad – „6: Information“ und „7: Debug“ finden im Rahmen dieser Norm keine Anwendung, da der Anwendungsbereich dieser Norm die Erzeugung von Protokollen für die Fehlerbeseitigung („Debugging“) und für Informationszwecke nicht vorsieht.

Zur Verdeutlichung des Abbildungsmechanismus sind nachfolgend zwei Beispiele aufgeführt:

Beispiel 1: Wenn in der abstrakten Informationsstruktur, wie in Tabelle 2 angegeben, der Schärfegrad des IT-Sicherheitsereignisses, d. h. das Attribut „Severity“, „error“ ist, dann wird die entsprechende Abbildung auf das Prioritätsattribut von Syslog [RFC 5424], d. h. „PRI“, als 8*[Facility] + [Severity] = 8*13+3= 107 berechnet, dargestellt als <107> in der generierten Syslog [RFC 5424]-Meldung. „13“ ist die Standard-Einrichtungsebene im Rahmen dieser Norm, und der numerische Code „3“ wird auf Grundlage der in Tabelle 14 beschriebenen Abbildung ausgewählt.

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62351-14:2020-09

Beispiel 2: Wenn in der abstrakten Informationsstruktur, wie in Tabelle 2 angegeben, der Schärfegrad des IT-Sicherheitsereignisses, d. h. das Attribut „Severity“, „alarm“ ist, dann wird die entsprechende Abbildung auf das Prioritätsattribut von Syslog [RFC 5424], d. h. „PRI“, als 8*[Facility] + [Severity] = 8*13+1= 105 berechnet, dargestellt als <105> in der generierten Syslog [RFC 5424]-Meldung. „13“ ist die Standard-Einrichtungsebene im Rahmen dieser Norm. Der numerische Code „1“ wird auf Grundlage der in Tabelle 14 beschriebenen Abbildung und auf Grundlage der des Endbenutzer-Sicherheitsgrundsatzes der Einheit ausgewählt, die das IT-Sicherheitsereignis als „Alarm“ klassifiziert, für den eine sofortige Maßnahme erforderlich ist.

6.3 Sichere und zuverlässige Übertragung von IT-Sicherheitsereignissen unter Verwendung von Syslog

Die Anforderungen, wie IT-Sicherheit und Zuverlässigkeit, die bei der Übermittlung von IT-Sicherheitsereignissen im Energieversorgungssystem, z. B. an einen Syslog-Empfänger, berücksichtigt werden müssen. Eine Einheit, die die Fähigkeit besitzt, über TCP zu kommunizieren, muss die [RFC 5425]-TLS-Abbildung für Syslog verwenden, um die mit Syslog [RFC 5424] formatierten IT-Sicherheitsereignisse dieser Norm sicher und zuverlässig zu übermitteln. [RFC 5425] bietet Schutzmaßnahmen für die IT-Sicherheit wie Authentifizierung, Integrität und Vertraulichkeit von Syslog-Meldungen während der Übertragung über ein TCP-basiertes Kommunikationsnetzwerk. Darüber hinaus bietet es eine zuverlässige Übertragung von Syslog-Meldungen an den Syslog-Empfänger auf der OSI-Transportschicht.

7 Abbildung von Syslog auf SNMP

Wenn Syslog [RFC 5424]-IT-Sicherheitsprotokollierungsmeldungen aus dieser Norm als SNMP-Meldung übertragen werden sollen, dann muss [RFC 5676] verwendet werden, um die Abbildung dieser Syslog-Meldungen auf SNMP durchzuführen und die IT-Sicherheitsereignisse als SNMP-Meldungen weiter zu übertragen.

8 Abbildung von SNMP auf Syslog

Wenn [IEC 62351-7]-SNMP-MIBs als mit Syslog [RFC 5424] formatierte Meldungen zu IT-Sicherheitsereignissen transportiert werden sollen, dann muss [RFC 5675] verwendet werden, um die Abbildung dieser [IEC 62351-7]-SNMP-Meldungen auf [RFC 5424] formatierte Ereignisse durchzuführen, und die weitere Übertragung der IT-Sicherheitsereignisse als [RFC 5424] Syslog-Meldungen mit IT-Sicherheitsschutz kann durch [RFC 5425]-TLS-Mapping für Syslog erfolgen.

9 Empfehlungen zur Speicherung von IT-Sicherheitsereignissen

[IEEE 1686] legt Empfehlungen zu Möglichkeiten zur Speicherung von IT-Sicherheitsereignissen fest. Diese Norm enthält außerdem Empfehlungen für die Endbenutzer, die Spezifikationen zur Möglichkeit der Speicherung von IT-Sicherheitsereignissen, wie in [IEEE 1686] festgelegt, zu berücksichtigen.

Diese Norm enthält auch Empfehlungen zum Schutz der Integrität einer Protokolldatei für IT-Sicherheitsereignisse, d. h. der computergenerierten Datei, in der alle IT-Sicherheitsereignisse aufgezeichnet werden. Eine solche Aufzeichnung findet üblicherweise auf Serverebene statt, wie z. B. im Fall von Syslog [RFC 5424], wo sie auf der Syslog-Serverebene erfolgt, auf der alle IT-Sicherheitsereignisse erfasst und aufgezeichnet werden. Auf dieser Serverebene empfiehlt die Norm einen Integritätsschutz für die Protokolldatei für Cybersicherheitsereignisse und empfiehlt somit, den Benutzern dieser jeweiligen Protokolldatei nur Lesezugriff zu gewähren. Daher empfiehlt diese Norm, dass die Einheit ihren Benutzern unter keinen Umständen erlauben darf, den Inhalt des IT-Sicherheitsprotokolls zu ändern. [IEEE 1686] bietet eine ähnliche Empfehlung zum Integritätsschutz für die Protokolldatei für IT-Sicherheitsereignisse.

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62351-14:2020-09

Anhang A
(informativ)

Auflistung von IT-Sicherheitsereignissen

Diese Norm enthält und klassifiziert IT-Sicherheitsereignisse, die für die Teile von IEC 62351 spezifisch sind, sowie eine Liste von allgemeinen Ereignissen, die im Zusammenhang mit der IT-Sicherheit von Energieversorgungssystemen als hilfreich angesehen werden. Sie stammen aus anderen Normen wie [IEEE 1686], [NERC-CIP], [IEC 62443], [IETF], [ISO 27001] und aus Diskussionen innerhalb des IEC TC57 WG15. Anhang A.1 listet diese „generischen" Ereignisse auf. Die IT-Sicherheitsereignisse, die für jeden Teil der Norm IEC 62351 spezifisch sind, müssen in die Kategorie „IT-Sicherheitsereignisse fallen, die für die Norm IEC 62351 spezifisch sind", wie in Anhang A.2 beschrieben.

Jedes dieser Ereignisse wird unter Verwendung der in 5.1, Tabelle 1 definierten Informationsstruktur beschrieben. Diese Ereignisse müssen nicht verbindlich in einer Einheit unterstützt werden. Sie müssen nur dann unterstützt werden, wenn das zugehörige Merkmal in einer Einheit vorhanden ist. Wenn z. B. eine Einheit keine Anmeldefunktion für Benutzer hat, ist es nicht zwingend erforderlich, dass diese Einheit die in Anhang A.1 aufgeführten IT-Sicherheitsereignisse für die Anmeldung von Benutzern unterstützt. In ähnlicher Weise ist es nicht zwingend erforderlich, die [IEC 62351-3]-spezifischen, auf TLS [RFC 5246] bezogenen IT-Sicherheitsereignisse, die in Anhang A.2 aufgeführt sind, zu unterstützen, wenn eine Einheit über keine für [IEC 62351-3] spezifischen Merkmale zur Sicherung der TC 57-Reihe an Kommunikationsprotokollen verfügt.

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62351-14:2020-09

A.1 Generische IT-Sicherheitsereignisse

Dieser Abschnitt enthält eine Liste von IT-Sicherheitsereignissen, die jedoch nicht auf diese Norm beschränkt sind und die unabhängig von anderen IEC-Normen wie [IEC 62351-3], [IEC 62351-5], [IEC 62351-6], [IEC 62351-7], [IEC 62351-8] usw. sind. Tabelle 5 führt diese generische Klasse von IT-Sicherheitsereignissen auf. Die Einheit muss sie nur dann unterstützen, wenn das entsprechende Merkmal in ihr vorhanden ist und auch auf dem Sicherheitsgrundsatz des Endbenutzers dieser Norm basiert. Eine Reihe dieser generischen IT-Sicherheitsereignisse, wie sie in Tabelle 5 aufgeführt sind, stammen aus Verweisungen auf bestehende Normen [IEEE 1686], [NERC-CIP] (wie NERC-CIP-007-5 und NERC-CIP-007-6), [IEC 62443] (wie IEC 62443-4-2), [RFC 2527], [RFC 3647] und [RFC 5425].

Die Endbenutzer dieser Norm können nur den Wert für den Schärfegrad, „Severity“, entsprechend ihrem Sicherheitsgrundsatz ändern. Allerdings wird in dieser Norm ein Schärfegrad für jedes dieser unten aufgeführten IT-Sicherheitsereignisse empfohlen. „MNEMONIC“, „LogType“, „IECversion“, „Numerische IT-Sicherheitsereignis-Kennung (ID)“ und „Text“ müssen für jedes dieser unten aufgeführten IT-Sicherheitsereignisse eindeutig sein, d. h. sie müssen einen eindeutigen Wert wie unten angegeben haben. Die numerische Kennung des Ereignisses wurde entsprechend dem Zuweisungsschema, wie in Abschnitt 5.3 beschrieben, zugewiesen.

Tabelle 5 – Allgemeine IT-Sicherheitsereignisse (1 von 19)

MNEMONIC	LogType	IECversion	Schärfegrad	Numerische IT-Sicherheitsereignis-Kennung (ID)	Text (Einzelnes Leerzeichen zwischen jeweils aufeinanderfolgenden Wörtern)	Verweisung
LOGIN_OK	IEC62351-14	1	notice	IEC 62351-14:1	Anmeldung erfolgreich	[IEEE 1686] legt fest, dass eine Ereignisprotokollierung für die erfolgreiche Anmeldung des Benutzers erforderlich ist. Im Allgemeinen verlangt [IEC 62443-4-2] Audit-Protokolle für die Zugangskontrolle.
LOGIN_OK_PW_EXPIRED	IEC62351-14	1	notice	IEC 62351-14:2	Passwort abgelaufen, Anmeldung erfolgreich	[NERC-CIP-007-5] erfordert einen Sicherheitsgrundsatz. Falls der lokale Sicherheitsgrundsatz der Einheit es einem Benutzer erlaubt, sich trotz abgelaufenem Passwort anzumelden, z. B. zur Behebung einer kritischen Notfallsituation, dann wäre dieses Ereignis nützlich. Im Allgemeinen verlangt [IEC 62443-4-2] Audit-Protokolle für die Zugangskontrolle.

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62351-14:2020-09

Tabelle 5 (2 von 19)

MNEMONIC	LogType	IECversion	Schärfegrad	Numerische IT-Sicherheitsereignis-Kennung (ID)	Text (Einzelnes Leerzeichen zwischen jeweils aufeinanderfolgenden Wörtern)	Verweisung
LOGIN_FAIL_WRONG_CR	IEC62351-14	1	notice	IEC 62351-14:3	Anmeldung fehlgeschlagen – Falsche Anmeldedaten	[NERC-CIP-007-5] erfordert IT-Sicherheit bzw. Protokollierung sowohl für erfolgreiche als auch für fehlgeschlagene Anmeldungen von Benutzern. Im Allgemeinen verlangt [IEC 62443-4-2] Audit-Protokolle für die Zugangskontrolle.
LOGIN_FAIL_PW_EXPIRED	IEC62351-14	1	alarm	IEC 62351-14:4	Anmeldung fehlgeschlagen – Passwort abgelaufen	
LOGIN_FAIL_3_TIMES	IEC62351-14	1	alarm	IEC 62351-14:5	Anmeldung 3 Mal fehlgeschlagen	[IEEE 1686] Auch wenn [IEEE 1686] angibt, dass ein Ereignis nach 3 nicht erfolgreichen Zugriffsversuchen protokolliert werden soll, gilt, dass eine Einheit umso sicherer ist je früher diese Anomalie protokolliert wird.
LOGIN_FAIL_SESSIONS_LIMIT	IEC62351-14	1	alarm	IEC 62351-14:6	Anmeldung fehlgeschlagen – zu viele Benutzersitzungen	[IEEE 1686] [NERC-CIP-007-5] erfordert IT-Sicherheit bzw. Protokollierung sowohl für erfolgreiche als auch für fehlgeschlagene Anmeldungen von Benutzern. Im Allgemeinen verlangt [IEC 62443-4-2] Audit-Protokolle für die Zugangskontrolle.

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62351-14:2020-09

Tabelle 5 (3 von 19)

MNEMONIC	LogType	IECversion	Schärfegrad	Numerische IT-Sicher-heitsereignis-Kennung (ID)	Text (Einzelnes Leerzeichen zwischen je-weils aufein-anderfolgen-den Wörtern)	Verweisung
LOCK_USER_WRONG_CR	IEC62351-14	1	alarm	IEC 62351-14:7	Benutzer ge-sperrt – Falsche Anmeldedaten	[NERC-CIP-007-6] empfiehlt, die Anzahl der erfolglosen Anmel-deversuche zu begren-zen und Maßnahmen zur Sperrung von Be-nutzerkonten zu ergrei-fen. Falls der lokale Sicher-heitsgrundsatz der Ein-heit ihren Zugriff auf ei-nen Benutzer für eine bestimmte Zeitspanne aufgrund einer be-stimmten Anzahl von wiederholten fehlge-schlagenen Anmelde-versuchen dieses Be-nutzers einschränkt, muss ein entsprechen-des Ereignis generiert werden. Diese Art von Ereignis verbessert die Sicherheit einer Einheit, indem es die Angriffs-fläche für Brute-Force-Angriffe reduziert. Im Allgemeinen verlangt [IEC 62443-4-2] Audit-Protokolle für die Zu-gangskontrolle.
LOGOUT_USER	IEC62351-14	1	notice	IEC 62351-14:8	Abmeldung (Benutzer ab-gemeldet)	[IEEE 1686] spezifiziert die Ereignisprotokollie-rung für die vom Benut-zer veranlasste Abmel-dung.
LOGOUT_TIMEOUT	IEC62351-14	1	notice	IEC 62351-14:9	Abmeldung durch Inaktivität des Benutzers (Timeout)	[IEEE 1686] legt die Er-eignisprotokollierung für Benutzer fest, wenn der Benutzer nach der An-meldung für eine be-stimmte Zeitspanne in-aktiv ist.

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62351-14:2020-09

Tabelle 5 (4 von 19)

MNEMONIC	LogType	IECversion	Schärfe-grad	Numerische IT-Sicherheitser-eignis-Kennung (ID)	Text (Einzelnes Leerzeichen zwischen je-weils aufein-anderfolgen-den Wörtern)	Verweisung
VIEW_SEC_EV_LIST_OK	IEC62351-14	1	notice	IEC 62351-14:10	Sicherheitser-eignis-Proto-kolle erfolgreich angezeigt	[IEEE 1686] legt fest, dass eine Ereignisprotokollie-rung für den „Audit-Protokollierungs-Zugriff“ erforderlich ist.
FILE_HASH_CHECK_FAIL	IEC62351-14	1	alarm	IEC 62351-14:11	Datei-Hash-Prüfung fehlge-schlagen	[NERC-CIP-007-5] legt fest, dass schäd-licher Code erkannt werden muss. Für diesen Zweck ist eine Protokollierung ein hervorragendes Ver-fahren. Dieses Ereig-nis könnte helfen, eine gefährliche bzw. schädliche Konfigura-tionsdatei zu erken-nen, da sich der Hash-Wert der Datei idealerweise vom Hash-Wert der echten Konfigurationsdatei unterscheidet. [IEEE 1686] empfiehlt außerdem eine Mög-lichkeit zur Erken-nung einer schädli-chen Konfigurations-datei und schlägt ei-nen kryptographi-schen Mechanismus, eine digitale Signatur vor, um sie zu si-chern.
FILE_DS_CHECK_FAIL	IEC62351-14	1	alarm	IEC 62351-14:12	Prüfung der di-gitalen Datei-signatur fehlge-schlagen	
WRITE_CERTS_FAIL	IEC62351-14	1	notice	IEC 62351-14:13	Speicherung und Schreiben von Zertifikaten in der Einheit fehlgeschlagen	[RFC 2527] legt fest, dass eine Ereignis-protokollierung für di-gitale Zertifikate, wie z. B. lebenszyklusbe-zogene Ereignisse, vorhanden sein muss.

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62351-14:2020-09

Tabelle 5 (5 von 19)

MNEMONIC	LogType	IECversion	Schärfegrad	Numerische IT-Sicher-heitsereignis-Kennung (ID)	Text (Einzelnes Leerzeichen zwischen je-weils aufein-anderfolgen-den Wörtern)	Verweisung
SW_UPDATE_OK	IEC62351-14	1	notice	IEC 62351-14:14	Software-Aktua-lisierung erfolg-reich	[IEEE 1686] erfordert eine Audit-Protokollierung für auf die Firmware be-zogene Aspekte. Eine Software ist ge-nerisch, dies umfasst auch Firmware.
SW_UPDATE_FAIL	IEC62351-14	1	alarm	IEC 62351-14:15	Software-Aktua-lisierung fehlge-schlagen	
VIEW_SEC_EV_LIST_FAIL	IEC62351-14	1	notice	IEC 62351-14:16	Anzeigen der Liste der Si-cherheitsereig-nisse fehlge-schlagen	[IEEE 1686] legt fest, dass eine Ereignisprotokollie-rung für den „Audit-Protokollierungs-Zugriff“ erforderlich ist.
PW_RESET_FACTORY_DEF	IEC62351-14	1	alarm	IEC 62351-14:17	Zurücksetzen auf Werksein-stellungen	[IEEE 1686] legt fest, dass eine Ereignisprotokollie-rung für die Änderung des Passworts erfor-derlich ist.
USER_ACCNT_CREATE_OK	IEC62351-14	1	notice	IEC 62351-14:18	Erstellung des Benutzerkontos erfolgreich	[IEEE 1686] legt fest, dass eine Ereignis-protokollierung für die erfolgreiche Anmel-dung des Benutzers erforderlich ist.
USER_ACCNT_ENABLE_OK	IEC62351-14	1	notice	IEC 62351-14:19	Aktivierung des Benutzerkontos erfolgreich	
USER_ACCNT_DISABLE_OK	IEC62351-14	1	notice	IEC 62351-14:20	Deaktivierung des Benutzer-kontos erfolg-reich	[IEEE 1686] legt fest, dass eine Ereignis-protokollierung für die Änderung eines Be-nutzerkontos erfor-derlich ist. Das Deak-tivieren und/oder Lö-schen eines Benut-zerkontos deutet auf eine Änderung des jeweiligen Benutzer-kontos hin.
USER_ACCNT_DEL_OK	IEC62351-14	1	notice	IEC 62351-14:21	Löschen des Benutzerkontos erfolgreich	

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62351-14:2020-09

Tabelle 5 (6 von 19)

MNEMONIC	LogType	IECversion	Schärfegrad	Numerische IT-Sicherheitsereignis-Kennung (ID)	Text (Einzelnes Leerzeichen zwischen jeweils aufeinanderfolgenden Wörtern)	Verweisung
USER_ACCNT_CREATE_FAIL	IEC62351-14	1	notice	IEC 62351-14:22	Erstellung des Benutzerkontos fehlgeschlagen	[IEEE 1686] legt fest, dass eine Ereignisprotokollierung für die erfolgreiche Anmeldung des Benutzers erforderlich ist. Wenn Erstellung, Aktivierung und Deaktivierung eines Benutzerkontos fehlschlagen, ist es wichtig, dass auch dieser Status protokolliert wird.
USER_ACCNT_ENABLE_FAIL	IEC62351-14	1	notice	IEC 62351-14:23	Aktivierung des Benutzerkontos fehlgeschlagen	
USER_ACCNT_DISABLE_FAIL	IEC62351-14	1	notice	IEC 62351-14:24	Deaktivierung des Benutzerkontos fehlgeschlagen	
USER_ACCNT_DEL_FAIL	IEC62351-14	1	notice	IEC 62351-14:25	Löschen des Benutzerkontos fehlgeschlagen	
USER_NEW_ROLE_OK	IEC62351-14	1	notice	IEC 62351-14:26	Zuweisung einer neuen Benutzerrolle erfolgreich	[IEEE 1686] legt fest, dass eine Ereignisprotokollierung für die rollenbasierte Zugriffssteuerung (RBAC) erforderlich ist.
USER_PERMISSION_CHANGE_OK	IEC62351-14	1	notice	IEC 62351-14:27	Änderung der Berechtigung erfolgreich	
USER_PERMISSION_ADDED_OK	IEC62351-14	1	notice	IEC 62351-14:28	Hinzufügen der Berechtigung erfolgreich	
USER_ROLE_REMOVED_OK	IEC62351-14	1	notice	IEC 62351-14:29	Entfernen der zugewiesenen Benutzerrolle erfolgreich	
USER_PERMISSION_REMOVED_OK	IEC62351-14	1	notice	IEC 62351-14:30	Entfernen der Benutzerberechtigung erfolgreich	
NEW_ROLE_CREATE_OK	IEC62351-14	1	notice	IEC 62351-14:31	Erstellung der neuen Rolle erfolgreich	

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62351-14:2020-09

Tabelle 5 (7 von 19)

MNEMONIC	LogType	IECversion	Schärfegrad	Numerische IT-Sicher-heitsereignis-Kennung (ID)	Text (Einzelnes Leerzeichen zwischen je-weils aufein-anderfolgen-den Wörtern)	Verweisung
ROLE_DELETE_OK	IEC62351-14	1	notice	IEC 62351-14:32	Löschen der Rolle erfolgreich	
USER_PW_CHANGE_OK	IEC62351-14	1	notice	IEC 62351-14:33	Änderung des Benutzerpass-worts erfolgreich	
USER_PW_CHANGE_FAIL	IEC62351-14	1	notice	IEC 62351-14:34	Änderung des Benutzerpass-worts fehlge-schlagen	
USER_NEW_ROLE_FAIL	IEC62351-14	1	notice	IEC 62351-14:35	Zuweisung der neuen Benut-zerrolle fehlge-schlagen	
USER_PERMISSION_CHANGE_FAIL	IEC62351-14	1	notice	IEC 62351-14:36	Änderung der Berechtigung fehlgeschlagen	
USER_PERMISSION_ADDED_FAIL	IEC62351-14	1	notice	IEC 62351-14:37	Hinzufügen der Berechtigung fehlgeschlagen	
USER_PW_CHANGE_FAIL_SHORT	IEC62351-14	1	notice	IEC 62351-14:38	Änderung des Benutzerpass-worts fehlge-schlagen – zu kurz	[NERC-CIP-007-5] empfiehlt, dass ein Sicherheitsgrundsatz für Benutzerpass-wörter vorhanden sein sollte. Zudem wird eine bestimmte Passwortlänge fest-gelegt. Daher ist die Protokollierung der Prüfung der Pass-wortrichtlinie wichtig.
USER_PW_CHANGE_FAIL_POLICY	IEC62351-14	1	notice	IEC 62351-14:39	Änderung des Benutzerpass-worts fehlge-schlagen – Richtlinienprü-fung fehlge-schlagen	
USER_SESSION_ROLE_CHANGE_OK	IEC62351-14	1	notice	IEC 62351-14:40	Änderung der Sitzungsrolle des Benutzers erfolgreich	[IEEE 1686] legt fest, dass eine Ereignis-protokollierung für die rollenbasierte Zugriffssteuerung (RBAC) erforderlich ist.

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62351-14:2020-09

Tabelle 5 (8 von 19)

MNEMONIC	LogType	IECversion	Schärfegrad	Numerische IT-Sicherheitsereignis-Kennung (ID)	Text (Einzelnes Leerzeichen zwischen jeweils aufeinanderfolgenden Wörtern)	Verweisung
USER_SESSION_ROLE_CHANGE_FAIL	IEC62351-14	1	notice	IEC 62351-14:41	Änderung der Sitzungsrolle des Benutzers fehlgeschlagen	
USER_ROLE_REMOVED_FAIL	IEC62351-14	1	notice	IEC 62351-14:42	Entfernung der Rollenzuweisung fehlgeschlagen	
USER_PERMISSION_REMOVED_FAIL	IEC62351-14	1	notice	IEC 62351-14:43	Entfernen der Benutzerberechtigung fehlgeschlagen	
NEW_ROLE_CREATE_FAIL	IEC62351-14	1	notice	IEC 62351-14:44	Erstellung der neuen Rolle fehlgeschlagen	
ROLE_DELETED_FAIL	IEC62351-14	1	notice	IEC 62351-14:45	Löschen der Rolle fehlgeschlagen	
TCP_COMM_LOG_SUBS_FAIL	IEC62351-14	1	alarm	IEC 62351-14:46	TCP-Kommunikation mit dem Sicherheitsprotokoll-Subscriber fehlgeschlagen	Der Sicherheitsprotokoll-Server (d. h. die Einheit, die sich üblicherweise für den Empfang der IT-Sicherheits-Ereignisprotokolle anmeldet) ist eine entscheidende Einheit, in der üblicherweise alle Protokolldaten gespeichert werden müssen. Wenn die Kommunikation mit dem Protokollserver, wie z. B. die TCP-Kommunikation, aus einem beliebigen Grund, wie z. B. einer Netzwerküberlastung, ausfällt, ist es wichtig, dass ein entsprechendes Ereignis protokolliert wird.

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62351-14:2020-09

Tabelle 5 (9 von 19)

MNEMONIC	LogType	IECversion	Schärfegrad	Numerische IT-Sicher-heitsereig-nis-Kennung (ID)	Text (Einzelnes Leerzeichen zwischen je-weils aufein-anderfolgen-den Wörtern)	Verweisung
						RFC 5425] weist auf die Initiierung der TLS-Kommunkation vom Absender der Übertra-gung (d. h. Protokoll-Sender) zum Empfän-ger der Übertragung (d. h. Protokoll-Server) hin. Wenn die Kommu-nikation in dieser Phase nicht zustande kommt, ist es wichtig, dass ein entsprechen-des Ereignis vorhan-den ist.
LOG_DATA_ HASH_FAIL	IEC62351-14	1	alarm	IEC 62351-14:47	Protokolldaten-Hash-Prüfung fehlgeschlagen (Protokolldaten verändert)	[IEEE 1686] und diese Norm empfehlen einen Integritätsschutz für die Protokolle. Kryp-tographisches Hashing ist eine Eigenschaft, die die Integrität, d. h. den Schutz vor einer Manipulation von Da-ten, sicherstellt. Wenn das Protokolldaten-Hashing aus einem be-liebigen Grund fehl-schlägt, sollte ein ent-sprechendes Ereignis generiert werden.

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62351-14:2020-09

Tabelle 5 (10von 19)

MNEMONIC	LogType	IECversion	Schärfegrad	Numerische IT-Sicher-heitsereig-nis-Kennung (ID)	Text (Einzelnes Leerzeichen zwischen je-weils aufein-anderfolgen-den Wörtern)	Verweisung
TCP_COMM _LOG_PUBL _FAIL	IEC62351-14	1	alarm	IEC 62351-14:48	TCP-Kommuni-kation mit dem Sicherheitspro-tokoll-Publisher fehlgeschlagen	Wenn der Sicherheits-protokoll-Server die Verbindung mit der Einheit, die die Sicher-heitsprotokolle an ihn übermittelt, schließt, wie in [RFC 5425] be-schrieben, wenn vom Syslog-Sender zum Syslog-Empfänger (d. h. Syslog-Server) für längere Zeit keine Daten erhalten wer-den, könnte der Sys-log-Server eine Über-mittlung einer „close_notify“-Alarm-meldung an den Ab-sender der Übertra-gung auslösen. Wenn zu diesem Zeitpunkt die Kommunikation aus einem bestimmten Grund abbricht, ist es wichtig, dass ein ent-sprechendes Ereignis generiert wird, das darauf hinweist, dass die „close_notify“-Mel-dung des Protokollser-vers (d. h. des Emp-fängers des Protokolls) an den Absender des Protokolls (der die Protokolle im Wesent-lichen sendet und da-mit veröffentlicht) nicht erfolgreich gesendet und zugestellt wird.

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62351-14:2020-09