

DIN EN 62734

ICS 35.100.70; 35.110; 35.240.50

**Industrielle Kommunikationsnetze –
Drahtlose Kommunikationsnetze und Kommunikationsprofile –
ISA 100.11a
(IEC 62734:2014);
Englische Fassung EN 62734:2015**

Industrial networks –
Wireless communication network and communication profiles –
ISA 100.11a
(IEC 62734:2014);
English version EN 62734:2015

Réseaux industriels –
Réseau de communication sans fil et profils de communication –
ISA 100.11a
(CEI 62734:2014);
Version anglaise EN 62734:2015

Gesamtumfang 903 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

Anwendungsbeginn

Anwendungsbeginn für die von CENELEC am 2014-12-02 angenommene Europäische Norm als DIN-Norm ist 2015-07-01.

Nationales Vorwort

Vorausgegangener Norm-Entwurf: E DIN EN 62734:2014-05.

Für dieses Dokument ist das nationale Arbeitsgremium K 956 „Feldbus“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE (www.dke.de) zuständig.

Die enthaltene IEC-Publikation wurde vom SC 65C „Industrial networks“ erarbeitet.

Das IEC-Komitee hat entschieden, dass der Inhalt dieser Publikation bis zu dem Datum (stability date) unverändert bleiben soll, das auf der IEC-Website unter „<http://webstore.iec.ch>“ zu dieser Publikation angegeben ist. Zu diesem Zeitpunkt wird entsprechend der Entscheidung des Komitees die Publikation

- bestätigt,
- zurückgezogen,
- durch eine Folgeausgabe ersetzt oder
- geändert.

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

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

Der Zusammenhang der zitierten Normen mit den entsprechenden Deutschen Normen 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.

Das Präsidium des DIN hat mit Präsidialbeschluss 1/2004 festgelegt, dass DIN-Normen, deren Inhalt sich auf internationale Arbeitsergebnisse der Informationsverarbeitung gründet, unter bestimmten Bedingungen allein in englischer Sprache veröffentlicht werden dürfen. Diese Bedingungen sind für die vorliegende Norm erfüllt.

Da sich die Benutzer der vorliegenden Norm der englischen Sprache als Fachsprache bedienen, wird die Englische Fassung der EN 62734 veröffentlicht. Zu deren Abschnitt 1, der den Anwendungsbereich festlegt, und Abschnitt 3, der die Begriffe festlegt, wurde eine Übersetzung angefertigt und als informativer Nationaler Anhang NA der vorliegenden Norm hinzugefügt. Für viele der verwendeten Begriffe existieren keine gebräuchlichen deutschen Benennungen, da sich die deutschen Anwender in der Regel ebenfalls der englischen Benennungen bedienen. Diese Norm steht nicht in unmittelbarem Zusammenhang mit Rechtsvorschriften und ist nicht als Sicherheitsnorm anzusehen.

Das Original-Dokument enthält Bilder in Farbe, die in der Papierversion in einer Graustufen-Darstellung wiedergegeben werden. Elektronische Versionen dieses Dokuments enthalten die Bilder in der originalen Farbdarstellung.

Nationaler Anhang NA (informativ)

0 Einleitung

0.1 Allgemeines

Die vorliegende Norm stellt Spezifikationen in Übereinstimmung mit dem OSI-Basis-Referenzmodell, ISO/IEC 7498-1, (PhL, DL usw.) sowie Sicherheits- und Management-Spezifikationen (einschließlich der Netz- und Gerätekonfiguration) für Funkgeräte der Nutzungsklassen 1 bis 5 nach Anhang C und möglicherweise für feste, tragbare und sich bewegende Geräte der Klasse 0 bereit.

Durch Anwendung der vorliegenden Norm soll ein zuverlässiger und sicherer Funkbetrieb von Anwendungen für die unkritische Beobachtung, Alarmierung, Überwachungssteuerung sowie von Steuerungs- und Regelungsanwendungen bereitgestellt werden. Die vorliegende Norm legt eine Protokollfamilie für Funkverbindungen mit niedriger Datenrate für fest installierte, tragbare und sich langsam bewegende Geräte - welche oftmals mit Einschränkungen im Hinblick auf die Stromversorgung betrieben werden - fest, die Systemmanagement, Gateway-Betrachtungen und IT-Sicherheitsspezifikationen mit einschließt. Den Anwendungsschwerpunkt bilden die Leistungsanforderungen der Überwachung der Prozessautomation und -steuerung, wobei Kommunikationslatenzzeiten zwischen Endpunkten von ungefähr 100 ms toleriert werden können.

Um den Anforderungen von Benutzern und Betreibern industrieller Funkgeräte gerecht zu werden, bietet die in diesem Dokument festgelegte Technologie Stabilität trotz Störungen, die in rauen industriellen Umgebungen vorkommen oder durch Funksysteme außerhalb des Anwendungsbereiches dieser Internationalen Norm verursacht werden. In Abschnitt 4 dieser Norm wird die Koexistenz mit anderen, in der industriellen Arbeitsumgebung vermutlich vorhandenen Funkgeräten behandelt, zu denen z. B. Mobiltelefone und Geräte auf der Grundlage von IEC 62591 (WirelessHART™¹), IEC 62601 (WIA-PA), IEEE 802.11 (WiFi), IEEE 802.15, IEEE 802.16 (WiMax) und anderen relevanten Normen gehören. Des Weiteren unterstützt diese Norm die Interoperabilität von mit dieser Internationalen Norm konformen Geräten hinsichtlich der Betriebsaspekte, die von ihr abgedeckt werden, wie in Abschnitt 5 beschrieben.

Die vorliegende Norm legt weder die Infrastruktur von Anlagen noch ihre Sicherheit oder Leistungsmerkmale fest. Es ist jedoch wichtig, dass die Sicherheit der Anlageninfrastruktur durch den Endnutzer sichergestellt wird.

0.2 Dokumentstruktur

Das vorliegende Dokument ist in Abschnitte zu einzelnen Netzfunktionen und Schichten der Protokollfamilie gegliedert. Die Abschnitte beschreiben das System, das Systemmanagement, das IT-Sicherheitsmanagement, Physical-Layer, Data-Link-Layer, Network-Layer, Transport-Layer, Application-Layer und die Bereitstellung. Weiterhin sind allgemeine Betrachtungen zu Protokoll-Gateways, jedoch keine Spezifikationen spezifischer Protokoll-Gateways enthalten. Jeder Abschnitt beschreibt eine Funktionalität oder Protokollschicht und gibt das Verhalten vor, das für den richtigen Betrieb erforderlich ist. Wenn ein Abschnitt Verhaltensweisen einer anderen Funktion oder Schicht beschreibt, ist ein Verweis auf den entsprechenden Abschnitt angegeben, um dort weitere Informationen erhalten zu können.

Die in diesem Dokument festgelegten obligatorischen und optionalen Kommunikationsprotokolle werden als „native Protokolle“ bezeichnet, während Protokolle, die von anderen Netzen verwendet werden, wie klassische Feldbus-Kommunikationsprotokolle, als „fremde Protokolle“ bezeichnet werden.

¹ Eigentum der HART Communication Foundation. Diese Information ist zum Vorteil der Anwender der Norm angegeben und stellt keine Empfehlung für den Markennameninhaber oder eines seiner Produkte dar. Für die Übereinstimmung mit diesem Profil ist die Verwendung des Markennamens nicht notwendig. Die Anwendung der Markennamen muss durch den Markennameninhaber genehmigt werden.

0.3 Potentiell relevante Patente

Die Internationale Elektrotechnische Kommission (IEC) macht auf die Tatsache aufmerksam, dass die Übereinstimmung mit diesem Dokument die Verwendung mehrerer Patente einschließen kann:

- a) hinsichtlich der (asymmetrischen) Elliptische-Kurven-Kryptografie, siehe 7.4.6 und 7.2.2.3;
- b) hinsichtlich der Synchronisierung von Uhren und der Bewertung der Verbindungszweigqualität, siehe 9.1.9.3 und 9.1.15;
- c) hinsichtlich nicht näher spezifizierter Fachgebiete;
- d) hinsichtlich der drahtlosen Bereitstellung sowie der Auswahl von und Weiterleitung zwischen mehreren Gateways.

Die IEC übernimmt keine Verantwortung in Bezug auf Richtigkeit, Gültigkeit und Anwendungsbereich der genannten Patente.

Die Inhaber der Patente haben sich gegenüber der IEC bereit erklärt, Lizenzen entweder kostenfrei oder unter angemessenen und nicht diskriminierenden Bedingungen (RAND) entsprechend den weltweiten Gepflogenheiten zu vergeben. Die entsprechenden Erklärungen wurden von den Patentinhabern bei der IEC hinterlegt.

Weitere Informationen sind unter folgenden Adressen erhältlich:

a)	Certicom Corporation 4701 Tahoe Blvd, Bldg A L4W 0B5 Mississauga, ON CANADA Betreff: Patent licensing Lizenzbedingungen: vorauss. RAND Relevante Patente: unbekannt; vom Patentinhaber nicht angegeben	b)	NIVIS LLC 1000 Circle 75 Pkwy, Suite 300 Atlanta, GA 30339-6051 USA Betreff: Patent licensing Lizenzbedingungen: RAND Relevante Patente: – US 20100027437 – US 20100098204
c)	General Electric 1 Research Cir Schenectady, NY 12309-1027 USA Betreff: Patent licensing Lizenzbedingungen: vorauss. RAND, Reziprozität Relevante Patente: unbekannt; vom Patentinhaber nicht angegeben	d)	Yokogawa Electric Corporation 2-9-32 Nakachou, Musashina-shi Tokyo JAPAN Betreff: Patent licensing Lizenzbedingungen: RAND, Reziprozität Relevante Patente: – JP 4129749 – US 8005514 – US 8031727 – US 8305927 – US 2009080394
Die oben genannten Patentinhaber, Patente und Lizenzbedingungen entsprechen den gegenüber der IEC erklärten Angaben, wie sie zum Zeitpunkt der Erarbeitung dieses Textes für IEC 62734 relevant waren.			

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

ISO (<http://www.iso.org/patents>) und IEC (<http://patents.iec.ch>) unterhalten Online-Datenbanken zu Patenten, die für ihre Normen relevant sind. Um aktuelle Informationen zu Patenten zu erhalten, werden Anwender auf diese Datenbanken verwiesen.

1 Anwendungsbereich

Die vorliegende Norm legt eine Methode für einen zuverlässigen und sicheren Funkbetrieb von Anwendungen für die unkritische Beobachtung, Alarmierung, Überwachungssteuerung sowie von Steuerungs- und Regelungsanwendungen fest. Die vorliegende Norm legt eine Protokollfamilie für Funkverbindungen mit niedriger Datenrate für fest installierte, tragbare und sich langsam bewegende Geräte – welche oftmals mit Einschränkungen im Hinblick auf die Stromversorgung betrieben werden – fest, die Systemmanagement, Gateway-Betrachtungen und IT-Sicherheitsspezifikationen mit einschließt. Den Anwendungsschwerpunkt dieser Norm bilden die Leistungsanforderungen der Überwachung der Prozessautomation und -steuerung, wobei Kommunikationsverzögerungszeiten zwischen Endpunkten von ungefähr 100 ms toleriert werden können.

Diese Norm legt Folgendes fest:

- Definition des Dienstes des Physical-Layer und Protokollspezifikation;
- Definition des Dienstes des Data-Link-Layer und Protokollspezifikation;
- Definition des Dienstes des Network-Layer und Protokollspezifikation;
- Definition des Dienstes des Transport-Layer und Protokollspezifikation;
- Definition des Dienstes des Application-Layer und Protokollspezifikation, einschließlich der Unterstützung von Protokoll-Tunneling und Gateways;
- IT-Sicherheit und IT-Sicherheitsmanagement;
- Bereitstellung und Konfiguration;
- Netzwerkmanagement; und
- zusätzliche Kommunikationsrollenprofile (d. h., es können mehrere gleichzeitig ausgewählt werden).

Die Funktionalität oberhalb der Application-Layer des OSI-Basis-Referenzmodells, wie die sogenannte „Benutzerschicht“ und verschiedene Profile für die Funktionalität auf dieser Schicht, wird nicht behandelt. Diese wird jedoch kurz in Anhang A erörtert.

3 Begriffe, Abkürzungen und Konventionen

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe, Abkürzungen und Konventionen.

3.1 Begriffe

3.1.1 (N)-Schicht und andere Begriffe aus dem Basis-Referenzmodell der Kommunikation offener Systeme

3.1.1.1

abstrakte Syntax

(en: abstract syntax)

Festlegung von (N)-PDUs durch Anwendung von Notationsregeln, die von den zu ihrer Darstellung verwendeten Codierungsverfahren unabhängig sind

[QUELLE: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 7.1.1.2, modifiziert – verallgemeinert für die N-Schicht]

3.1.1.2

Zurechenbarkeit

(en: accountability)

Eigenschaft, die gewährleistet, dass Aktionen einer Instanz auch auf diese zurückgeführt werden können

[QUELLE: ISO 7489-2:1989, 3.3.3]

3.1.1.3

Quittierung

(en: **acknowledgement**)

Funktion der (N)-Schicht, die es einer empfangenden Instanz einer (N)-Schicht ermöglicht, eine sendende Instanz einer (N)-Schicht über den Empfang einer (N)-PDU zu informieren

[QUELLE: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.8.1.16]

3.1.1.4

Anwendungsinstanz

(en: **application-entity**)

aktives Element innerhalb eines Anwendungsprozesses, welches ein bestimmtes Leistungspotential im Rahmen von OSI verkörpert, das für den AL definiert ist und einem bestimmten Anwendungsinstanztyp entspricht (ohne Verwendung zusätzlicher Leistungspotentiale)

Anmerkung 1 zum Begriff: Dabei handelt es sich um eine geringfügige Spezialisierung der (N)-Instanz, weil der AL für OSI nicht relevante Anwendungsfunktionen enthält. Jede Anwendungsinstanz stellt genau einen Prozess in der Umgebung der Kommunikation offener Systeme dar.

[QUELLE: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 7.1.1.1]

3.1.1.5

Anwendungsmanagement

(en: **application-management**)

auf das Management von OSI-Anwendungsprozessen bezogene Funktionen im AL

[QUELLE: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 8.1.1]

3.1.1.6

Assoziation

(en: **association**)

zusammenwirkende Beziehung zwischen Systeminstanzen, gewöhnlich zum Zweck der Übertragung von Informationen zwischen ihnen

[QUELLE: IEC/TC 62443-1-1:2009, 3.2.7]

3.1.1.7

(N)-Assoziation

(en: **(N)-association**)

zusammenwirkende Beziehung zwischen Aufrufen von Instanzen der (N)-Schicht

[QUELLE: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.3.1.1]

3.1.1.8

Berechtigung

(en: **authorization**)

Erteilung von Rechten, wozu auch die Gewährung des Zugriffs basierend auf Zugriffsrechten gehört

[QUELLE: ISO 7498-2:1989, 3.3.10]

3.1.1.9

Verfügbarkeit

(en: **availability**)

Eigenschaft, einer berechtigten Instanz auf Verlangen zugänglich und nutzbar zu sein

[QUELLE: ISO 7498-2:1989, 3.3.11]

3.1.1.10

Blockbildung

(en: **blocking**)

von einer (N)-Instanz ausgeführte Funktion zur Abbildung mehrerer (N)-SDUs auf eine (N)-PDU

[QUELLE: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.8.1.11]

3.1.1.11**Mehrpunktverbindung mit zentraler Steuerung****(en: centralized-multi-endpoint-connection)**

Mehrpunktverbindung, bei der Daten, die von der an den zentralen Verbindungsendpunkt angeschlossenen Instanz gesendet werden, von allen anderen Instanzen empfangen werden, während von den anderen Instanzen gesendete Daten nur von der zentralen Instanz empfangen werden

[QUELLE: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.8.1.2]

3.1.1.12**verschlüsselter Text****(en: ciphertext)**

durch Verschlüsselung erzeugte Daten, so dass der semantische Inhalt der resultierenden Daten nicht einsehbar ist

Anmerkung 1 zum Begriff: Siehe Klartext.

Anmerkung 2 zum Begriff: Bezogen auf eine PDU ist verschlüsselter Text eine Information in einer PDU, die durch Verschlüsselung verdeckt wird, in seiner verdeckten Form nach der Verschlüsselung und vor der Entschlüsselung.

[QUELLE: ISO 7489-2:1989, 3.3.1]

3.1.1.13**Klartext****(en: cleartext)**

<allgemein> allgemein verständliche Daten mit einsehbarem semantischem Inhalt

[QUELLE: ISO 7498-2:1989, 3.3.15]

3.1.1.14**Klartext****(en: cleartext)**

<kommunikationsprotokollspezifisch> Information in einer PDU, die nicht durch Verschlüsselung verdeckt wird

Anmerkung 1 zum Begriff: Bezogen auf eine PDU ist Klartext eine Information in der PDU, die nicht durch Verschlüsselung verdeckt wird und die in der PDU, wenn vorhanden, immer einsehbar ist.

3.1.1.15**Gefährdung****(en: compromise)**

Verletzung der Computersicherheit, wobei Programme oder Daten möglicherweise modifiziert, zerstört oder unberechtigten Instanzen zugänglich gemacht worden sind

[QUELLE: ISO/IEC 2382-8:1998, 08.05.11]

3.1.1.16**Verkettung****(en: concatenation)**

von einer (N)-Instanz durchgeführte Funktion zur Abbildung mehrerer (N)-PDUs auf eine (N-1)-SDU

Anmerkung 1 zum Begriff: Blockbildung und Verkettung dienen verschiedenen Zwecken, obwohl sie ähnliche Funktionen ausführen (sie ermöglichen beide die Zusammenfassung von Dateneinheiten). Verkettung ermöglicht z. B. der (N)-Schicht die Zusammenfassung einer oder mehrerer Quittierungs-(N)-PDUs mit einer (oder mehreren) (N)-PDU(s), die Benutzerdaten enthält (enthalten). Das wäre mit der Blockbildungsfunktion allein nicht möglich. Außerdem ist zu beachten, dass die beiden Funktionen so miteinander kombinierbar sind, dass die (N)-Schicht Blockbildung und Verkettung ausführt.

[QUELLE: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.8.1.13]

3.1.1.17

konkrete Syntax

(en: **concrete syntax**)

diejenigen Aspekte der bei der Spezifikation von Daten angewendeten Regeln, die eine spezifische Darstellung dieser Daten verkörpern

[QUELLE: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 7.2.1.1]

3.1.1.18

Vertraulichkeit

(en: **confidentiality**)

Eigenschaft, dass Informationen unberechtigten Personen, Instanzen oder Prozessen nicht verfügbar gemacht oder ihnen gegenüber enthüllt werden

Anmerkung 1 zum Begriff: Im allgemeinen Kontext der Informationssicherheit wahrt die Vertraulichkeit eine berechtigte Sperrung des Informationszugriffs und der Offenlegung der Information, einschließlich von Mitteln zur Wahrung der Privatsphäre und von anwendereigenen Informationen.

[QUELLE: ISO 7498-2:1989, 3.3.16]

3.1.1.19

(N)-Verbindung

(en: **(N)-connection**)

von einer Instanz der (N+1)-Schicht für die Übertragung von Daten zwischen zwei oder mehr (N+1)-Instanzen angeforderte Assoziation

Anmerkung 1 zum Begriff: Die Assoziation wird durch die (N)-Schicht aufgebaut und legt explizit eine Menge von (N)-Datenübertragungen sowie die Vereinbarung über die für diese Menge bereitzustellenden (N)-Datenübertragungsdienste an.

[QUELLE: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.3.1.2]

3.1.1.20

(N)-Verbindungsendpunkt

(en: **(N)-connection endpoint**)

Abschluss an einem Ende einer (N)-Verbindung innerhalb eines (N)-Dienstzugangspunkts

[QUELLE: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.3.1.3]

3.1.1.21

(N)-Verbindungsendpunkt-Bezeichner

(en: **(N)-connection-endpoint-identifier**)

Bezeichner eines (N)-Verbindungsendpunkts zur Bezeichnung der entsprechenden (N)-Verbindung an einem (N)-SAP

[QUELLE: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.4.1.5]

3.1.1.22

(N)-Verbindungsendpunkt-Suffix

(en: **(N)-connection-endpoint-suffix**)

Teil eines (N)-Verbindungsendpunkt-Bezeichners, der im Bereich eines (N)-SAP eindeutig ist

[QUELLE: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.4.1.6]

3.1.1.23

(N)-verbindungsorientierte Übertragung

(en: **(N)-connection-mode-transmission**)

(N)-Datenübertragung im Kontext einer (N)-Verbindung

[QUELLE: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.3.1.17]

3.1.1.24**(N)-verbindungslose Übertragung****(en: (N)-connectionless-mode-transmission)**

(N)-Datenübertragung, die nicht im Kontext einer (N)-Verbindung stattfindet und die nicht erforderlich ist, um eine logische Beziehung zwischen (N)-SDUs aufrechtzuerhalten

[QUELLE: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.3.1.18]

3.1.1.25**korrespondierende (N)-Instanzen****(en: correspondent-(N)-entities)**

(N)-Instanzen, die über eine (N-1)-Verbindung verbunden sind

[QUELLE: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.3.1.5]

3.1.1.26**Kryptoanalyse****(en: cryptanalysis)**

Analyse eines kryptografischen Systems und/oder von dessen Ein- und Ausgabewerten zur Ableitung vertraulicher Variablen und/oder sensibler Daten, einschließlich von Klartext

[QUELLE: ISO 7498-2:1989, 3.3.18]

3.1.1.27**Datenintegrität****(en: data integrity)**

Eigenschaft, dass Daten nicht unberechtigt geändert oder zerstört worden sind

[QUELLE: ISO 7498-2:1989, 3.3.21]

3.1.1.28**Authentifizierung des Datenursprungs****(en: data-origin authentication)**

Bestätigung, dass die Quelle der empfangenen Daten die geforderte Quelle ist

[QUELLE: ISO 7498-2:1989, 3.3.22]

3.1.1.29**(N)-Datenübertragung****(en: (N)-data transmission)**

(N)-Teildienst, der SDUs von einer Instanz einer (N+1)-Schicht zu einer oder mehreren (N+1)-Instanzen übermittelt

[QUELLE: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.3.1.9]

3.1.1.30**Aufheben der Blockbildung****(en: deblocking)**

von einer (N)-Instanz ausgeführte Funktion zur Identifikation mehrerer (N)-SDUs, die in einer (N)-PDU enthalten sind

Anmerkung 1 zum Begriff: Wenn kein Fehler vorliegt, ist das Aufheben der Blockbildung die Umkehrfunktion der Blockbildung.

[QUELLE: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.8.1.12]

3.1.1.31**Mehrpunktverbindung ohne zentrale Steuerung****(en: decentralized-multi-endpoint-connection)**

Mehrpunktverbindung, bei der Daten, die von einer an einen Verbindungsendpunkt angeschlossenen Instanz gesendet werden, von allen anderen Instanzen empfangen werden

[QUELLE: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.8.1.3]

3.1.1.32

Entschlüsselung

(en: **decryption**)

Umkehrung einer entsprechenden umkehrbaren Verschlüsselung

[QUELLE: ISO 7498-2:1989, 3.3.23]

3.1.1.33

Demultiplexen

(en: **demultiplexing**)

von einer (N)-Instanz ausgeführte Funktion, die (N)-PDUs für mehr als eine (N)-Verbindung innerhalb einer (N-1)-Verbindung identifiziert

Anmerkung 1 zum Begriff: Wenn kein Fehler vorliegt, ist das Demultiplexen die Umkehrfunktion des Multiplexens.

[QUELLE: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.8.1.5]

3.1.1.34

digitale Signatur

(en: **digital signature**)

an eine Dateneinheit angefügte Daten oder eine kryptografische Transformation einer Dateneinheit, mit der ein Empfänger der Dateneinheit die Möglichkeit der Überprüfung der Quelle und Integrität der Dateneinheit erhält und die einen Schutz gegen Fälschung z. B durch den Empfänger bietet

[QUELLE: ISO 7498-2:1989, 3.3.26]

3.1.1.35

(N)-Instanz

(en: **(N)-entity**)

aktives Element innerhalb eines (N)-Teilsystems, welches ein bestimmtes Leistungspotential verkörpert, das für die (N)-Schicht definiert ist und einem bestimmten (N)-Instanztyp entspricht (ohne Verwendung zusätzlicher Leistungspotentiale)

[QUELLE: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.2.1.11]

3.1.1.36

(N)-Instanzaufruf

(en: **(N)-entity-invocation**)

spezielle Nutzung eines Teils oder des gesamten Leistungspotentials einer gegebenen (N)-Instanz (ohne Verwendung zusätzlicher Leistungspotentiale)

[QUELLE: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.2.1.12]

3.1.1.37

(N)-Instanztyp

(en: **(N)-entity-type**)

Beschreibung einer Klasse von (N)-Instanzen in Form der für die (N)-Schicht definierten Leistungspotentiale

[QUELLE: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.2.1.10]

3.1.1.38

(N)-Schnittstellen-Steuerinformationen

(en: **(N)-interface-control-information**)

zwischen einer (N+1)-Instanz und einer (N)-Instanz lokal ausgetauschte Informationen zur Koordinierung ihres gemeinsamen Betriebs

3.1.1.39

(N)-Schicht

(en: **(N)-layer**)

Unterteilung der OSI-Architektur, die aus Teilsystemen desselben Ranges (N) gebildet wird

[QUELLE: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.2.1.2]

3.1.1.40**(N)-Schicht-Management****(en: (N)-layer-management)**

auf das Management der (N)-Schicht bezogene Funktionen, die teilweise in der (N)-Schicht selbst gemäß dem (N)-Protokoll der Schicht (Aktivitäten wie Aktivierung und Übertragungssicherung) und teilweise als Teilmenge des Systemmanagements ausgeführt werden

[QUELLE: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 8.1.6]

3.1.1.41**Mehrpunktverbindung****(en: multi-endpoint-connection)**

Verbindung mit mehr als zwei Verbindungsendpunkten

[QUELLE: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.3.1.4]

3.1.1.42**Multiplexen****(en: multiplexing)**

von einer (N)-Instanz ausgeführte Funktion, bei der eine (N-1)-Verbindung zur Unterstützung von mehreren (N)-Verbindungen benutzt wird

Anmerkung 1 zum Begriff: Die Benennung „Multiplexen“ wird im engeren Sinn auch für die Funktion benutzt, die von der sendenden (N)-Instanz ausgeführt wird, während die Benennung „Demultiplexen“ für die Funktion benutzt wird, die von der empfangenden (N)-Instanz ausgeführt wird.

[QUELLE: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.8.1.4]

3.1.1.43**Password****(en: password)**

vertrauenswürdige Authentifizierungsinformation, die in der Regel aus einer Zeichenfolge besteht

[QUELLE: ISO 7498-2:1989, 3.3.39]

3.1.1.44**Partner-(N)-Instanzen****(en: peer-(N)-entities)**

Instanzen innerhalb derselben (N)-Schicht

[QUELLE: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.2.1.3]

3.1.1.45**Authentifizierung der Partnerinstanz****(en: peer-entity authentication)**

Bestätigung, dass eine Partnerinstanz in einer Assoziation die geforderte Assoziation ist

[QUELLE: ISO 7498-2:1989, 3.3.40]

3.1.1.46**(N)-Protokoll****(en: (N)-protocol)**

Menge von Regeln und Formaten (Semantik und Syntax), die das Kommunikationsverhalten von (N)-Instanzen bei der Ausführung von (N)-Funktionen bestimmen

[QUELLE: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.2.1.9]

3.1.1.47**Adressierungsinformation des (N)-Protokolls****(en: (N)-protocol-addressing-information)**

diejenigen Elemente der (N)-PCI mit der Adressierungsinformation

[QUELLE: ISO/IEC 7498-3:1997, 3.4.20]

3.1.1.48

Steuerinformation des (N)-Protokolls

(en: (N)-protocol-control-information)

zwischen (N)-Instanzen ausgetauschte Informationen zur Koordinierung ihres gemeinsamen Betriebs

[QUELLE: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.6.1.1]

3.1.1.49

(N)-Protokolldateneinheit

(en: (N)-protocol-data-unit)

in einem (N)-Protokoll festgelegte Dateneinheit, die aus der Steuerinformation des (N)-Protokolls und möglichen (N)-Benutzerdaten besteht

[QUELLE: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.6.1.3]

3.1.1.50

Versionsbezeichner des (N)-Protokolls

(en: (N)-protocol-version-identifier)

zwischen korrespondierenden (N)-Instanzen übermittelter Bezeichner, der die Auswahl der Version eines (N)-Protokolls ermöglicht

Anmerkung 1 zum Begriff: Die Festlegung eines neuen Versionsbezeichners eines N-Protokolls setzt ein minimales allgemeines Wissen über das N-Protokoll voraus, das durch den vorhergehenden Versionsbezeichner gekennzeichnet war. Kann ein solches minimales allgemeines Wissen nicht erreicht werden, sind die N-Protokolle als unabhängig voneinander und verschieden zu betrachten.

[QUELLE: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.8.1.18]

3.1.1.51

Dienstgüte

(en: quality of service)

<allgemein> Gesamtheit der Merkmale einer einem Benutzer gebotenen Dienstleistung, die dessen Zufriedenheit mit dieser Dienstleistung bestimmt

Anmerkung 1 zum Begriff: Die Dienstgüte ist durch das Zusammenwirken der Dienstbereitschaft, der Dienstanwendbarkeit, der Dienstverfügbarkeit, der Dienstintegrität und anderer diensteigener Einflüsse gekennzeichnet.

Anmerkung 2 zum Begriff: ISO definiert „Qualität“ als Fähigkeit eines Produkts oder einer Dienstleistung, den Bedarf eines Benutzers zu befriedigen.

[QUELLE: IEC 61907:2009, 3.1.15]

3.1.1.52

Dienstgüte

(en: quality of service)

<Datensicherungsdienst> für eine Verbindungsstrecke vereinbarte Parameter, einschließlich

- Priorität;
- Zeitfenster für Steuernachrichten;
- Zulässigkeit einer Nachrichtenzustellung außerhalb der Reihenfolge; und
- Zulässigkeit einer Nachrichtenzustellung in Teilschritten

3.1.1.53

Vereinigen

(en: reassembling)

von einer (N)-Instanz durchgeführte Funktion zur Abbildung mehrerer (N)-PDUs auf eine (N)-SDU

Anmerkung 1 zum Begriff: Wenn kein Fehler vorliegt, ist das Vereinigen die Umkehrfunktion des Segmentierens.

[QUELLE: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.8.1.10]

3.1.1.54**Rekombination****(en: recombining)**

von einer (N)-Instanz ausgeführte Funktion, die (N)-PDUs für eine einzelne (N)-Verbindung in (N-1)-SDUs identifiziert, die auf mehr als einer (N-1)-Verbindung empfangen werden

Anmerkung 1 zum Begriff: Wenn kein Fehler vorliegt, ist die Rekombination die Umkehrfunktion des Aufteilens.

[QUELLE: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.8.1.7]

3.1.1.55**(N)-Weiterleitung****(en: (N)-relay)**

(N)-Funktion, mit der eine (N)-Instanz von einer Partner-(N)-Instanz erhaltene Daten zu einer anderen Partner-(N)-Instanz weiterleitet

[QUELLE: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.3.1.6]

3.1.1.56**Rücksetzen****(en: reset)**

Funktion, die die entsprechenden (N)-Instanzen auf einen vordefinierten Zustand zurücksetzt, wobei ein Datenverlust oder eine Vervielfältigung von Daten möglich ist

[QUELLE: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.8.1.17]

3.1.1.57**Sicherheitskennzeichen****(en: security label)**

an eine Ressource (die eine Dateneinheit sein kann) gebundene Markierung, die die Sicherheitsattribute dieser Ressource benennt oder bezeichnet

[QUELLE: ISO 7498-2:1989, 3.3.49]

3.1.1.58**Segmentieren****(en: segmenting)**

von einer (N)-Instanz ausgeführte Funktion zur Abbildung einer (N)-SDU auf mehrere (N)-PDUs

[QUELLE: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.8.1.9]

3.1.1.59**(N)-Wähler****(en: (N)-selector)**

der Teil einer (N)-Adresse, der speziell zum adressierten (N)-Teilsystem gehört, d. h., der einen oder mehrere (N)-SAPs innerhalb eines OSI-Endsystems bezeichnet, sobald dieses OSI-Endsystem eindeutig adressiert ist

Anmerkung 1 zum Begriff: Da das OSI-Endsystem im Network-Layer implizit bekannt ist, werden oberhalb der Netzwerkschicht N-Wähler zusammen mit lokalen Informationen zur Adressierung der geforderten (N+1)-Instanz innerhalb des offenen Systems benutzt. N-Wählerwerte werden zwischen offenen Systemen als Teil der (N)-PAI ausgetauscht.

[QUELLE: ISO/IEC 7498-3:1997, 6.2.3]

3.1.1.60**Trennung****(en: separation)**

von einer (N)-Instanz ausgeführte Funktion zur Identifikation mehrerer (N)-PDUs, die in einer (N)-SDU enthalten sind

Anmerkung 1 zum Begriff: Wenn kein Fehler vorliegt, ist die Trennung die Umkehrfunktion der Verkettung.

[QUELLE: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.8.1.14]

3.1.1.61

Sequenzierung

(en: sequencing)

von der (N)-Schicht ausgeführte Funktion zur Wahrung der Reihenfolge der (N)-SDUs, die der (N)-Schicht übergeben wurden

[QUELLE: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.8.1.15]

3.1.1.62

(N)-Dienst

(en: (N)-service)

Leistungspotential der (N)-Schicht und der darunter liegenden Schichten, das für die (N+1)-Instanzen an der Grenze zwischen der (N)-Schicht und der (N+1)-Schicht bereitgestellt wird

[QUELLE: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.2.1.5]

3.1.1.63

(N)-Dienstzugangspunkt

(en: (N)-service access point)

Punkt, an dem einer Instanz der (N+1)-Schicht (N)-Dienste von einer Instanz der (N)-Schicht bereitgestellt werden

[QUELLE: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.2.1.8]

3.1.1.64

Adresse des (N)-Dienstzugangspunkts

(en: (N)-service-access-point-address)

(N)-Adresse zur Identifikation eines einzelnen (N)-SAP

[QUELLE: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.4.1.2]

3.1.1.65

(N)-Dienst-Dateneinheit

(en: (N)-service-data-unit)

Informationsmenge, deren Identität bei einer Übertragung zwischen Partner-(N+1)-Instanzen gewahrt bleibt und die von den unterstützenden (N)-Instanzen nicht interpretiert wird

[QUELLE: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.6.1.4]

3.1.1.66

Aufteilung

(en: splitting)

Funktion innerhalb der (N)-Schicht, mit der eine (N)-Verbindung durch mehrere (N-1)-Verbindungen unterstützt wird

Anmerkung 1 zum Begriff: Die Benennung „Aufteilung“ wird im engeren Sinn auch für die Funktion benutzt, die von der sendenden (N)-Instanz ausgeführt wird, während die Benennung „Rekombination“ für die Funktion benutzt wird, die von der empfangenden (N)-Instanz ausgeführt wird.

[QUELLE: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.8.1.6]

3.1.1.67

Systemverwaltung

(en: system management)

auf das Management verschiedener OSI-Ressourcen und deren Status über alle Schichten der OSI-Architektur hinweg bezogene Funktionen im AL

[QUELLE: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 8.1.4]

3.1.1.68**Transfersyntax****(en: transfer syntax)**

abstrakte und konkrete Syntax, die für die Übertragung von Daten zwischen offenen Systemen verwendet wird

[QUELLE: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 7.2.1.2]

3.1.1.69**Benutzeranwendungsprozess****(en: user application process)**

aktiver Prozess innerhalb des obersten Teilbereichs des AL, d. h. beim Benutzer der OSI-Dienste

Anmerkung 1 zum Begriff: Die Aspekte eines UAP, die für die Zwecke von OSI berücksichtigt werden müssen, werden von einer oder mehreren Anwendungsinstanzen eines oder mehrerer Anwendungstypen dargestellt, die in ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 7.1.2.2 und 7.1.2.3, definiert sind.

Anmerkung 2 zum Begriff: Die Sammlung von UAPs wird mitunter als „Benutzerschicht“ bezeichnet, auch wenn ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 7.1.2.1, angibt, dass die AL keine Grenze zu einer höheren Schicht besitzt. Im OSI-Basis-Referenzmodell umfasst die AL die UAPs.

3.1.1.70**(N)-Benutzerdaten****(en: (N)-user-data)**

im Auftrag der (N+1)-Instanzen, für die die (N)-Instanzen Dienste bereitstellen, zwischen (N)-Instanzen übertragene Daten

[QUELLE: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.6.1.2]

3.1.2 Weitere Begriffe

ANMERKUNG Quellen von Definitionen ohne Verweisung in der vorliegenden Norm können den Literaturhinweisen entnommen werden.

3.1.2.1**Zugriffssteuerung****(en: access control)**

Sicherstellung, dass der Zugriff auf Werte autorisiert und eingeschränkt nach den Unternehmens- und Sicherheitsanforderungen erfolgt

[QUELLE: ISO/IEC 27000:2014, 2.1]

3.1.2.2**Adapter****(en: adapter)**

Spezialisierung eines Geräts, das das Protokoll in dem (den) angeschlossenen veralteten Gerät(en) intern in das eines dieser Norm entsprechenden Netzgerätes umwandelt

3.1.2.3**Alarm****(en: alarm)**

Bedingung, deren Zustand beibehalten wird, bis die Bedingung nach einer gemeldeten Zustandsänderung beseitigt ist

BEISPIEL: Das Auftreten einer Alarmbedingung oder einer Rückkehrbedingung zum Normalbetrieb, die für einen entsprechenden UAP von möglicher Bedeutung ist.

3.1.2.4**Warnung****(en: alert)**

Meldung einer Ereignisbedingung oder einer Alarmbedingung

3.1.2.5

Endanwendung

(en: end application)

Anwendung

(en: application)

System oder Problem, für das ein Computer angewendet wird

3.1.2.6

Anwendungsprogramm

(en: application program)

Anwendung

(en: application)

Programm, welches die Funktionen für Endbenutzer zur Verfügung stellt

3.1.2.7

Application-Layer

(en: application layer)

Anwendung

(en: application)

oberste Protokollschicht im ISO/IEC-Basis-Referenzmodell, in der Arten der Anwendung nach Kritikalität klassifiziert werden

3.1.2.8

Anwendungsprozess

(en: application process)

Element, welches die Informationsverarbeitung für eine bestimmte Anwendung ausführt

3.1.2.9

asymmetrischer Verschlüsselungsalgorithmus

(en: asymmetric-key algorithm)

asymmetrischer kryptografischer Algorithmus

(en: asymmetric-key cryptographic algorithm)

kryptografischer Algorithmus mit einem öffentlichen Schlüssel

(en: public key cryptographic algorithm)

<Informationssicherheit> Algorithmus für die Verschlüsselung oder die entsprechende Entschlüsselung, bei dem sich die für die Ver- und Entschlüsselung verwendeten Schlüssel unterscheiden

[QUELLE: ISO/IEC 10181-1:1996, 3.3.1]

3.1.2.10

Authentifizierung

(en: authentication)

<Informationssicherheit> Nachweis der Identität eines Benutzers, eines Prozesses oder eines Geräts, häufig als Vorbedingung, um den Zugriff auf Ressourcen in einem Informationssystem zuzulassen

Anmerkung 1 zum Begriff: Siehe „Authentifizierung des Datenursprungs“ (3.1.1.28) und/oder „Authentifizierung der Partnerinstanz“ (3.1.1.45).

3.1.2.11

Authentifizierungscode

(en: authentication code)

<Informationssicherheit> vollständige oder abgeschnittene kryptografische Prüfsumme, die auf einer geeigneten Sicherheitsfunktion beruht

Anmerkung 1 zum Begriff: Siehe 3.1.2.97.

Anmerkung 2 zum Begriff: Der Authentifizierungscode wird auch als „Nachrichtenauthentifizierungscode (MAC)“ bezeichnet. Wird er in einem Kontext benutzt, in dem das Akronym „MAC“ anders definiert ist, wie in Normen über lokale Netzwerke, wird er als „Nachrichtenintegritätscode (MIC)“ bezeichnet.

[QUELLE: ISO/IEC 19790:2012, 3.8, modifiziert durch den Vorsatz „vollständig oder abgeschnitten“]

3.1.2.12**Backbone-Netzwerk****(en: backbone network)****Backbone-Subnetz****(en: backbone subnet)**

in der vorliegenden Norm nicht festgelegtes Netzwerk – im Allgemeinen mit der Netzwerktechnologie „IPv6“ oder „IPv4“ – für das Routing zwischen dem drahtlosen Netzwerk des Industriesensors (und -aktors) (WISN) nach dieser Norm und

- a) verbundenen Back-End-Geräten, die teilweise in dieser Norm festgelegt sind, wie Systemmanager, IT-Sicherheitsmanager und Protokoll-Gateways;
- b) Geräten, die die drahtlose TL, AL und die Managementprotokolle dieser Norm in natürlicher Form unterstützen; und
- c) anderen Backbone-Routern in demselben Backbone-Subnetz

3.1.2.13**Backbone-Router****(en: backbone router)**

Router für die Übermittlung zwischen dem drahtlosen Netzwerk dieser Norm und einem Hochgeschwindigkeits-Backbone-Netzwerk

3.1.2.14**Datensicherung****(en: backup)**

Prozedur, Verfahren oder Hardware zur Wiederherstellung verlorener oder zerstörter Daten oder zur Aufrechterhaltung des Systembetriebs

[QUELLE: ISO 2382-12:1988, 12.01.17]

3.1.2.15**Bandbreite****(en: bandwidth)**

<analoger Bereich> numerische Differenz zwischen der oberen und der unteren Frequenz eines Frequenzbereichs

Anmerkung 1 zum Begriff: Die analoge Bandbreite wird in Hz ausgedrückt.

3.1.2.16**Bandbreite****(en: bandwidth)**

<digitaler Bereich> Datenmenge, die innerhalb eines gegebenen Zeitraums einen Kommunikationskanal durchlaufen kann

Anmerkung 1 zum Begriff: Die digitale Bandbreite wird in bit/s ausgedrückt.

3.1.2.17**Black Channel****(en: black channel)**

Kommunikationskanal eines Sicherheitssystems ohne Sicherheitsfunktionen zusätzlich zur grundlegenden Kommunikationsfähigkeit

3.1.2.18**Blacklist****(en: blacklist)**

Liste von HF-Kanälen, über die die Übertragung verboten ist

Anmerkung 1 zum Begriff: Eine Blacklist gilt zeitweilig oder dauerhaft, lokal oder netzwerkweit.

3.1.2.19

Blockverschlüsselung

(en: **block cipher**)

<Informationssicherheit> kryptografisches Element, das mit einem symmetrischen Schlüssel eine schlüsselabhängige pseudozufällige Permutation einer Bitfolge fester Größe erzeugt

3.1.2.20

Sammelaufruf

(en: **broadcast**)

für alle Knoten vorgesehene Übertragung

Anmerkung 1 zum Begriff: Der Empfang eines Sammelaufrufs ist häufig auf bestimmte Schichten beschränkt, z. B. MAC- oder Network-Layer.

Anmerkung 2 zum Begriff: Viele Protokolle unterer Schichten geben keine Quittierung für Sammelaufrufe.

3.1.2.21

kanonische Transfersyntax

(en: **canonical transfer syntax**)

vollständige Transfersyntax

(en: **full transfer syntax**)

vollständige Codierung eines Objekts für eine Übertragung zwischen Geräten vor der Komprimierung

3.1.2.22

Verschlüsseln

(en: **cipher**)

<Informationssicherheit> kryptografisches Verfahren für den Schutz der Vertraulichkeit von Daten, bestehend aus drei Komponenten: einem Verschlüsselungsalgorithmus, einem Entschlüsselungsalgorithmus und einem Verfahren zur Erzeugung von Schlüsseln

[QUELLE: wird in anderen ISO/IEC-Normen auf eine unbekannte Ausgabe von ISO/IEC 18033-1 zurückgeführt, modifiziert – für eine bessere Lesbarkeit abgestimmt]

3.1.2.23

Koexistenz

(en: **coexistence**)

Fähigkeit mehrerer Systeme, ihre Aufgaben in einer vorgegebenen Umgebung auszuführen, wobei sie nach ähnlichen Regeln handeln können oder nicht

3.1.2.24

komprimierte Transfersyntax

(en: **compressed transfer syntax**)

Codierung eines Objekts für eine Übertragung zwischen Geräten nach der Komprimierung

3.1.2.25

Kommunikationslatenzzeit

(en: **communications latency**)

Verzögerungszeit zwischen einem initialen Kommunikationsereignis, wie der Ausgabe einer Übertragungsanforderung, und einem zugehörigen nachfolgenden Kommunikationsereignis, wie der Zustellung einer Nachricht bei einem vorgesehenen Empfänger

3.1.2.26

Kommunikationszuverlässigkeit

(en: **communications reliability**)

Umfang, in dem Nachrichten ihr Endziel vollständig und unbeschädigt sowie innerhalb einer angemessenen Latenzzeit erreichen

3.1.2.27

Kommunikationsdurchsatz

(en: **communications throughput**)

Kapazität eines Kommunikationskanals, üblicherweise gemessen in Nachrichten/s oder Oktetten/s

3.1.2.28**Konstruktionsoption****(en: construction option)**

Menge von Leistungsmerkmalen, die ein Entwickler in ein Gerät aufnehmen oder daraus ausschließen kann

3.1.2.29**Vertrag****(en: contract)**

Vereinbarung zwischen dem Systemmanager und einem Gerät im Netzwerk, die die Zuweisung von Netzwerkressourcen durch den Systemmanager umfasst, um einen bestimmten Kommunikationsbedarf dieses Geräts zu unterstützen

3.1.2.30**kryptografischer Algorithmus****(en: cryptographic algorithm)**

<Informationssicherheit> Algorithmus auf der wissenschaftlichen Grundlage der Kryptografie, einschließlich Verschlüsselungsalgorithmen, kryptografischen Hash-Algorithmen, digitalen Signaturalgorithmen und Schlüsselvereinbarungsalgorithmen

Anmerkung 1 zum Begriff: Beispiele für kryptografische Algorithmen sind Block- und Bitstromverschlüsselung und verschlüsselte Hash-Funktionen. Eine unverschlüsselte Hash-Funktion ist formal kein kryptografischer Algorithmus, obwohl es sich oft um eine Einwegfunktion mit einer ähnlichen Beständigkeit gegen Angriffe handelt und sie mit einem kryptografischen Algorithmus mit einem festen Schlüssel erzeugt wird. Die SHA-Familie der Hash-Funktionen ist so aufgebaut.

[QUELLE: IEC TS 62443-1-1:2009, 3.2.34, modifiziert – Anmerkung hinzugefügt]

3.1.2.31**kryptografischer Schlüssel****(en: cryptographic key)****Schlüssel****(en: key)**

<Informationssicherheit> mathematischer Wert, der

- a) in einem Algorithmus zur Erzeugung von verschlüsseltem Text aus Klartext oder umgekehrt, und
- b) zur Festlegung des Ablaufs einer kryptografischen Funktion (z. B. die synchronisierte Erzeugung des Schlüsselmaterials) oder zur Berechnung oder Validierung einer digitalen Signatur benutzt wird

[QUELLE: ISO/TS 62351-2:2008, 2.2.64]

3.1.2.32**kryptografische Schlüsselkomponente****(en: cryptographic key component)****Schlüsselkomponente****(en: key component)**

<Informationssicherheit> in einer Sicherheitsfunktion benutzte(r) Parameter zur Ausführung einer kryptografischen Funktion

[QUELLE: ISO/IEC 19790:2012, 3.24]

3.1.2.33**kryptografisches Modul****(en: cryptographic module)**

<Informationssicherheit> in der kryptografischen Umgebung enthaltene Hardware, Software und/oder Firmware zur Umsetzung geeigneter Sicherheitsfunktionen

[QUELLE: ISO/IEC 19790:2012, 3.25]

3.1.2.34

Kryptoperiode

(en: cryptoperiod)

<Informationssicherheit> Zeitspanne, für die die Anwendung eines spezifischen Schlüssels zugelassen ist oder in der die Schlüssel für ein gegebenes System oder eine gegebene Anwendung wirksam bleiben

[QUELLE: ISO/IEC 11568-4:2007, 3.9]

3.1.2.35

Datenauthentizität

(en: data authenticity)

<Informationssicherheit> Gewissheit über die Informationsquelle

[QUELLE: IEEE 802-15-4:2011, 3.1]

3.1.2.36

Datenschlüssel

(en: data key)

Datenauthentifizierungsschlüssel

(en: data authenticating key)

kryptografischer Datenschlüssel

(en: data encrypting key)

<Informationssicherheit> kryptografischer Schlüssel für die Verschlüsselung, Entschlüsselung oder Authentifizierung von Daten

[QUELLE: ISO/IEC 11568-2:2012, 3.5]

3.1.2.37

Implementierungsoption

(en: deployment option)

Menge von Leistungsmerkmalen, die ein Geräteentwickler in ein Gerät aufnimmt, über deren Nutzung der Endbenutzer oder dessen Vertreter (z. B. der Netzwerksicherheitsmanager) jedoch entscheiden kann

3.1.2.38

abgeleiteter Schlüssel

(en: derived key)

<Informationssicherheit> symmetrischer Schlüssel, der aus einem vorherigen symmetrischen Schlüssel abgeleitet wird

Anmerkung 1 zum Begriff: Solche Schlüssel dienen der Begrenzung der Kryptoperiode eines einzelnen Schlüssels, während die Anforderungen des Schlüsselarchivs erfüllt werden, sofern der unabhängige Schlüssel, von dem der abgeleitete Schlüssel abgeleitet wurde (eventuell über viele Erzeugungen von Ableitungen), vorher diese Archivanforderungen erfüllt hat.

3.1.2.39

Schlüsselzerstörung

(en: key destruction)

Zerstörung

(en: destruction)

<Informationssicherheit> vollständige Löschung oder physische Zerstörung des Schlüsselmaterials, so dass es nicht wiederhergestellt werden kann

3.1.2.40

deterministischer Zufallsbitgenerator

(en: deterministic random bit generator)

<Informationssicherheit> Prozess zur Erzeugung einer nicht vorhersagbaren Bitserie, die in dem Sinne zufällig ist, dass der Ausgabewert des Generators auf keine Weise beschrieben werden kann; der Prozess ist wirksamer als die einfache Auflistung der gesamten Zeichenfolge der Ausgabewerte

Anmerkung 1 zum Begriff: Deterministische Zufallsbitgeneratoren besitzen nachweisbare Vorteile. Die Nichtvorhersagbarkeit ihrer Ausgabewerte hängt von der Nichtvorhersagbarkeit ihres Startwerts ab und bei Hybridgeneratoren von der Rate, mit der neue nichtvorhersagbare Eingabewerte (mit hoher Entropie) bezogen auf die Anzahl der erzeugten

Ausgabebits eingegeben werden. Die gemeinsamen Quellen dieser Nichtvorhersagbarkeit können der Anmerkung in 3.1.2.102, „nicht deterministischer Zufallsbitgenerator“, entnommen werden.

3.1.2.41

Gerätesicherheits-Managementobjekt

(en: device security management object)

Anwendungssoftware innerhalb eines Geräts, die als lokaler Partner eines Sicherheitsmanagers wirkt

3.1.2.42

Duocast

(en: duocast)

Variante des Einzelaufrufs, bei der ein zweiter Empfänger so zeitgesteuert wird, dass er die DPDU mithört und innerhalb einer einzelnen D-Transaktion eine zweite Quittierung liefert

Anmerkung 1 zum Begriff: Duocast ist in Bild 84 grafisch dargestellt.

3.1.2.43

verschlüsselter Schlüssel

(en: encrypted key)

<Informationssicherheit> kryptografischer Schlüssel, der mit einer zugelassenen Sicherheitsfunktion mit einem Schlüssel zur Schlüsselverschlüsselung (KEK) verschlüsselt wurde

Anmerkung 1 zum Begriff: Mit diesem Vorgang wird der Wert des zugrunde liegenden Klartextschlüssels verdeckt.

[QUELLE: ISO/IEC 19790:2012, 3.36]

3.1.2.44

Verschlüsselung

(en: encryption)

<Informationssicherheit> umkehrbare Operation, bei dem Daten durch einen kryptografischen Algorithmus in verschlüsselten Text umgewandelt werden, so dass der Informationsinhalt der Daten verdeckt wird

[QUELLE: ISO/IEC 9798-1:2010, 3.13]

3.1.2.45

Instanz

(en: entity)

Person, Organisation, Gerät oder Prozess

3.1.2.46

flüchtiger Schlüssel

(en: ephemeral key)

<Informationssicherheit> kryptografischer Schlüssel, der für jede Ausführung eines Schlüsseleinführungsprozesses erzeugt wird und der andere Anforderungen des Schlüsseltyps erfüllt (z. B. für jeden Nachrichtenaustausch oder jede Sitzung eindeutig zu sein)

Anmerkung 1 zum Begriff: In bestimmten Fällen werden flüchtige Schlüssel innerhalb einer einzigen Sitzung mehr als einmal benutzt (z. B. bei Sammelaufrufen), wobei der Absender nur ein flüchtiges Schlüsselpaar je Nachricht erzeugt und der private Schlüssel (dieses Paares) mit dem öffentlichen Schlüssel jedes Empfängers gesondert kombiniert wird.

3.1.2.47

Ereignis

(en: event)

vorübergehende (d. h. zustandslose) Bedingung, mit der gemeldet wird, wenn etwas geschehen ist

BEISPIELE sind das Auftreten einer Alarmbedingung oder einer Rückkehrbedingung zum Normalbetrieb, die für einen entsprechenden UAP von möglicher Bedeutung ist.

3.1.2.48

Feldgerät

(en: field device)

technisches Gerät, das so konstruiert ist, dass es dem Anlagenbetrieb standhält, und das über DPDU's und Protokolle höherer Schichten in Übereinstimmung mit der vorliegenden Norm kommuniziert

Anmerkung 1 zum Begriff: Feldgeräte schließen Router, Sensoren und Aktoren ein.

3.1.2.49

Feldnetzwerk

(en: field network)

Aufbau aus zwei oder mehr Feldgeräten, die mit dem in der vorliegenden Norm definierten drahtlosen Protokoll verbunden sind

3.1.2.50

Feld-Router

(en: field router)

Router innerhalb eines Feldnetzwerks, der gleichzeitig ein Feldgerät darstellt (d. h. kein Backbone-Router)

3.1.2.51

Kommunikation durch Anwendung eines Fremdprotokolls

(en: foreign protocol application communication)

optimierte Übermittlung von PDUs oder Teilen von PDUs von einem ersten Protokoll innerhalb eines zweiten Protokolls durch selektiven Gebrauch von Caching, Komprimierung, Adressenumwandlung und Proxy-Verfahren

3.1.2.52

fragmentieren

(en: fragment)

segmentieren

(en: segment)

(Verb) in angrenzende einzelne Teile zerlegen oder aufteilen

Anmerkung 1 zum Begriff: „Fragment“ und „Fragmentierung“ sind von IETF in Internetprotokollspezifikationen benutzte Benennungen zur Beschreibung der OSI-Konzepte „Segment“ und „Segmentierung“. In der vorliegenden Norm werden die Benennungen „Fragment“ und „Segment“ im Grunde synonym benutzt, wobei „Fragment“ in der Regel im Network-Layer und mitunter in anderen Protokollschichten benutzt wird, während „Segment“ üblicherweise im Application-Layer und manchmal in anderen Protokollschichten verwendet wird.

3.1.2.53

Fragment

(en: fragment)

Segment

(en: segment)

eine der N-Protokolldateneinheiten, die aufgrund der Segmentierung entstanden sind

Anmerkung 1 zum Begriff: „Fragment“ und „Fragmentierung“ sind von IETF in Internetprotokollspezifikationen benutzte Benennungen zur Beschreibung der OSI-Konzepte „Segment“ und „Segmentierung“. In der vorliegenden Norm werden die Benennungen „Fragment“ und „Segment“ im Grunde synonym benutzt, wobei „Fragment“ in der Regel im Network-Layer und mitunter in anderen Protokollschichten benutzt wird, während „Segment“ üblicherweise im Application-Layer und manchmal in anderen Protokollschichten verwendet wird.

3.1.2.54

Gateway

(en: gateway)

Funktion (eines Geräts), die als Protokollübersetzer zwischen einer AE entsprechend der vorliegenden Norm und anderen, verschiedenartigen AEs wirkt

3.1.2.55**Hash-basierter Nachrichtenauthentifizierungscode****(en: hash-based message authentication code)**

<Informationssicherheit> Nachrichtenauthentifizierungscode, der eine geeignete verschlüsselte Hash-Funktion benutzt

Anmerkung 1 zum Begriff: Diese Definition wurde aus der zweiten Ausführung von ISO/IEC 9797-2 verallgemeinert, die sich auf die HMAC-Konstruktion bezieht, welche auch in FIPS 198 [USA] festgelegt ist.

[QUELLE: ISO/IEC 9797-2:2011, modifiziert – verallgemeinert]

3.1.2.56**Hash-Funktion****(en: hash function)**

<Informationssicherheit> Funktion zur Abbildung von Bitfolgen auf Bitfolgen fester Länge, die die folgenden zwei Eigenschaften erfüllen: für einen gegebenen Ausgabewert ist es mathematisch unmöglich, auf dessen ursprünglichen Eingabewert zurückzuschließen; für einen gegebenen Eingabewert ist es mathematisch unmöglich, einen zweiten Eingabewert zu finden, der denselben Ausgabewert ergibt

Anmerkung 1 zum Begriff: Die mathematische Machbarkeit hängt von den spezifischen Sicherheitsanforderungen und der Sicherheitsumgebung ab.

Anmerkung 2 zum Begriff: Siehe Anmerkung 1 zum Begriff 3.1.2.30.

[QUELLE: ISO/IEC 9796-2:2010, 3.6, modified – Anmerkungen zum Begriff hinzugefügt]

3.1.2.57**Hash-Wert****(en: hash value)**

<Informationssicherheit> vollständiges oder abgeschnittenes Ergebnis nach der Anwendung einer Hash-Funktion auf Informationen

3.1.2.58**Identität****(en: identity)**

kennzeichnende Eigenschaft oder Persönlichkeit einer Person oder Instanz

3.1.2.59**unabhängiger Schlüssel****(en: independent key)**

<Informationssicherheit> symmetrischer Schlüssel, der aus einer Bitquelle hoher Entropie und nicht aus einem vorherigen Schlüssel abgeleitet wird

3.1.2.60**Infrastruktur****(en: infrastructure)**

technische Strukturen, die die Datenkommunikation innerhalb einer Anlage unterstützen

BEISPIEL Teile des IT-Netzes einer Anlage, etwa unter Anwendung von IEEE 802.3 oder IEEE 802.11 oder IEC 61158, Typ 10 (PROFINet), oder IEC 61158, Typ 9 (FOUNDATION™ Fieldbus HSE).²

² PROFINet und FOUNDATION Fieldbus sind Handelsnamen von verschiedenen Nutzerorganisationen. Diese Angabe dient nur der Unterrichtung der Anwender dieses Dokuments und bedeutet keine Anerkennung des Inhabers des Warenzeichens oder eines seiner Produkte. Die Übereinstimmung mit diesem Profil erfordert nicht die Verwendung des Handelsnamens. Die Verwendung des Handelsnamens erfordert die Erlaubnis seines Inhabers.

3.1.2.61

Initialisierungsvektor

(en: initialization vector)

<Informationssicherheit> Bitblock, der notwendig ist, damit eine kryptografische Verschlüsselung im Streaming-Betrieb einen einmaligen Bitstrom unabhängig von anderen Bitströmen, die mit derselben kryptografischen Verschlüsselung erzeugt werden, generieren kann

3.1.2.62

interoperabel

(en: interoperable)

Fähigkeit zur Zusammenarbeit, um eine bestimmte Rolle in einer oder mehreren verteilten Anwendungsprogrammen auszuführen

Anmerkung 1 zum Begriff: Im Falle der Interoperabilität passen Parameter und deren anwendungsbezogene Funktionalität sowohl syntaktisch als auch semantisch zusammen. Interoperabilität wird erreicht, wenn die Geräte sich gegenseitig ergänzende Parametersätze und Funktionen desselben Profils unterstützen.

[QUELLE: IEC TR 62390:2005, 6.2.2.6, modifiziert – angepasst]

3.1.2.63

anbindungsfähig

(en: interworkable)

Fähigkeit zur Übertragung von Parametern zwischen Korrespondenten

Anmerkung 1 zum Begriff: Zusätzlich zum Kommunikationsprotokoll, der Kommunikationsschnittstelle und dem Datenzugriff stimmen auch die Parameter-Datentypen überein.

[QUELLE: IEC TR 62390:2005, 6.2.2.5, modifiziert – angepasst]

3.1.2.64

Kerberos-Protokoll

(en: kerberos protocol)

spezifisches Netzwerk-Authentifizierungsprotokoll, mit dem über ein unsicheres Netzwerk kommunizierende Einzelpersonen auf sichere Weise gegenseitig ihre Identität prüfen können

3.1.2.65

Schlüsselvereinbarung

(en: key agreement)

<Informationssicherheit> Einführung eines vorher vereinbarten, geheimen Schlüssels zwischen Instanzen auf eine Weise, dass keine von ihnen den Wert dieses Schlüssels vorher bestimmen kann

[QUELLE: ISO/IEC 11770-1:2010, 2.13]

3.1.2.66

Schlüsselarchiv

(en: key archive)

Schlüsselmanagementarchiv

(en: key management archive)

<Informationssicherheit> Verschlüsselungssystem mit der Fähigkeit einer Ersatzentschlüsselung, das es berechtigten Personen ermöglicht, unter bestimmten vorgeschriebenen Bedingungen verschlüsselten Text mit Hilfe von Informationen zu entschlüsseln, die von einer oder mehreren vertrauenswürdigen Stellen bereitgestellt werden, welche spezielle Datenwiederherstellungsschlüssel besitzen

3.1.2.67

Schlüsselzentrale

(en: key center)

<Informationssicherheit> zentralisierter Schlüsselverteilungsprozess, gewöhnlich unter Anwendung eines gesonderten Computersystems, der zur Verschlüsselung und Verteilung von T-Schlüsseln, die von einer Benutzergemeinschaft benötigt werden, Schlüssel zur Schlüsselverschlüsselung (KEK) benutzt

Anmerkung 1 zum Begriff: Schlüsselzentralen sind in der Regel zertifiziert und auf eine zugelassene, unabhängige Prüfstelle rückführbar, so dass sie die Anforderungen von ISO/IEC 19790 (entspricht FIPS 140-2) für kryptografische Module der Ebene 3 oder der Ebene 4 erfüllen.

3.1.2.68

Schlüsselbestätigung

(en: key confirmation)

<Informationssicherheit> Zusicherung für eine Instanz, dass eine andere bezeichnete Instanz im Besitz des richtigen Schlüssels ist

[QUELLE: ISO/IEC 11770-1:2010, 2.16]

3.1.2.69

Schlüsselderegistrierung

(en: key de-registration)

<Informationssicherheit> Kennzeichnung aller Datensätze und Assoziationen des Schlüsselmaterials zur Angabe, dass der Schlüssel nicht mehr benutzt wird

3.1.2.70

Schlüsselableitung

(en: key derivation)

<Informationssicherheit> Prozess, mit dem ein oder mehrere Schlüssel aus einem vorher vereinbarten, geheimen Schlüssel und anderen Informationen abgeleitet werden

3.1.2.71

Schlüsselverteilung

(en: key distribution)

<Informationssicherheit> Weitergabe eines Schlüssels und von anderem Verschlüsselungsmaterial von einer Instanz, der der Schlüssel entweder gehört oder die den Schlüssel erzeugt, zu einer anderen Instanz, die den Schlüssel benutzen soll

3.1.2.72

Schlüsselverteilungszentrale

(en: key distribution center)

vertrauenswürdige Instanz, die Schlüssel erzeugt oder erwirbt und die Schlüssel an kommunizierende Stellen verteilt und die mit jeder dieser Stellen vorher einen eindeutigen symmetrischen Schlüssel vereinbart hat

[QUELLE: ISO/IEC 11770-1:2010, 2.22]

3.1.2.73

Schlüssel zur Schlüsselverschlüsselung (KEK)

(en: key encryption key)

<Informationssicherheit> kryptografischer Schlüssel zur Ver- oder Entschlüsselung anderer Schlüssel

Anmerkung 1 zum Begriff: Bei der bewährten Vorgehensweise wird die Verwendung von symmetrischen (geheimen) KEKs auf eine Schlüsselverpackung und nicht die Schlüsselweitergabe oder die Anwendung als Sitzungsschlüssel (d. h. Datenschlüssel) beschränkt.

Anmerkung 2 zum Begriff: KEKs können eine Hierarchie bilden. In der vorliegenden Norm werden KEKs häufig als „Masterschlüssel“ bezeichnet, obwohl die beiden Benennungen nicht als Synonyme gelten.

3.1.2.74

Schlüsselhinterlegung

(en: key escrow)

<Informationssicherheit> Vorgang der Speicherung von Schlüsseln und aller zugehörigen grundlegenden Informationen zur Schlüsselwiederherstellung in einem Schlüsselarchiv

3.1.2.75

Schlüsseleinführung

(en: key establishment)

<Informationssicherheit> Prozess, mit dem kryptografische Schlüssel unter kryptografischen Modulen von Hand (z. B. Key Loader), automatisch (z. B. Schlüsselweitergabe- und/oder -vereinbarungsprotokolle) oder durch eine Kombination beider Verfahren (bestehend aus Schlüsselweitergabe und Schlüsselvereinbarung) sicher verteilt werden

3.1.2.76

Installation von Schlüsselmaterial

(en: keying material installation)

<Informationssicherheit> Installation von Schlüsselmaterial für den operativen Einsatz

3.1.2.77

Schlüsselmanagement

(en: key management)

<Informationssicherheit> Regulierung und Durchführung von Erzeugung, Registrierung, Zertifizierung, De-registrierung, Verteilung, Installation, Speicherung, Archivierung, Aufhebung, Ableitung und Löschung von Schlüsselmaterial entsprechend einer Sicherheitsrichtlinie

[QUELLE: ISO/IEC 11770-1:2010, 2.28]

3.1.2.78

Infrastruktur des Schlüsselmanagements

(en: key management infrastructure)

<Informationssicherheit> Rahmen und Dienste zur Generierung, Herstellung, Verteilung, Lenkung, Darstellung und Löschung des gesamten kryptografischen Materials, einschließlich symmetrischer Schlüssel, sowie Signierung öffentlicher Schlüssel und Erzeugung eigener statischer und flüchtiger asymmetrischer Schlüsselpaare

Anmerkung 1 zum Begriff: Dazu gehören alle Elemente (Hardware, Software, andere Ausrüstung und Dokumentation), Anlagen, Mitarbeiter, Verfahren, Normen und Informationsprodukte, die das System bilden, welches die Zustellung und Verteilung kryptografischer Produkte und Dienste zum Endbenutzer verwaltet und unterstützt.

Anmerkung 2 zum Begriff: Schlüsselmanagementdienste umfassen Schlüsselbestellung, Verteilung, Erneuerung, Aktualisierung von Attributen des Schlüsselmaterials, Aufhebung des Zertifikats, Schlüsselwiederherstellung und die Verteilung, Darstellung, Rückverfolgung und Lenkung der Software, die entweder Sicherheitsfunktionen des Schlüsselmaterials oder kryptografische Funktionen ausführt.

3.1.2.79

Schlüsselmanager

(en: key manager)

<Informationssicherheit> Infrastrukturgerät des Schlüsselmanagements, das Schlüsselmanagementdienste zur Verfügung stellt

3.1.2.80

Schlüsselpaar

(en: key pair)

asymmetrisches Schlüsselpaar

(en: asymmetric key pair)

<Informationssicherheit> Paar zusammengehöriger Schlüssel, wobei der private Schlüssel die private Umwandlung und der öffentliche Schlüssel die öffentliche Umwandlung festlegt

Anmerkung 1 zum Begriff: Ein Schlüsselpaar wird zusammen mit asymmetrischen kryptografischen Algorithmen benutzt.

[QUELLE: ISO/IEC 11770-1:2010, 2.2]

3.1.2.81**Schlüsselwiederherstellung****(en: key recovery)**

<Informationssicherheit> Mechanismen und Prozesse, die es berechtigten Instanzen ermöglichen, Schlüsselmaterial aus sicheren Schlüsselreserve- oder -archivspeichern wiederherzustellen

3.1.2.82**Schlüsselregistrierung****(en: key registration)**

<Informationssicherheit> Vorgang der offiziellen Eintragung des Schlüsselmaterials von einer Registrierungsstelle

3.1.2.83**Schlüsselaufhebung****(en: key revocation)**

<Informationssicherheit> Vorgang, mit dem betroffenen Instanzen vor dem Ende der festgelegten Kryptoperiode des Schlüsselmaterials mitgeteilt wird, dass dieses Schlüsselmaterial operativ nicht mehr genutzt werden sollte

3.1.2.84**Schlüsselweitergabe****(en: key transport)**

<Informationssicherheit> Vorgang der Übergabe eines Schlüssels von einer Instanz zu einer anderen Instanz mit einem geeigneten Schutz

Anmerkung 1 zum Begriff: Im Zusammenhang mit einem öffentlichen (asymmetrischen) Verschlüsselungsalgorithmus wird das Schlüsselmaterial mit dem öffentlichen Schlüssel des Empfängers verschlüsselt und anschließend mit dem privaten Schlüssel des Empfängers entschlüsselt. Im Zusammenhang mit einem symmetrischen Algorithmus wird das Schlüsselmaterial mit einem vorher von den beiden Stellen vereinbarten Schlüssel zur Schlüsselverschlüsselung (KEK) verpackt.

[QUELLE: ISO/IEC 11770-1:2010, 2.33]

3.1.2.85**Schlüsselaktualisierung****(en: key update)**

<Informationssicherheit> an einem kryptografischen Schlüssel durchgeführte Funktion zur Berechnung eines neuen zugehörigen Schlüssels

3.1.2.86**Schlüsselnutzungsdauer****(en: key usage period)**

<Informationssicherheit> entweder die Absendernutzungsdauer oder die Empfängernutzungsdauer eines symmetrischen Schlüssels

3.1.2.87**Schlüsselverpackung****(en: key wrapping)**

<Informationssicherheit> Verfahren zur Verschlüsselung von Schlüsseln (zusammen mit der zugehörigen Integritätsfunktion), das sowohl Vertrauenswürdigkeit als auch den Schutz der Integrität unter Anwendung eines symmetrischen Schlüssels bietet

3.1.2.88**Schlüssel zur Schlüsselverpackung****(en: key wrapping key)**

<Informationssicherheit> (symmetrischer) Schlüssel zur Schlüsselverpackung (KEK)

3.1.2.89

Schlüsselmaterial

(en: **keying material**)

<Informationssicherheit> Daten, die zur Einführung und Aufrechterhaltung kryptografischer Verschlüsselungsbeziehungen notwendig sind

BEISPIEL Schlüssel, Initialisierungswerte, Gültigkeitsdauern.

[QUELLE: ISO/IEC 11770-1:2010, 2.27]

3.1.2.90

Latenzzeit

(en: **latency**)

Dauer von der Erzeugung der Daten im Datenquellgerät bis zur Bereitstellung im Zielgerät

Anmerkung 1 zum Begriff: Die vorgesehenen Messpunkte sind a) technische Geräte oder b) Schichtgrenzen innerhalb von mehrschichtiger Software (z. B. von der sendenden Transportfunktion zur empfangenden Transportfunktion oder von der sendenden Anwendung zum sendenden Modem).

3.1.2.91

Lease

(en: **lease**)

differenzierte Zuweisung der Kommunikationsressource je Sitzung an einem GIAP

3.1.2.92

geringstes Recht

(en: **least privilege**)

<Informationssicherheit> Sicherheitsgrundsatz, nach dem Zugriffsrechte (z. B. Programmausführungsrechte, Dateiänderungsrechte) von berechtigten Personen und deren Vertretern im Netz auf die geringsten notwendigen Rechte zur Ausführung ihrer Aufgaben beschränkt werden

3.1.2.93

Verbindungsweig

(en: **link**)

kurzzeitiger oder dauerhafter Verbindungspfad zwischen zwei oder mehr Geräten für die Sendung oder den Empfang von Nachrichten

3.1.2.94

Masterschlüssel

(en: **master key**)

<Informationssicherheit> kryptografischer Schlüssel zur Ableitung anderer Schlüssel

Anmerkung 1 zum Begriff: Bei der bewährten Vorgehensweise ist die Nutzung von Masterschlüsseln als Sitzungsschlüssel (d. h. Datenschlüssel), was deren Kryptoanalyse vereinfachen würde, verboten. Sie dürfen als KEKs häufig auf der obersten Ebene einer KEK-Hierarchie eingesetzt werden.

3.1.2.95

Maschentopologie

(en: **mesh topology**)

Netztopologie, bei der redundante, physisch verschiedene Routing-Pfade zwischen jedem Paar von Netzknoten zur Verfügung stehen

Anmerkung 1 zum Begriff: Mit einer drahtlosen Maschentopologie kann der Deckungsgrad über die Multihop-Fähigkeit erweitert und/oder die Kommunikationszuverlässigkeit durch die Bereitstellung redundanter Pfade zwischen Geräten erhöht werden.

3.1.2.96**Nachrichtenauthentifizierung****(en: message authentication)****PDU-Authentifizierung****(en: PDU authentication)**

<Informationssicherheit> Feststellung, dass eine Nachricht von einem Mitglied einer berechtigten Gruppe von Kommunizierenden erstellt und seitdem nicht verändert wurde

3.1.2.97**Nachrichtenauthentifizierungscode****(en: message authentication code)****Nachrichtenintegritätscode****(en: message integrity code)**

<Informationssicherheit> mit einem symmetrischen Schlüssel erzeugte kryptografische Prüfsumme, die gewöhnlich an Daten angefügt wird, um ähnlich einer digitalen Signatur die Datenintegrität und die Authentifizierung der Quelle zu sichern

[QUELLE: ISO/IEC 26907:2009, 4.16]

3.1.2.98**Nachrichtenauthentifizierungscode-Algorithmus****(en: message authentication code algorithm)**

<Informationssicherheit> Algorithmus zur Berechnung einer Funktion, die Bitfolgen und einen geheimen Schlüssel auf Bitfolgen fester Länge abbildet und die die folgenden beiden Eigenschaften erfüllt:

- für jeden Schlüssel und jede Eingabefolge kann die Funktion erfolgreich berechnet werden;
- für jeden festen Schlüssel und unter der Voraussetzung, dass der Schlüssel vorher nicht bekannt ist, ist es mathematisch unmöglich, den Funktionswert einer neuen Eingabefolge zu berechnen, selbst bei Kenntnis einer Menge von Eingabefolgen und entsprechender Funktionswerte, wenn der Wert der i-ten Eingabefolge nach Untersuchung des ersten Wertes der i-1-ten Funktionswerte (für ganzzahlige Werte von $i > 1$) ausgewählt worden ist

[QUELLE: ISO/IEC 9797-1:2011, 3.10, modifiziert – Löschung von für diese Norm nicht relevanten Anmerkungen]

3.1.2.99**MIC-Berechnungssyntax****(en: MIC-computation syntax)**

<Informationssicherheit> konkrete Darstellung einer N-SDU-verbundenen Protokollinformation, die gewöhnlich über einen vorgesetzten Pseudo-Header angefügt wird und für die Anbindung von selektiven N-Adressen und der N-PCI und mitunter selektiven (N-1)-Adressen und einer (N-1)-PCI an die N-SDU benutzt wird, bevor ein Integritätsprüfcode (MIC) für diesen Verbund berechnet wird

3.1.2.100**Gruppenaufruf****(en: multicast)**

Nachrichtenübermittlung von einer Quelle zu einer Menge vorgesehener Empfänger

Anmerkung 1 zum Begriff: Die Teilnehmer der Menge sind entweder unbestimmt oder bestimmt, wobei letztere einer Nullmenge entsprechen können.

Anmerkung 2 zum Begriff: Ein Sammelaufruf ist eine besondere Form des Gruppenaufrufs, gewöhnlich mit einer unbestimmten Menge vorgesehener Empfänger. Siehe auch „Einzelaufruf“.

Anmerkung 3 zum Begriff: Im Gegensatz zum Sammelaufruf wird der Gruppenaufruf in der vorliegenden Norm nicht unterstützt.

3.1.2.101**Netzwerk-Managementobjekt****(en: network management object)**

Anwendungssoftware innerhalb eines Geräts, die als lokaler Partner eines Netzwerkmanagers wirkt

3.1.2.102

nicht-deterministischer Bitgenerator

(en: **non-deterministic bit generator**)

<Informationssicherheit> Zufallsbitgenerator, dessen Sicherheit von der Abtastung einer Entropiequelle abhängt

Anmerkung 1 zum Begriff: Quellen solcher Bits sind der Lawinendurchbruch einer Zenerdiode, Schrotrauschen, Wärmerauschen, radioaktiver Zerfall, kosmische Strahlung usw.

Anmerkung 2 zum Begriff: Zur Bereinigung ihrer Ausgabewerte und zur Ermittlung von Fehlern in dem Kreis, der die Zufälligkeit sichert, ist eine Nachverarbeitung solcher Rauschquellen erforderlich. Nur der nachverarbeitete Bitstrom ist als Startwert für einen deterministischen Bitgenerator geeignet.

[QUELLE: ISO/IEC 18031:2011, 3.23, modifiziert – ursprüngliche Anmerkung zum Begriff gelöscht und neue Anmerkungen zum Begriff hinzugefügt]

3.1.2.103

Nicht-Abstreitbarkeit

(en: **non-repudiation**)

<Informationssicherheit> Fähigkeit, das Auftreten eines behaupteten Ereignisses oder einer behaupteten Handlung und die verursachenden Instanzen nachzuweisen, um Streitigkeiten über das Auftreten oder Nichtauftreten des Ereignisses oder der Handlung und die Beteiligung von Instanzen an dem Ereignis zu entscheiden

Anmerkung 1 zum Begriff: Im allgemeinen Kontext der Informationssicherheit bietet die Nicht-Abstreitbarkeit die Zusicherung, dass der Absender der Informationen einen dauerhaften Zustellungsnachweis oder der Empfänger einen dauerhaften Nachweis der Absenderidentität erhält, so dass die Stelle, die den nicht-abstreitbaren Nachweis erhalten hat, später nicht glaubhaft bestreiten kann, die Information verarbeitet zu haben.

[QUELLE: ISO/IEC 27000:2014, 2.54, modifiziert – Infinitivsatz „um...zu“ hinzugefügt]

3.1.2.104

Nonce

(en: **nonce**)

<Informationssicherheit> einmalig verwendete Zahl oder Wert, bei dem die Aussicht auf eine Wiederholung (meistens) gering ist

3.1.2.105

operative Phase

(en: **operational phase**)

operativer Einsatz

(en: **operational use**)

<Informationssicherheit> Phase im Lebenszyklus des Schlüsselmaterials, in der dieses für kryptografische Standardvorgänge benutzt wird

3.1.2.106

operative Speicherung

(en: **operational storage**)

<Informationssicherheit> normale Speicherung von operativem Schlüsselmaterial während dessen Kryptoperiode

3.1.2.107

Absendernutzungsdauer

(en: **originator usage period**)

<Informationssicherheit> Dauer in der Kryptoperiode eines symmetrischen Schlüssels, während der Daten kryptografisch geschützt sein können

3.1.2.108**Schutzdauer****(en: period of protection)**

<Informationssicherheit> Zeitspanne, während der die Integrität und/oder die Vertrauenswürdigkeit eines Schlüssels aufrechterhalten werden muss/müssen

3.1.2.109**Klartext****(en: plaintext)**

<Informationssicherheit> unverschlüsselte Informationen (bezogen auf einen Ver- oder Entschlüsselungsvorgang)

Anmerkung 1 zum Begriff: In der Regel ist die Klartexteingabe in eine Verschlüsselungsoperation noch nicht verschlüsselt, aber in einigen Fällen ist die Eingabe selbst eine Ausgabe einer anderen kryptografischen Operation.

[QUELLE: ISO/IEC 10116:2006, 3.11, modifiziert durch einen eingeklammerten Kommentar]

3.1.2.110**Management auf der Grundlage einer Sicherheitsrichtlinie****(en: policy-based management)**

administrativer (innerbetrieblicher) Ansatz zur Vereinfachung des Managements eines vorgegebenen Systems über das Aufstellen von Sicherheitsrichtlinien zur Behandlung von Situationen, deren Eintreten nachvollziehbar möglich ist

3.1.2.111**privater Schlüssel****(en: private key)**

<Informationssicherheit> (kryptografischer) Schlüssel eines asymmetrischen Schlüsselpaars einer Instanz, der privat bleibt

Anmerkung 1 zum Begriff: Die Sicherheit eines asymmetrischen Systems hängt von der Geheimhaltung dieses Schlüssels ab.

Anmerkung 2 zum Begriff: In einem asymmetrischen (öffentlichen) Verschlüsselungssystem ist der private Schlüssel an einen öffentlichen Schlüssel gebunden. Der private Schlüssel ist nur dem Eigentümer des Schlüsselpaars bekannt und wird verwendet für:

- die Berechnung des entsprechenden öffentlichen Schlüssels;
- die Berechnung einer digitalen Signatur, die durch den entsprechenden öffentlichen Schlüssel verifizierbar ist;
- die Entschlüsselung der Daten, die mit dem entsprechenden öffentlichen Schlüssel verschlüsselt worden sind; oder
- die Berechnung eines Teils gemeinsam genutzter Daten zusammen mit anderen Informationen.

[QUELLE: ISO/IEC 11770-1:2010, 2.35, modifiziert – zweite Anmerkung zum Begriff hinzugefügt]

3.1.2.112**Pseudo-Header****(en: pseudo-header)**

Informationen, die einer PDU vor der Berechnung eines MIC für die PDU logisch vorangestellt werden, die aber ansonsten in der PDU nicht enthalten sind

3.1.2.113**öffentlicher Schlüssel****(en: public key)**

<Informationssicherheit> Schlüssel eines asymmetrischen Schlüsselpaars einer Instanz, der in der Regel ohne Gefährdung der Sicherheit öffentlich verfügbar gemacht werden kann

[QUELLE: ISO/IEC 11770-1:2010, 2.36]

3.1.2.114

Zertifikat des öffentlichen Schlüssels

(en: public key certificate)

<Informationssicherheit> Informationen über den öffentlichen Schlüssel einer Instanz, die von einer Zertifizierungsstelle eingetragen sind

Anmerkung 1 zum Begriff: Mit Zusatzinformationen im Zertifikat kann die Kryptoperiode des Schlüssels angegeben werden und wie er anzuwenden ist.

[QUELLE: ISO/IEC 11770-1:2010, 2.37, modifiziert – Anmerkung zum Begriff hinzugefügt]

3.1.2.115

Empfängernutzungsdauer

(en: recipient usage period)

<Informationssicherheit> Dauer in der Kryptoperiode eines symmetrischen Schlüssels, während der die geschützten Informationen verarbeitet werden

Anmerkung 1 zum Begriff: Diese Dauer erstreckt sich häufig über die zulässige Absendernutzungsdauer.

3.1.2.116

dynamisches Störausgleichsverhalten

(en: resilience)

Fähigkeit einer Funktionseinheit, beim Auftreten von Fehlern oder Fehlzuständen eine geforderte Funktion weiterhin auszuführen

[QUELLE: ISO/IEC 2382-14:1997, 14.04.06]

3.1.2.117

Sperrfrist

(en: retention period)

<Informationssicherheit> Minstdauer, die ein Schlüssel oder andere mit der Verschlüsselung im Zusammenhang stehende Informationen in einem Archiv aufbewahrt werden sollten

3.1.2.118

Stabilität

(en: robustness)

Umfang, in dem ein System oder ein Bauteil beim Auftreten von ungünstigen Eingabewerten oder bei ungünstigen Umgebungsbedingungen einwandfrei funktionsfähig ist

[QUELLE: ISO/IEC/IEEE 24765:2010, 3.2601]

3.1.2.119

Router

(en: router)

Gerät, das NPDUs in einem Computernetzwerk auf der Basis von Informationen der Netzwerkschicht befördert

3.1.2.120

Kurzsignalisierung zur Steuerung

(en: short control signaling)

MAC-Kurznachrichten, die von einem entsprechenden Empfänger von MAC-Nachrichten als unmittelbare Antwort an den Absender dieser MAC-Nachrichten gesendet werden, um Steuerinformationen, wie ARQ-ACK/NAK-Status, Qualität und Pegel des empfangenen Signals usw., zu senden, die das sendende Gerät über den Empfangsstatus und über aktuelle Bedingungen im Medium informieren

Anmerkung 1 zum Begriff: Diese Anmerkung betrifft nur die französische Sprache.

3.1.2.121

geheimer Schlüssel

(en: secret key)

<Informationssicherheit> mit symmetrischen Verschlüsselungsverfahren von einer festgelegten Menge von Instanzen verwendeter Schlüssel

[QUELLE: ISO/IEC 11770-3:2008, 3.35]

3.1.2.122

sicheres Kommunikationsprotokoll

(en: **secure communications protocol**)

<Informationssicherheit> Kommunikationsprotokoll, das eine angemessene Vertraulichkeit, Authentifizierung, Integrität des Inhalts und Nachrichtenlaufzeitüberwachung bereitstellt

3.1.2.123

Sicherheitsassoziation

(en: **security association**)

<Informationssicherheit> Beziehung zwischen zwei oder mehr Instanzen, für die Attribute (Zustandsinformationen und Vorschriften) bestehen, nach denen die Bereitstellung von Sicherheitsdiensten, die diese Instanzen betreffen, geregelt wird

[QUELLE: ISO/IEC 10745:1995, 3.8]

3.1.2.124

Sicherheitsdomäne

(en: **security domain**)

<Informationssicherheit> Menge von Werten und Ressourcen, die einer gemeinsamen Sicherheitsrichtlinie unterliegen

Anmerkung 1 zum Begriff: Sicherheitsdomänen sind oft so organisiert (z. B. hierarchisch), dass sie größere Domänen bilden.

[QUELLE: ISO/IEC 18028-3:2005, 3.19, modifiziert – Anmerkung zum Begriff hinzugefügt]

3.1.2.125

Sicherheitsmanager

(en: **security manager**)

<Informationssicherheit> Anwendungssoftware, die verschiedene Aspekte der operativen Sicherheit eines Netzwerks mit mehreren Geräten in der Regel durch Wechselwirkung mit Gerätesicherheits-Management-objekten (DSMO) im (in den) überwachten Gerät(en) überwacht

Anmerkung 1 zum Begriff: Ein Netzwerksicherheitsmanager ist häufig ein dediziertes Gerät, das sowohl physisch als auch konstruktiv geschützt ist. (Siehe ISO/IEC 19790 (entspricht FIPS 140-2) und NIST/CSE Cryptographic Module Validation Program, <http://csrc.nist.gov/cryptval/cmvp.htm>).

3.1.2.126

Sicherheitsdienste

(en: **security services**)

<Informationssicherheit> Mechanismen zur Sicherung von Vertraulichkeit, Datenintegrität, Authentifizierung und/oder Nicht-Abstreitbarkeit von Informationen

3.1.2.127

Aufgabentrennung

(en: **separation of duties**)

<Informationssicherheit> Sicherheitsgrundsatz, nach dem kritische Funktionen unter verschiedenen Mitarbeitern aufgeteilt werden, im Bestreben sicherzustellen, dass keine Einzelperson genug Informationen oder Zugriffsrechte besitzt, um schädigende Betrugsdelikte zu begehen

3.1.2.128

Sitzung

(en: **session**)

T-Assoziation

3.1.2.129

Sitzungsschlüssel

(en: session key)

T-Schlüssel

(en: T-key)

kurzzeitiger Datenschlüssel, der von TLEs benutzt wird

3.1.2.130

Signaturerzeugung

(en: signature generation)

<Informationssicherheit> Anwendung eines digitalen Signaturalgorithmus und eines privaten Schlüssels zur Erzeugung einer digitalen Signatur für Daten

3.1.2.131

Signaturauthentifizierung

(en: signature authentication)

<Informationssicherheit> Anwendung eines digitalen Signaturalgorithmus und eines öffentlichen Schlüssels zur Überprüfung einer digitalen Signatur für Daten

3.1.2.132

Quellenauthentifizierung

(en: source authentication)

<Informationssicherheit> Bestätigung, dass die Quelle der Daten die geforderte Quelle ist

3.1.2.133

aufgeteiltes Wissen

(en: split knowledge)

<Informationssicherheit> Vorgang, bei dem ein kryptografischer Schlüssel in mehrere Schlüsselkomponenten aufgeteilt wird, die einzeln keine anderen Kenntnisse über den ursprünglichen Schlüssel als eventuell dessen Größe offenlegen und die anschließend in einer Anzahl von vordefinierten Gruppierungen der mehrfachen spezifischen Schlüssel zur Wiederherstellung des ursprünglichen Schlüssels zusammengefasst werden können

3.1.2.134

statischer Schlüssel

(en: static key)

<Informationssicherheit> Schlüssel, der kein flüchtiger Schlüssel ist und der für eine relativ lange Anwendungsdauer vorgesehen ist, in der Regel in aufeinander folgenden Aufrufen eines Einführungsschemas für einen kryptografischen Schlüssel

3.1.2.135

Bitstromverschlüsselung

(en: stream cipher)

<Informationssicherheit> kryptografisches Element, das einen symmetrischen Schlüssel und einen Initialisierungsvektor benutzt und mit ununterbrochenen Strömen von Eingabewerten anstatt mit festen Blöcken arbeitet

3.1.2.136

Teilnetz

(en: subnet)

(N)-Teilnetz

(en: (N)-subnet)

D-Teilnetz

(en: D-subnet)

N-Teilnetz

(en: N-subnet)

Teilnetzwerk, d. h. Untermenge eines vollständigen Netzwerks, entweder in der des Data-Link-Layer oder des Network-Layer (Schichten 2 oder 3 des OSI-Basis-Referenzmodells), das aus mehreren Endpunkt- und Weiterleitungsknoten besteht, die über eine oft homogene (N–1)-Schicht miteinander verbunden sind

3.1.2.137**Überrahmen****(en: superframe)**

Zusammenfassung von Zeitschlitzten mit gemeinsamer Wiederholungsperiode und möglicherweise anderen gemeinsamen Attributen

3.1.2.138**symmetrischer Schlüssel****(en: symmetric key)**

<Informationssicherheit> geheimer Schlüssel, der von zwei oder mehr Stellen gemeinsam benutzt wird und der sowohl für die Ver- und Entschlüsselung als auch für die Berechnung und Verifizierung des Nachrichtenintegritätscodes benutzt werden kann

[QUELLE: ISO/IEC 26907:2009, 4.27]

3.1.2.139**symmetrischer Verschlüsselungsalgorithmus****(en: symmetric-key algorithm)****symmetrischer (kryptografischer) Algorithmus****(en: symmetric-key (cryptographic) algorithm)**

<Informationssicherheit> kryptografischer Algorithmus, der den gleichen (gewöhnlich geheimen) Schlüssel für eine Operation und deren Umkehrung (z. B. Ver- und Entschlüsselung) benutzt

3.1.2.140**Systeminitialisierung****(en: system initialization)**

<Informationssicherheit> Einrichtung und Konfiguration eines Systems für einen sicheren Betrieb

3.1.2.141**Systemmanager****(en: system manager)**

Anwendungssoftware, die verschiedene operative Aspekte eines Netzwerks mit mehreren Geräten mit Ausnahme der Sicherheit in der Regel durch Wechselwirkung mit Netzwerk-Managementobjekten im (in den) überwachten Gerät(en) überwacht

Anmerkung 1 zum Begriff: Ein Netzwerkmanager überwacht entweder ein gesamtes Netzwerk mit mehreren Geräten oder er wirkt untergeordnet zu einem anderen Netzwerkmanager und überwacht dabei nur einen Teil des gesamten Netzwerks.

Anmerkung 2 zum Begriff: Ein Netzwerkmanager ist nicht immer ein dediziertes Gerät.

3.1.2.142**System-/Sicherheitsmanager****(en: system/security manager)**

Funktionalität des Systemmanagers im Auftrag der Funktionalität des Sicherheitsmanagers

3.1.2.143**Bedrohung****(en: threat)**

<Informationssicherheit> Umstand oder Ereignis mit der Möglichkeit der nachteiligen Beeinflussung von Anlagenbetrieb (einschließlich Funktion, Erscheinungsbild oder Ansehen), Werten oder Einzelpersonen durch ein Informationssystem über unberechtigten Zugriff, Zerstörung, Löschung, Modifikation von Daten, Nachrichtenlaufzeit und/oder Dienstverweigerung

3.1.2.144**Schwellenwert****(en: threshold)**

Wert, der bei Überschreitung in eine bestimmte Richtung eine bestimmte Reaktion hervorruft

3.1.2.145

Zeitfenster

(en: time window)

Zeitintervall

3.1.2.146

D-Transaktion

(en: D-transaction)

MPDU, die keine MPDU mit direkter Quittierung ist, zuzüglich einer Folge von null oder mehr MPDUs mit direkter Quittierung, die unmittelbar folgen und ein Resultat der ersten MPDU (und möglicherweise aller anderen) sind, alle im selben Kanal und im selben Zeitschlitz

3.1.2.147

Tunneling

(en: tunneling)

Einkapselung eines ersten Protokolls innerhalb eines zweiten Kommunikationsprotokolls zur Beförderung von PDUs aus dem ersten Protokoll

3.1.2.148

Dienstleistungsfeld

(en: type-of-service)

gemeinsamer Name, der einer Menge von Protokollelementen und zugehörigen Attributen der Dienstgüte gegeben wird, die zusammen ein Teilprotokoll (z. B. Echtzeit für Audio, zeitkritische Daten und nicht zeitkritische Daten) mit eindeutigen Funktionen bilden

3.1.2.149

unberechtigte Offenlegung

(en: unauthorized disclosure)

<Informationssicherheit> Ereignis, bei dem Informationen gegenüber Instanzen enthüllt werden, die keinen berechtigten Zugriff darauf haben

3.1.2.150

Einzelaufruf

(en: unicast)

Nachrichtenübermittlung von einer Quelle zu einem einzigen vorgesehenen Empfänger

Anmerkung 1 zum Begriff: Siehe auch „Gruppenaufruf“ und „Sammelaufruf“.

3.1.2.151

Benutzerinitialisierung

(en: user initialization)

Vorgang, mit dem ein Benutzer die kryptografische Anwendung für den Einsatz vorbereitet (z. B. Installation und Konfiguration von Software und Hardware)

3.1.2.152

Benutzerregistrierung

(en: user registration)

Vorgang, mit dem eine Instanz Mitglied einer Sicherheitsdomäne wird

3.1.2.153

vollständige Löschung

(en: zeroisation)

<Informationssicherheit> Verfahren der Löschung elektronisch gespeicherter Daten, kryptografischer Schlüssel und kritischer gespeicherter Parameter durch Veränderung oder Löschung des Speicherinhalts in einer Weise, dass die Wiederherstellung der Daten verhindert wird

3.1.3 Symbole für symmetrische Schlüssel, asymmetrische Schlüssel und Zertifikate

ANMERKUNG In der vorliegenden Norm definierte symmetrische Schlüssel sind 128-Bit-Schlüssel. In der vorliegenden Norm definierte asymmetrische Schlüssel weisen vermutlich eine ähnliche kryptografische Bitstärke von 128 Bit oder mehr auf. Die genaue Beschreibung des kryptografischen Materials kann Abschnitt 7 entnommen werden.

3.1.3.1

K_DL

aktueller Datenschlüssel für alle Geräte im lokalen D-Teilnetz

3.1.3.2

K_global

bekannter Schlüssel mit einem statischen und veröffentlichten Wert, der die PDU-Struktur und die Verarbeitung vereinheitlicht, wenn ein gemeinsam benutzter, geheimer Schlüssel ungeeignet oder unbekannt ist

3.1.3.3

K_open

bekannter Schlüssel begrenzter Nutzbarkeit mit einem statischen und veröffentlichten Wert, der sich von „K_global“ unterscheidet, der aber als Wert für „K_join“ benutzt werden kann, um ein Gerät über seine Luftschnittstelle bereitzustellen

Anmerkung 1 zum Begriff: Die Verwendung dieses Schlüssels in einer Umgebung, in der Lauschangriffe auftreten könnten, kann die Sicherheit des Geräts und seiner Verbindungen zu den anderen Komponenten des Funksystems beeinträchtigen.

3.1.3.4

K_join

Schlüssel zum sicheren Laden (Bootstrap) eines neuen Geräts in ein Netzwerk

3.1.3.5

K_join_wrapped

verpackte Version eines „K_join“-Schlüssels, der zur Wiederherstellung bei einem ausgefallenen Sicherheitsmanager benutzt wird

3.1.3.6

K_master

Masterschlüssel, der als KEK zur Schlüsselverteilung und für das Sicherheitsmanagement eines einzelnen Geräts benutzt wird

3.1.3.7

K_session_AB

aktueller Datenschlüssel für eine Sitzung zwischen Gerät A und Gerät B, der mit „K_session_BA“ identisch ist

3.1.3.8

CA_root

öffentlicher Schlüssel einer Zertifizierungsstelle, die ein Zertifikat eines öffentlichen Schlüssels für ein Gerät ausgestellt hat

Anmerkung 1 zum Begriff: Dieser Schlüssel wird im Allgemeinen als „Wurzelschlüssel“ bezeichnet und unterstützt den Nachweis der wahren Identität des Geräts, das das Zertifikat übermittelt, sowie einiger zugehöriger Verschlüsselungsinformationen.

3.1.3.9

Cert-A

Zertifikat des öffentlichen Schlüssels von Gerät A, das während der Ausführung eines authentifizierten Einführungsprotokolls für einen öffentlichen Schlüssel den Nachweis der wahren Identität des Geräts sowie einiger zugehöriger Verschlüsselungsinformationen unterstützt

3.1.4 Begriffe zur Beschreibung des Geräteverhaltens

3.1.4.1

Leistungspotential

(en: **capability**)

Fähigkeit der Ausführung von Aktionen, einschließlich Attributen der Befähigungen und Maße der Fähigkeiten, wie Kapazität

BEISPIEL Anzahl der verbundenen Geräte, die ein Router unterstützen kann.

Anmerkung 1 zum Begriff: Das Mindest-Leistungspotential wird durch Profile bestimmt.

[QUELLE: ISO 18435-2:2012, 3.6, modifiziert – Beispiel und Anmerkung hinzugefügt]

3.1.4.2

Konfiguration

(en: **configuration**)

Parametersatz, der 1) das Verhalten ändert und 2) vom Systemmanager eingestellt werden kann

BEISPIEL Hop-Limit des Network-Layer.

Anmerkung 1 zum Begriff: Konfigurationen mit entsprechenden Standardwerten (z. B. Hop-Limit der NL = 64).

3.1.4.3

konfigurieren

(en: **configure**)

Vorgang der Festlegung und Verwaltung von Konfigurationsparametern

3.1.4.4

Leistungsmerkmal

(en: **feature**)

offensichtliche Eigenschaft eines Geräts

BEISPIEL Batteriebetrieben.

3.1.4.5

verbindlich

(en: **mandatory**)

gefordertes Element für die Beanspruchung der Übereinstimmung mit der vorliegenden Norm

BEISPIEL Unterstützung der Kryptografie mit einem symmetrischen Schlüssel.

3.1.4.6

wahlfrei

(en: **optional**)

Element, für das keine Übereinstimmung mit der vorliegenden Norm gefordert wird, das aber bei Vorhandensein ein Verhalten in Übereinstimmung mit der vorliegenden Norm aufweisen muss

BEISPIEL Unterstützung der Kryptografie mit einem asymmetrischen Schlüssel.

English Version

Industrial networks - Wireless communication network and
communication profiles - ISA 100.11a
(IEC 62734:2014)

Réseaux industriels - Réseau de communication sans fil et
profils de communication - ISA 100.11a
(IEC 62734:2014)

Industrielle Kommunikationsnetze - Drahtlose
Kommunikationsnetze und Kommunikationsprofile - ISA
100.11a
(IEC 62734:2014)

This European Standard was approved by CENELEC on 2014-12-02. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.



European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Foreword

The text of document 65C/778/FDIS, future edition 1 of IEC 62734, prepared by SC 65C "Industrial networks" of IEC/TC 65 "Industrial-process measurement, control and automation" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN 62734:2015.

The following dates are fixed:

- latest date by which the document has to be (dop) 2015-09-02
implemented at national level by
publication of an identical national
standard or by endorsement
- latest date by which the national (dow) 2017-12-02
standards conflicting with the
document have to be withdrawn

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC [and/or CEN] shall not be held responsible for identifying any or all such patent rights.

Endorsement notice

The text of the International Standard IEC 62734:2014 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standards indicated:

IEC 61158 Series	NOTE	Harmonized as EN 61158 Series.
IEC 61499-4:2005	NOTE	Harmonized as EN 61499-4:2006 ¹⁾ (not modified).
IEC 61512-1	NOTE	Harmonized as EN 61512-1.
IEC 61804-3	NOTE	Harmonized as EN 61804-3.
IEC 62264-1:2013	NOTE	Harmonized as EN 62264-1:2013 (not modified).
IEC 62591	NOTE	Harmonized as EN 62591.
ISO 3166-1	NOTE	Harmonized as EN ISO 3166-1.

¹⁾ Superseded by EN 61499-4:2013 (IEC 61499-4:2013): DOW = 2016-03-06.

CONTENTS

0	Introduction	32
0.1	General.....	32
0.2	Document structure	32
0.3	Potentially relevant patents	32
1	Scope.....	34
2	Normative references	34
3	Terms, definitions, abbreviated terms, acronyms, and conventions	35
3.1	Terms and definitions	35
3.1.1	(N)-layer and other terms and definitions from the open systems interconnection Basic Reference Model	35
3.1.2	Other terms and definitions	44
3.1.3	Symbols for symmetric keys, and for asymmetric keys and certificates	62
3.1.4	Terms used to describe device behavior	63
3.2	Abbreviated terms and acronyms.....	63
3.3	Conventions.....	70
3.3.1	Service interfaces	70
3.3.2	Table cells	71
3.3.3	Italics.....	71
3.3.4	Bold face	71
3.3.5	Informal declarations of named constants	71
4	Overview	71
4.1	General.....	71
4.2	Interoperability and related issues	72
4.3	Quality of service	72
4.4	Worldwide applicability	72
4.5	Network architecture	73
4.5.1	Interfaces	73
4.5.2	Data structures	73
4.5.3	Network description	74
4.5.4	Generic protocol data unit construction.....	76
4.5.5	Abstract data and concrete representations	76
4.6	Network characteristics	79
4.6.1	General	79
4.6.2	Scalability	79
4.6.3	Extensibility	79
4.6.4	Simple operation	80
4.6.5	Site-license-exempt operation	80
4.6.6	Robustness in the presence of interference, including from other wireless systems	80
4.6.7	Determinism and contention-free media access	80
4.6.8	Self-organizing networking with support for redundancy	81
4.6.9	Internet-protocol-compatible NL.....	81
4.6.10	Coexistence with other radio frequency systems	81
4.6.11	Time-slotted assigned-channel D-transactions as the basis for communication	83
4.6.12	Robust and flexible security	85

4.6.13	System management	85
4.6.14	Application process using standard objects	86
4.6.15	Tunneling	86
5	System.....	86
5.1	General	86
5.2	Devices	86
5.2.1	General	86
5.2.2	Device interworkability	86
5.2.3	Profiles.....	87
5.2.4	Quality of service	87
5.2.5	Device worldwide applicability	87
5.2.6	Device description	88
5.2.7	Device addressing	92
5.2.8	Device phases	92
5.2.9	Device energy sources.....	94
5.3	Networks	94
5.3.1	General	94
5.3.2	Minimal network.....	94
5.3.3	Basic network topologies supported	95
5.3.4	Network configurations.....	98
5.3.5	Gateway, system manager, and security manager	103
5.4	Protocol suite structure	104
5.5	Data flow	106
5.5.1	General	106
5.5.2	Native communications	106
5.5.3	Basic data flow	106
5.5.4	Data flow between I/O devices	107
5.5.5	Data flow with legacy I/O device.....	107
5.5.6	Data flow with backbone	111
5.5.7	Data flow between I/O devices via backbone	111
5.5.8	Data flow to a standard-aware control system or device.....	111
5.6	Time reference.....	112
5.6.1	General	112
5.6.2	Time synchronization	112
5.7	Firmware upgrades	113
5.8	Wireless backbones and other infrastructures	113
6	System management role	113
6.1	General	113
6.1.1	Overview	113
6.1.2	Components and architecture.....	113
6.1.3	Management functions	115
6.2	DMAP	115
6.2.1	General	115
6.2.2	Architecture of device management.....	115
6.2.3	Definition of management objects.....	116
6.2.4	Management objects in DMAP.....	116
6.2.5	Communications services provided to device management objects	118
6.2.6	Attributes of management objects	119

6.2.7	Definitions of management objects in DMAP	120
6.2.8	Functions of device management and layer management	129
6.3	System manager	139
6.3.1	General	139
6.3.2	System management architecture	139
6.3.3	Standard system management object types	140
6.3.4	Security management	141
6.3.5	Addresses and address allocation	142
6.3.6	Firmware upgrade	146
6.3.7	System performance monitoring	147
6.3.8	Device provisioning service	148
6.3.9	Device management services	148
6.3.10	System time services	157
6.3.11	System communication configuration	160
6.3.12	Redundancy management	193
6.3.13	System management protocols	194
6.3.14	Management policies and policy administration	194
6.3.15	Operational interaction with plant operations or maintenance personnel	194
7	Security	194
7.1	General	194
7.2	Security services	195
7.2.1	Overview	195
7.2.2	Keys	196
7.3	PDU security	200
7.3.1	General	200
7.3.2	DPDU security	201
7.3.3	TL security functionality	217
7.4	Joining process	233
7.4.1	General	233
7.4.2	Prerequisites	233
7.4.3	Desired device end state and properties	233
7.4.4	Joining process steps common for symmetric-key and asymmetric-key approaches	234
7.4.5	Symmetric-key joining process	237
7.4.6	Asymmetric-key joining process	246
7.4.7	Joining process and device lifetime failure recovery	262
7.5	Session establishment	264
7.5.1	General	264
7.5.2	Description	264
7.5.3	Application protocol data unit protection using the master key	266
7.5.4	Proxy security management object methods related to the session establishment	266
7.6	Key update	269
7.6.1	General	269
7.6.2	Description	269
7.6.3	Device security management object methods related to T-key update	270
7.6.4	Failure recovery	274
7.7	Functionality of the security manager role	276
7.7.1	Proxy security management object	276

7.7.2	Authorization of network devices and generation or derivation of initial master keys	276
7.7.3	Interaction with device security management objects	277
7.7.4	Management of operational keys	277
7.8	Security policies	278
7.8.1	Definition of security policy	278
7.8.2	Policy extent	278
7.8.3	Unconstrained security policy choices	278
7.8.4	Policy structures	278
7.9	Security functions available to the AL	281
7.9.1	Parameters on transport service requests that relate to security	281
7.9.2	Direct access to cryptographic primitives	282
7.9.3	Symmetric-key cryptography	283
7.10	Security statistics collection, threat detection, and reporting	284
7.11	DSMO functionality	284
7.11.1	General	284
7.11.2	DSMO attributes	284
7.11.3	KeyDescriptor	286
7.11.4	DSMO alerts	291
8	Physical layer	292
8.1	General	292
8.2	Default physical layer	293
8.2.1	General requirements	293
8.2.2	Additional requirements of IEEE 802.15.4	293
8.2.3	Exceptions to the IEEE 802.15.4 physical layer	294
9	Data-link layer	294
9.1	General	294
9.1.1	Overview	294
9.1.2	Coexistence strategies in the DL	295
9.1.3	Allocation of digital bandwidth	295
9.1.4	Structure of the DPDU	296
9.1.5	The DL and the IEEE 802.15.4 MAC	296
9.1.6	Routes and graphs	297
9.1.7	Slotted-channel-hopping, slow-channel-hopping, and timeslots	304
9.1.8	Superframes	315
9.1.9	DL time keeping	327
9.1.10	D-subnet addressing	346
9.1.11	DL management service	347
9.1.12	Relationship between DLE and DSC	349
9.1.13	DLE neighbor discovery	350
9.1.14	Neighbor discovery and joining – DL considerations	353
9.1.15	Radio link control and quality measurement	358
9.1.16	DLE roles and options	362
9.1.17	DLE energy considerations	363
9.2	DDSAP	364
9.2.1	General	364
9.2.2	DD-DATA.request	364
9.2.3	DD-DATA.confirm	365
9.2.4	DD-DATA.indication	366

9.3	Data DPDU's and ACK/NAK DPDU's	367
9.3.1	General	367
9.3.2	Octet and bit ordering	368
9.3.3	Media access control headers	369
9.3.4	MAC acknowledgment DPDU's.....	375
9.3.5	DL auxiliary subheader.....	378
9.4	DL management information base	393
9.4.1	General	393
9.4.2	DL management object attributes	393
9.4.3	DLMO attributes (indexed OctetStrings).....	413
9.5	DLE methods	441
9.5.1	Method for synchronized cutover of DLE attributes	441
9.5.2	Methods to access indexed OctetString attributes	441
9.6	DL alerts	443
9.6.1	DL_Connectivity alert.....	443
9.6.2	NeighborDiscovery alert	445
10	Network layer	446
10.1	General.....	446
10.2	NL functionality overview.....	446
10.2.1	General	446
10.2.2	Addressing	447
10.2.3	Address translation	447
10.2.4	Network protocol data unit headers	449
10.2.5	Fragmentation and reassembly.....	449
10.2.6	Routing.....	452
10.2.7	Routing examples	458
10.3	NLE data services	466
10.3.1	General	466
10.3.2	N-DATA.request.....	467
10.3.3	N-DATA.confirm	468
10.3.4	N-DATA.indication.....	468
10.4	NL management object.....	469
10.4.1	NL management information base	469
10.4.2	Structured management information bases	473
10.4.3	NL management object methods	474
10.5	NPDU formats.....	477
10.5.1	General	477
10.5.2	Basic header format for NL.....	479
10.5.3	Contract-enabled network header format	480
10.5.4	Full header (IPv6) format.....	482
10.5.5	Fragmentation header format	484
11	Transport layer	485
11.1	General.....	485
11.2	TLE reference model.....	486
11.3	Transport security entity	486
11.3.1	General	486
11.3.2	Securing the TL	486
11.4	Transport data entity	487

11.4.1	General	487
11.4.2	UDP over IPv6	487
11.4.3	UDP header transmission and compression	488
11.4.4	TSAPs and UDP ports	491
11.4.5	Good network citizenship	491
11.5	TPDU encoding	491
11.5.1	General	491
11.5.2	Header compression – User datagram protocol encoding	492
11.5.3	TPDU security header	493
11.6	TL model	493
11.6.1	General	493
11.6.2	Data services	494
12	Application layer	503
12.1	General	503
12.2	Energy considerations	504
12.3	Legacy control system considerations	504
12.4	Overview of object-oriented modeling	505
12.4.1	General	505
12.4.2	Object-to-object communication concept	505
12.4.3	AL structure	505
12.4.4	UAP structure	506
12.5	Object model	507
12.6	Object attribute model	508
12.6.1	General	508
12.6.2	Attributes of standard objects	509
12.6.3	Attribute classification	509
12.6.4	Attribute accessibility	510
12.7	Method model	510
12.8	Alert model	510
12.9	Alarm state model	511
12.10	Event state model	512
12.10.1	General	512
12.10.2	State table and transitions	512
12.11	Alert reporting	513
12.11.1	General	513
12.11.2	Alert types	513
12.11.3	Alert report information	514
12.11.4	Alarm state recovery	514
12.12	Communication interaction model	515
12.12.1	General	515
12.12.2	Buffered unidirectional publication communication	515
12.12.3	Queued unidirectional communication	516
12.12.4	Queued bidirectional communication	516
12.12.5	Communication service contract	524
12.13	AL addressing	525
12.13.1	General	525
12.13.2	Object addressing	525
12.13.3	Object attribute addressing	526

12.13.4	Object attribute addressing	526
12.13.5	Object method addressing.....	528
12.14	Management objects	528
12.15	User objects.....	528
12.15.1	General	528
12.15.2	Industry-independent objects.....	529
12.16	Data types	562
12.16.1	Basic data types	562
12.16.2	Derived atomic data types	562
12.16.3	Industry-independent standard data structures	562
12.17	Application services provided by application sublayer	569
12.17.1	General	569
12.17.2	Publish/subscribe application communication model	570
12.17.3	Scheduled periodic buffered communication	571
12.17.4	Client/server interactions.....	576
12.17.5	Unscheduled acyclic queued unidirectional messages (source/sink).....	592
12.17.6	Client/server and source/sink commonalities.....	599
12.18	AL flow use of lower layer services	605
12.18.1	General	605
12.18.2	AL use of TDSAPs	605
12.18.3	Mapping AL service primitives to TL service primitives	605
12.19	AL management.....	606
12.19.1	General	606
12.19.2	Application sublayer handling of malformed application protocol data units.....	606
12.19.3	Application sublayer management object attributes	607
12.19.4	Application sublayer management object methods	609
12.19.5	Application sublayer management object alerts.....	610
12.19.6	DMAP services invoked by application sublayer.....	611
12.19.7	Process industries standard objects	611
12.19.8	Factory automation industries profile	624
12.20	Process control industry standard data structures	625
12.20.1	General	625
12.20.2	Status for analog information.....	625
12.20.3	Value and status for analog information	626
12.20.4	Value and status for binary information.....	626
12.20.5	Process control mode.....	627
12.20.6	Scaling	628
12.21	Additional tables	628
12.21.1	Process control profile standard objects	628
12.21.2	Services	629
12.22	Coding.....	629
12.22.1	General	629
12.22.2	Coding rules for application protocol data units.....	629
12.22.3	Coding of application data	643
12.22.4	Time-related data types.....	651
12.23	Syntax	654
12.23.1	Application protocol data unit	654
12.23.2	Alert reports and acknowledgments	661
12.23.3	Service feedback code	664

12.23.4	Read, write, and execute	665
12.23.5	Tunnel	666
12.23.6	End of contained module	666
12.24	Detailed coding examples (informative)	666
12.24.1	Read	666
12.24.2	Tunnel	667
13	Provisioning	667
13.1	General	667
13.2	Terms and definitions for devices with various roles or states	667
13.3	Provisioning procedures	670
13.4	Pre-installed symmetric keys	670
13.5	Provisioning using out-of-band mechanisms	671
13.6	Provisioning networks	671
13.6.1	General	671
13.6.2	Provisioning over-the-air using asymmetric cryptography	672
13.6.3	Provisioning over-the-air using an open symmetric join key	673
13.7	State transition diagrams	674
13.8	Device management application protocol objects used during provisioning	678
13.9	Management objects	681
13.9.1	Device provisioning object	681
13.9.2	Device provisioning object methods and alerts	686
13.10	Device provisioning service object	687
13.10.1	Device provisioning service object attributes	687
13.10.2	Device provisioning service object structured attributes	691
13.10.3	Device provisioning service object methods	693
13.10.4	Device provisioning service object alerts	694
13.10.5	Summary of attributes that can be provisioned	695
13.11	Provisioning functions (informative)	695
13.11.1	General	695
13.11.2	Examples of provisioning methods	696
Annex A (informative)	User layer/application profiles	699
A.1	Overview	699
A.2	User layer	699
A.3	Application profile	699
Annex B (normative)	Communication role profiles	701
B.1	Overview	701
B.1.1	General	701
B.1.2	Purpose	701
B.1.3	System size	701
B.1.4	Abbreviations and special symbols	701
B.1.5	Role profiles	701
B.2	System	702
B.3	System manager	702
B.4	Security manager	703
B.5	Physical layer	704
B.6	Data-link layer	704
B.6.1	General	704
B.6.2	Role profiles	705

B.7	Network layer	709
B.8	Transport layer.....	710
B.9	Application layer	710
B.10	Provisioning	711
B.11	Gateway (informative)	711
Annex C (informative) Background information		713
C.1	Industrial needs	713
C.2	Usage classes.....	713
C.2.1	General	713
C.2.2	Class examples.....	714
C.2.3	Other uploading and downloading alarms (human or automated action).....	715
C.3	The Open Systems Interconnection Basic Reference Model	715
C.3.1	Overview	715
C.3.2	Application layer	716
C.3.3	Transport layer	717
C.3.4	Network layer.....	717
C.3.5	Data-link layer	717
C.3.6	Physical layer	717
Annex D (normative) Configuration defaults.....		719
D.1	General.....	719
D.2	System management.....	719
D.3	Security	720
D.4	Data-link layer.....	720
D.5	Network layer.....	722
D.6	Transport layer.....	722
D.7	Application layer	722
D.8	Provisioning	724
D.9	Gateway (informative)	725
Annex E (informative) Use of backbone networks		726
E.1	General.....	726
E.2	Recommended characteristics	726
E.3	Internet protocol backbones	726
E.3.1	Methods of IPv6 protocol data unit transmission	726
E.3.2	Backbone router peer device discovery	727
E.3.3	Security	727
Annex F (normative) Basic security concepts – Notation and representation.....		728
F.1	Strings and string operations	728
F.2	Integers, octets, and their representation	728
F.3	Entities	728
Annex G (informative) Using certificate chains for over-the-air provisioning.....		729
Annex H (normative) Security building blocks		730
H.1	Symmetric key cryptographic building blocks	730
H.1.1	Overview	730
H.1.2	Symmetric key domain parameters	730
H.1.3	Block cipher.....	730
H.1.4	Mode of operation	730
H.1.5	Cryptographic hash function	730
H.1.6	Keyed hash function for message authentication.....	730

H.1.7	Specialized keyed hash function for message authentication	731
H.1.8	Challenge domain parameters	731
H.2	Asymmetric-key cryptographic building blocks	731
H.2.1	General	731
H.2.2	Elliptic curve domain parameters	731
H.2.3	Elliptic curve point representation	731
H.2.4	Elliptic curve public-key pair	731
H.3	Keying information	731
H.3.1	General	731
H.3.2	Elliptic curve cryptography implicit certificates	731
H.3.3	Elliptic curve cryptography manual certificates	732
H.3.4	Additional information	732
H.4	Key agreement schemes	733
H.4.1	Symmetric-key key agreement scheme	733
H.4.2	Asymmetric-key key agreement scheme	733
H.5	Keying information schemes	733
H.5.1	Implicit certificate scheme	733
H.5.2	Manual certificate scheme	734
H.6	Challenge domain parameter generation and validation	734
H.6.1	Overview	734
H.6.2	Challenge domain parameter generation	734
H.6.3	Challenge domain parameter verification	734
H.7	Challenge validation primitive	735
H.8	Secret key generation (SKG) primitive	735
H.9	Block-cipher-based cryptographic hash function	736
H.10	Elliptic curve cryptography manual certificate scheme	737
H.10.1	Overview	737
H.10.2	Elliptic curve cryptography manual certificate generation transformation	738
H.10.3	Elliptic curve cryptography manual certificate processing transformation	738
Annex I (informative)	Definition templates	740
I.1	Object type template	740
I.2	Standard object attributes template	740
I.3	Standard object methods	741
I.4	Standard object alert reporting template	742
I.5	Data structure definition	743
Annex J (informative)	Operations on attributes	745
J.1	Operations on attributes	745
J.1.1	General	745
J.1.2	Attribute classification	745
J.1.3	Retrieving, setting, and resetting attributes	745
J.1.4	Retrieving and setting structured attributes	746
J.1.5	Resetting structured attribute values	748
J.1.6	Deleting structured attribute values	748
J.2	Synchronized cutover	749
Annex K (normative)	Standard object types	750
Annex L (informative)	Standard data types	755
Annex M (normative)	Identification of tunneled legacy fieldbus protocols	757
Annex N (informative)	Tunneling and native object mapping	758