

DIN EN ISO 16484-5

ICS 35.240.99; 91.140.01

Entwurf

Einsprüche bis 2014-04-14
Vorgesehen als Ersatz für
DIN EN ISO 16484-5:2012-11;
Ersatz für
E DIN EN ISO 16484-5:2013-09

**Systeme der Gebäudeautomation –
Teil 5: Datenkommunikationsprotokoll (ISO/FDIS 16484-5:2013);
Englische Fassung FprEN ISO 16484-5:2013, nur auf CD-ROM**

Building automation and control systems –
Part 5: Data communication protocol (ISO/FDIS 16484-5:2013);
English version FprEN ISO 16484-5:2013, only on CD-ROM

Systèmes d'automatisation et de gestion technique du bâtiment –
Partie 5: Protocole de communication de données (ISO/FDIS 16484-5:2013);
Version anglaise FprEN ISO 16484-5:2013, seulement en CD-ROM

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2014-02-14 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

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

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal des DIN unter www.entwuerfe.din.de bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an nhrs@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/stellungnahme oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den Normenausschuss Heiz- und Raumluftechnik (NHRS) im DIN, 10772 Berlin (Hausanschrift: Burggrafenstr. 6, 10787 Berlin).

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

Gesamtumfang 1100 Seiten

Normenausschuss Heiz- und Raumluftechnik (NHRS) im DIN
DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE

Nationales Vorwort

Dieses Dokument (FprEN ISO 16484-5:2013) wurde vom Technischen Komitee ISO/TC 205 „Building environment design“ in Zusammenarbeit mit dem Technischen Komitee CEN/TC 247 „Gebäudeautomation und Gebäudemanagement“ (Sekretariat: SNV, Schweiz) unter Beteiligung deutscher Experten erarbeitet.

Das zuständige deutsche Gremium ist der Arbeitsausschuss NA 041-03-68 AA „Gebäudeautomation und -kommunikation (SpA CEN/TC 247/WG 4)“ im Normenausschuss Heiz- und Raumlufttechnik (NHRS).

Dieses Dokument (FprEN ISO 16484-5:2013) übernimmt den englischen Originaltext des ANSI/ASHRAE Standard 135 „BACnet — A Data Communication Protocol for Building Automation and Control Networks“, Ausgabe 2012. In derselben Weise sollen zwischenzeitlich veröffentlichte bzw. noch zu veröffentlichende Änderungen und Erweiterungen von ANSI/ASHRAE Standard 135 bei der Fortschreibung von EN ISO 16484-5 übernommen werden. Der Inhalt dieses Dokumentes befindet sich auf der beiliegenden CD-ROM.

Der NHRS war für das DIN Deutsches Institut für Normung e. V. an der Erstellung dieser Norm beteiligt. Da davon auszugehen ist, dass die Fachleute der Kommunikationstechnik sich bereits mit der englischen Fassung befasst haben, wurde von einer Übersetzung ins Deutsche abgesehen. Nach dem DIN-Präsidialbeschluss 13/1983 ist insbesondere auf dem Gebiet der Informatik die Veröffentlichung in Englisch zulässig, insbesondere wenn dadurch Fehler bei der Übertragung vermieden werden können.

Dieses Dokument (FprEN ISO 16484-5:2013) stellt ein Kommunikationsverfahren zur Verfügung, mit dem Geräte der Gebäudeautomation untereinander Informationen austauschen können, unabhängig von der gebäudetechnischen Anlage, zu der sie gehören. Das in dieser Norm spezifizierte Protokoll kann universell für den Datenaustausch von Geräten und Systemen in der Gebäudeautomation sowohl zum allgemeinen Einsatz, als auch für anwenderspezifische Lösungen eingesetzt werden.

Für die in diesem Dokument zitierten Internationalen Normen wird im Folgenden auf die entsprechenden Deutschen Normen hingewiesen:

ISO/IEC 9545 siehe DIN ISO/IEC 9545

Änderungen

Gegenüber DIN EN ISO 16484-5:2012-11 wurden folgende Änderungen vorgenommen:

- a) Inhalt technisch überarbeitet.

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN ISO/IEC 9545, *Informationstechnik — Kommunikation Offener Systeme — Struktur der Anwendungsschicht*

Nationaler Anhang NB (informativ)

Begriffe

Im Folgenden wird ISO 16484-5:2013, Abschnitt 3 ins Deutsche übersetzt. Die Benennung der folgenden Begriffe und Abkürzungen ist identisch mit der Benennung in der englischen Fassung.

3 Begriffe und Abkürzungen

Für die Anwendung dieses Dokuments gelten die folgenden aus Internationalen Normen übernommenen bzw. für die vorliegende Norm definierten Begriffe.

ANMERKUNG Die folgenden in dieser Norm verwendeten Begriffe sind in Internationalen Normen bzw. Norm-Entwürfen zur Kommunikation offener Systeme (open system interconnection, OSI) definiert. Diese Definitionen sind an dieser Stelle unter Verweisung auf die entsprechende Norm erneut aufgeführt. Abschnitt 25 enthält die Titel aller im vorliegenden Abschnitt und an weiteren Stellen in dieser Norm genannten nationalen und Internationalen Normen. Kursiv dargestellte Wörter oder Wortgruppen beziehen sich auf Begriffe, die an anderer Stelle im vorliegenden Abschnitt definiert sind.

3.1

abstrakte Syntax

(en: abstract syntax)

Festlegung von Daten der Anwendungsschicht oder von *Anwendungsprotokoll-Steuerinformationen* durch Anwendung von Notationsregeln, die von der zu ihrer Darstellung verwendeten Kodierungstechnik unabhängig sind

[ISO 8822]

3.2

Anwendung

(en: application)

Menge von Informationsverarbeitungsanforderungen eines *Benutzers*

[ISO 8649]

3.3

Anwendungsentität

(en: application-entity)

die OSI betreffenden Aspekte eines *Anwendungsprozesses*

[ISO 7498]

3.4

Anwendungsprozess

(en: application-process)

Element innerhalb eines *realen offenen Systems*, das die Informationsverarbeitung für eine bestimmte *Anwendung* durchführt

[ISO 7498]

3.5**Anwendungsprotokoll-Steuerinformationen**

(en: application-protocol-control-information)

Informationen, die mit Hilfe von Darstellungsdiensten zwischen *Anwendungsentitäten* ausgetauscht werden, um deren gemeinsame Operation zu koordinieren

[ISO 9545]

3.6**Anwendungsprotokoll-Dateneinheit**

(en: application-protocol-data-unit)

in einem Anwendungsprotokoll festgelegte Dateneinheit, die aus *Anwendungsprotokoll-Steuerinformationen* (3.5) und eventuell Anwendungsbenutzerdaten besteht

[ISO 9545]

3.7**Anwendungsdienstelement**

(en: application-service-element)

Teil einer *Anwendungsentität* (3.3), der eine OSI-Umgebungsfähigkeit bereitstellt, gegebenenfalls unter Verwendung zugrunde liegender Dienste

[ISO 7498]

3.8**konkrete Syntax**

(en: concrete syntax)

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

[ISO 7498]

3.9**Bestätigung (primitiv)**

(en: confirm (primitive))

Darstellung einer Interaktion, bei der ein *Dienstanbieter* an einem bestimmten *Dienstzugangspunkt* anzeigt, dass er eine Prozedur abgeschlossen hat, die an diesem *Dienstzugangspunkt* zuvor durch eine durch ein *Anforderungsprimitiv* dargestellte Interaktion aufgerufen wurde

[ISO/TR 8509]

3.10**Anzeige (primitiv)**

(en: indication (primitive))

Darstellung einer Interaktion, bei der ein *Dienstanbieter* entweder

- a) anzeigt, dass er auf eigene Veranlassung hin eine Prozedur aufgerufen hat oder
- b) anzeigt, dass eine Prozedur vom *Dienstbenutzer* am gleichrangigen *Dienstzugangspunkt* aufgerufen wurde

[ISO TR 8509]

3.11**Peer-Entitäten**

(en: peer-entities)

Entitäten innerhalb derselben Schicht

[ISO 7498]

3. 12**reales offenes System**

(en: real open system)

reales System, das bei seiner Kommunikation mit anderen *realen Systemen* die Anforderungen von OSI-Normen einhält

[ISO 7498]

3. 13**reales System**

(en: real system)

Satz von einem oder mehreren Rechnern, der dazugehörigen Software, Peripheriegeräten, Endgeräten, menschlichen Bedienern, physikalischen Prozessen, Informationsübertragungsmitteln usw., der ein autonomes Ganzes bildet, das in der Lage ist, Informationsverarbeitung und/oder Informationstransfer durchzuführen

[ISO 7498]

3. 14**Anforderung(primitiv)**

(en: request (primitive))

Darstellung einer Interaktion, bei der ein *Dienstbenutzer* eine Prozedur aufruft

[ISO/TR 8509]

3. 15**Antwort (primitiv)**

(en: response (primitive))

Darstellung einer Interaktion, bei der ein *Dienstbenutzer* anzeigt, dass er eine Prozedur abgeschlossen hat, die zuvor durch eine durch ein *Anzeigeprimitiv* dargestellte Interaktion aufgerufen wurde

[ISO/TR 8509]

3. 16**(N)-Dienstzugangspunkt**

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

Punkt, an dem (N)-Dienste von einer (N)-*Entität* für eine (N+1)-*Entität* bereitgestellt werden

[ISO 7498]

3. 17**(N)-Dienstdateneinheit**

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

Menge von (N)-Schnittstellendaten, deren Identität vom einen Ende einer (N)-Verbindung bis zum anderen gewahrt bleibt

[ISO 7498]

3.18**Dienstbenutzer**

(en: service-user)

Entität in einem einzelnen offenen System, die über *Dienstzugangspunkte* einen Dienst benutzt

[ISO/TR 8509]

3. 19

Dienstprimitiv; Primitiv

(en: service-primitive; primitive)

abstrakte, implementierungsunabhängige Darstellung einer Interaktion zwischen dem *Dienstbenutzer* und dem *Dienstanbieter*

[ISO/TR 8509]

3. 20

Dienstanbieter

(en: service-provider)

Abstraktum der Gesamtheit der Entitäten, die gleichrangigen *Dienstbenutzern* einen Dienst bereitstellen

[ISO TR 8509]

3. 21

Transfersyntax

(en: transfer syntax)

bei der Übertragung von Daten zwischen offenen Systemen verwendete *konkrete Syntax*

[ISO 7498]

3. 22

Benutzerelement

(en: user element)

Darstellung des Teils eines *Anwendungsprozesses*, der die zur Erreichung der Kommunikationsziele dieses *Anwendungsprozesses* notwendigen *Anwendungsdienstelemente* nutzt

[ISO 7498]

3.23

Zugriffskontrolle

(en: access control)

Verfahren zur Regelung oder Einschränkung des Zugriffs auf *Netzwerkressourcen*

3.24

Zugriffsrechte (physische Zugangskontrolle)

(en: access rights (physical access control))

Zugriffsrechte, die auf Anmeldedaten gewährt werden

3.25

Zugreifender Benutzer (physische Zugangskontrolle)

(en: access user (physical access control))

Person oder Inhalt, welche/welcher ein oder mehrere Anmeldeinformationen hat

3.26

Alarm

(en: alarm)

hörbare und/oder sichtbare Meldung, die einen Bediener auf einen nicht normalen Zustand, der eine Korrekturmaßnahme erfordern kann, aufmerksam macht

3.27

Alarm

von einem Gerät oder Controller erkannter nicht normaler Zustand, wobei das Gerät bzw. der Controller eine speziell für diesen Zustand ausgelegte Regel oder Logik implementiert

3.28

Alarm-Bestätigung

Verfahren, das anzeigt, dass ein Bediener eine Ereignisbenachrichtigung gesehen und auf diese reagiert hat

3.29**Algorithmic Change Reporting**

(en: algorithmic change reporting)

Erkennen und Berichten eines Alarms oder Ereignisses auf der Grundlage eines in einem Event-Enrollment-Objekt festgelegten Algorithmus

Anmerkung 1 zum Begriff: Siehe auch *Intrinsic Reporting* unter 3.70

3.30**Authentifizierung**

(en: authentication)

Vorgang zur Verifizierung der Identität

3.31**Authentifizierungs-Faktor**

(en: authentication factor)

Datenelement der Anmeldeinformationen, das verwendet wird, um die Identität des Anmeldenden zu verifizieren

3.32**Autorisierung (Netzwerksicherheit)**

(en: authorization (network security))

Kontrolle des Zugangs zu Netzwerkressourcen basierend auf Identitätsprüfung und Zugriffsregeln

3.33**Autorisierung (physische Zugangskontrolle)**

(en: authorization (physical access control))

Prozess zur Bestimmung, ob es für den Anwender zulässig ist, einen geschützten Bereich über einen zugangskontrollierten Punkt zu betreten

3.34**BACnet-Gerät**

(en: BACnet device)

jedes reale oder virtuelle Gerät, das eine digitale Kommunikation unter Anwendung des BACnet-Protokolls unterstützt

3.35**BACnet-Benutzer**

(en: BACnet-user)

Teil eines *Anwendungsprozesses*, der durch das *BACnet-Benutzerelement* repräsentiert wird

3.36**Warnblinklicht**

(en: blink-warn)

Verfahren zur Benachrichtigung der Raumnutzer vor einem bevorstehenden automatisierten Befehl das Licht auszuschalten, die Lichter können dabei einmal oder mehrmals blinken oder ein akustisches Signal wird erzeugt

Anmerkung 1 zum Begriff: Nachdem die Warnung auftritt, bleibt die Raumbeleuchtung für einen Übergangszeitraum aktiv um Raumnutzern zu erlauben den Raum zu verlassen oder eine Anfrage (3.14) zu initiieren, um die Raumbeleuchtung aktiviert zu lassen.

3.37**Bridge**

(en: bridge)

Einrichtung, die zwei oder mehr *Segmente* auf der physikalischen Schicht und der Daten Verbindungsschicht miteinander verbindet

Anmerkung 1 zum Begriff: Diese Einrichtung kann auf der Grundlage von MAC-Schicht-Adressen auch Nachrichten filtern.

3.38

Broadcast

(en: broadcast)

als einzelne Einheit gesendete Nachricht, die sich an mehr als ein Gerät richten kann

3.39

Zustandsänderung

(en: change of state)

Ereignis, das dann auftritt, wenn sich ein gemessener oder berechneter Boolescher Wert oder ein diskreter numerischer bzw. Zählwert ändert

3.40

Wertänderung

(en: change of value)

Ereignis, das dann auftritt, wenn sich ein Messwert oder ein berechneter Analogwert um einen definierten Wert ändert

3.41

Client

(en: client)

System oder Einrichtung, das/die eine andere Einrichtung für einen bestimmten Zweck über eine *Dienstanforderungsinstanz* einsetzt

Anmerkung 1 zum Begriff: Ein Client fordert einen Dienst bei einem *Server* an.

3.42

konfigurierbar

(en: configurable)

Eigenschaft, Einstellung oder Wert in einem Gerät ist konfigurierbar, wenn er/sie über BACnet-Dienste oder ein anderes Verfahren geändert werden kann

Anmerkung 1 zum Begriff: Eine Eigenschaft, Einstellung, oder ein Wert, die/der nur einmal beschreibbar oder in situ nicht veränderbar ist, wird nicht als konfigurierbar betrachtet-

3.43

Kontext

(en: context)

Satz von Daten oder Informationen, der eine bestimmte Kommunikationsumgebung zu einem bestimmten Zeitpunkt vollständig beschreibt

3.44

Controller

(en: controller)

Einrichtung zur Regelung bzw. zum Management eines Systems oder einer Komponente

3.45

Anmeldeinformationen (physische Zugangskontrolle)

(en: credentials (physical access control))

Kombination aus Authentifizierungs-Faktoren und Zugangsrechten

3.46

Vertraulichkeit von Daten

(en: data confidentiality)

Eigenschaft, dass Informationen unbefugten Personen, Entitäten oder Prozessen nicht zur Verfügung gestellt oder offengelegt werden

3.47**Datenintegrität**

(en: data integrity)

Eigenschaft, dass Daten nicht auf nicht autorisierte Weise verändert oder zerstört wurden

3.48**Authentifizierung der Datenherkunft**

(en: data origin authentication)

Bestätigung, dass die Quelle der empfangenen Daten tatsächlich den Angaben entspricht

3.49**Datumsmuster**

(en: date pattern)

Datum, das eine oder mehrere nicht spezifische Oktette oder spezielle Datumswerte enthalten kann

3.50**direkt verbundenes Netzwerk**

(en: directly connected network)

Netzwerk, das von einem Router aus zugänglich ist, ohne dass Nachrichten über einen Zwischenrouter weitergeleitet werden müssen

Anmerkung 1 zum Begriff: Zu einem direkt verbundenen Netzwerk besteht eine PTP-Verbindung, wenn die PTP-Verbindung gerade aktiv ist und kein Zwischenrouter verwendet wird

3.51**Download**

Herunterladen

(en: download)

bestimmte Art der Dateiübertragung, die sich auf die Übertragung eines ausführbaren Programms oder einer Datenbank auf ein abgesetztes Gerät bezieht, auf dem die Datei ausgeführt werden kann

3.52**verschlüsselte Nachricht**

(en: encrypted message)

Nachricht, die in einen Security Header eingehüllt, signiert, und verschlüsselt ist

3.53**Entität**

Gebilde

(en: entity)

eigenständiger, sich unterscheidender Gegenstand der Betrachtung. Ein identifizierbares Element, das mittels einer Sammlung oder eines Satzes von Eigenschaften beschrieben wird

3.54**Fehlererkennung**

(en: error detection)

Prozedur, die dazu verwendet wird, das Vorhandensein von Fehlern in einer Kommunikation zu identifizieren

3.55**Fehlerbehebung**

(en: error recovery)

Prozedur, die als Reaktion auf einen erkannten Fehler aufgerufen wird und ein Fortsetzen des Informationsaustausches erlaubt

3.56**Ereignis-Algorithmus**

(en: event algorithm)

Regeln, die bestimmen, wann ein ereignis-initiierendes Objekt zwischen normalen und offnormal Status wechselt

Anmerkung 1 zum Begriff: Der Ereignis-Algorithmus hat keine Auswirkungen auf den Übergang eines ereignis-initiierenden Objektes zu oder von einem Fehler.

3.57

ereignis-initiierendes Objekt

(en: event-initiating object)

Objekt, das so konfiguriert ist, seinen Ereignis-Zustand zu überwachen und Änderungen seines Ereignis-Zustandes zu melden

3.58

Ereignis-Benachrichtigungs-Verteilung

(en: event-notification-distribution)

Prozess, den ein Benachrichtigung-Server bei der Bestimmung der Notification-Clients und der Zusendung von Benachrichtigungen an Notification-Clients durchführt, wenn ein ereignis-initiierendes Objekt das Ereignis oder den Anerkennungs-Zustand (en: acknowledgment state) wechselt

3.59

Ereignisbenachrichtigung

(en: event notification message)

ConfirmedEventNotification oder UnconfirmedEventNotification Dienstanforderung, die dazu verwendet wird, um eine Veränderung des Ereignisses oder des Anerkennungs-Zustandes eines ereignis-initiierenden Objektes anzuzeigen

3.60

Ereignisstatus-Feststellung

(en: event-state-detection)

Prozess der Ausführung des Ereignis-Algorithmus eines ereignis-initiierenden Objektes und die Überwachung der Zuverlässigkeitseigenschaft des Objektes um Veränderungen des Ereignis-Zustands des Objektes zu erfassen

3.61

Ereigniszusammenfassung

(en: event-summarization)

Abfrage von ereignis-initiierenden Objekten in einem Gerät durch einen der Ereigniszusammenfassungs-Dienste um diejenigen zu bestimmen, die bestimmte Ereignis-Zustand- oder Berichterstattungs-Bedingungen erfüllen

3.62

Fading

(en: fading)

allmähliche Erhöhung oder Verringerung der tatsächlichen Ausgabe von einer Einstellung in eine andere über einen bestimmten Zeitraum

3.63

Gateway

Netzübertragungseinheit

(en: gateway)

Einrichtung zur Verbindung zweier oder mehrerer nicht gleicher *Netzwerke*, um den Informationsaustausch zwischen diesen Netzwerken zu ermöglichen

3.64

global

(en: global)

alle Geräte oder Knoten auf einem *Inter-Netzwerk* betreffend

3.65

globales Broadcast

(en: global broadcast)

an alle Geräte oder *Knoten* auf allen Netzwerken in einem BACnet-*Internet* adressierte Nachricht

3.66**Halbrouter**

(en: half router)

Gerät oder *Knoten*, der als ein Partner an einer PTP-Verbindung teilnehmen kann

Anmerkung 1 zum Begriff: Die beiden Halbrouter-Partner, die zusammen eine aktive PTP-Verbindung bilden, ergeben einen einzelnen *Router*.

3.67**unfähiges Gerät**

(en: incapable device)

Gerät, das von Natur aus unfähig ist oder konfiguriert wurde, unfähig zu erscheinen, sichere BACnet Nachrichten zu produzieren oder zu verarbeiten

Anmerkung 1 zum Begriff: Alle unfähigen Geräte sind einfache Geräte.

3.68**Initialisierung**

(en: initialization)

Vorgang des Herbeiführens eines bekannten Zustands, üblicherweise nach einer Stromanschaltung. Die Initialisierung kann eine Wiedereingabe der logischen oder physikalischen Adresse eines Knotens erfordern

3.69**Inter-Netzwerk**

Verbindungsnetzwerk

(en: internetwork)

Verbindung von zwei oder mehreren *Netzwerken* über *Router*

Anmerkung 1 zum Begriff: In einem BACnet-*Inter-Netzwerk* gibt es zwischen zwei beliebigen Knoten genau einen Nachrichtenweg.

3.70**Intrinsic Reporting**

(en: intrinsic reporting)

Erkennen und Berichten eines Alarms oder Ereignisses auf der Grundlage eines als Teil der *Objektyp*-Spezifikation definierten Algorithmus

Anmerkung 1 zum Begriff: Dabei findet keine externe Verweisung auf ein „Event Enrollment“ statt

Anmerkung 2 zum Begriff: Siehe auch *Algorithmic Change Reporting* unter 3.29

3.71**invertiertes Netzwerk**

(en: inverted network)

BACnet Inter-Netzwerk, bei dem zwei oder mehr Netzwerke durch ein Netzwerk verbunden sind, dessen NPDU kleiner als die des beitretenden Netzwerkes ist

3.72**Schlüssel**

(en: key)

Symbolsequenz zur Regelung der Chiffrierung und Dechiffrierung

3.73**lokal**

(en: local)

Geräte auf demselben *Netzwerk* wie das betrachtete Gerät betreffend

3.74

lokales Broadcast

(en: local broadcast)

Nachricht, die an alle Geräte oder *Knoten* adressiert ist, die sich auf demselben *Netzwerk* wie die Nachrichtenquelle befinden

3.75

Medium

(en: medium)

physikalische Übertragungsentität. Typische Medien sind verdrehte Doppelader-Leitungen, Faseroptik-Kabel und Koaxialkabel

3.76

Medienzugriffskontrolle

(en: medium access control)

Vorgang zur Wahrung der Ordnung und zur Gewährung des Zugriffs auf das Kommunikationsmedium

3.77

Netzwerk

(en: network)

Satz von einem oder mehreren durch *Bridges* verbundenen *Segmenten* mit derselben Netzwerkadresse

3.78

Netzwerkressource

(en: network resource)

jede physikalische oder logische *Entität*, auf die über ein Kommunikationsmedium zugegriffen werden kann

3.79

Knoten

(en: node)

mit dem Kommunikationsmedium verbundene adressierbare Einrichtung

3.80

Notification-Client

(en: notification-client)

BACnet-Gerät, das Ereignisbenachrichtigungen empfängt und verarbeitet

3.81

Benachrichtigungsserver

(en: notification-server)

BACnet-Gerät, das ereignis-initiiierende Objekte enthält und die Verteilung von Ereignisbenachrichtigungen durchführt

3.82

Objekt

(en: object)

spezifische Instanz eines *Objektyps*

Anmerkung 1 zum Begriff: Während ein Objekttyp durch eine eindeutige *Object_Type*-Eigenschaft bezeichnet ist, ist ein Objekt durch seine *Object_Identifier*-Eigenschaft bezeichnet

3.83

Objektprofil

(en: object profile)

Mittel zum Definieren von Objekten über die in Abschnitt 12 definierten Objekte hinaus

Anmerkung 1 zum Begriff: Ein Profil definiert den Satz von Eigenschaften, Verhalten und/oder Anforderungen, der für ein proprietäres Objekt oder proprietäre Erweiterungen eines Normobjekts gilt

3.84**Objekttyp**

Objektart

(en: object type)

generische Datenklassifizierung, definiert durch einen Satz *Eigenschaften***3.85****Bediener-Authentifizierung**

(en: operator authentication)

Bestätigung der Identität des sich an einer Einrichtung anmeldenden Bedieners

3.86**Authentifizierung der Peer-Entität**

(en: peer entity authentication)

die Bestätigung der Identität einer assoziierten Peer-Entität

3.87**physische Zugangskontrolle (PACS)**

(en: physical access control (PACS))

elektronisches System, das durch Authentifizierung und Autorisierung an Zugangskontrollpunkten die Fähigkeit von Personen und Fahrzeugen, einen geschützten Bereich zu betreten, kontrolliert

3.88**physikalisches Segment**

(en: physical segment)

einzelnes zusammenhängendes *Medium*, an das BACnet-Knoten angebunden sind**3.89****physisch unsicher**

(en: physically insecure)

nicht physisch sicher

3.90**physisch sicher**

(en: physically secure)

Gerät oder Netzwerk, das vor physischem Zugang nicht autorisierter Individuen geschützt ist

3.91**einfaches Gerät**

(en: plain device)

Gerät, das normalerweise keine sicheren BACnet-Nachrichten erzeugt oder verarbeitet

Anmerkung 1 zum Begriff: Alle unfähigen Geräte sind einfache Geräte. Ein einfaches Gerät, das kein unfähiges Gerät ist, ist fähig, sichere BACnet-Nachrichten zu erzeugen und zu verarbeiten, wenn die Kommunikation mit einem anderen Gerät dies erfordert.

3.92**einfaches Netzwerk**

(en: plain network)

Netzwerk, das keinen signierten oder verschlüsselten Datenverkehr benötigt

3.93**einfache Nachricht**

(en: plain message)

Nachricht, die nicht durch einen BACnet Security Wrapper geschützt ist

3.94**druckbares Zeichen**

(en: printable character)

Zeichen, das im Gegensatz zu einem Gerätesteuerzeichen ein druckbares Symbol darstellt. Dazu gehören unter anderem Groß- und Kleinbuchstaben, Satzzeichen und mathematische Symbole.

Anmerkung 1 zum Begriff: Der genaue Satz hängt von dem verwendeten Zeichensatz ab.

3.95**Eigenschaft**

(en: property)

spezielles Charakteristikum eines *Objektyps*

3.96**proprietär**

herstellerspezifisch

(en: proprietary)

im BACnet-Kontext jede Erweiterung oder Ergänzung der in dieser Norm festgelegten *Objektypen*, *Eigenschaften*, PrivateTransfer-Diensten oder Aufzählungen

3.97**Ramping**

(en: ramping)

allmähliche Zunahme oder Abnahme des tatsächlichen Ausgangs von einer Einstellung zur anderen mit einer festen Veränderungsrate

3.98**empfangender BACnet-Benutzer**

(en: receiving BACnet-user)

der *BACnet-Benutzer*, der ein *Anzeige-* oder *Bestätigungs-*Dienstprimitiv empfängt

3.99**abgesetzt**

Fern-

(en: remote)

Geräte oder *Knoten* betreffend, die sich auf einem anderen Netzwerk als das referenzierte Gerät befinden

3.100**Fern-Broadcast**

(en: remote broadcast)

Nachricht, die an alle Geräte oder *Knoten* adressiert ist, die sich auf einem anderen *Netzwerk* als die Nachrichtenquelle befinden

3.101**Repeater**

Verstärker

(en: repeater)

Einrichtung, die zwei oder mehr *physikalische Segmente* auf der physikalischen Schicht verbindet

3.102**anfordernder BACnet-Benutzer**

(en: requesting BACnet-user)

BACnet-Benutzer, der in einem bestätigten Dienst die Rolle eines *Clients* übernimmt

3.103**antwortender BACnet-Benutzer**

(en: responding BACnet-user)

BACnet-Benutzer, der in einem bestätigten Dienst die Rolle eines *Servers* übernimmt

3.104**Funktionsgruppenbasierte Zugangskontrolle (RBAC)**

(en: role-based access control)

Zugangsrechte, die spezifischen Funktionsgruppen zugewiesen sind

Anmerkung 1 zum Begriff: Der Nutzer erhält die Zugangsrechte über die ihm zugewiesene Funktionsgruppe.

3.105**Router**

Wegwahleinheit

(en: router)

Gerät zur Verbindung eines oder mehrerer *Netzwerke* auf der Vermittlungsschicht**3.106****sicheres Netzwerk**

(en: secure network)

Netzwerk, in dem sämtlicher Datenverkehr signiert oder verschlüsselt sein muss

3.107**Sicherheit**

Schutz

(en: security)

eine von einer Vielzahl von Vorgehensweisen zur Sicherstellung der Überwachung des Informationsaustausches, um einer Offenlegung gegenüber unbefugten Personen vorzubeugen

Anmerkung 1 zum Begriff: Sicherheitsmaßnahmen sollen die Offenlegung sensibler Informationen auch gegenüber jenen verhindern, die einen gültigen Zugriff auf das Kommunikations*netzwerk* haben.

Anmerkung 2 zum Begriff: Sicherheit unterscheidet sich von Zugriffskontrolle, wenngleich auch durch die Einschränkung des physischen Zugriffs auf das Kommunikationsmedium selbst ein gewisses Maß an Sicherheit erreicht werden kann.

3.108**Segment**

(en: segment)

Segment besteht aus einem oder mehreren miteinander über Repeater verbundenen *physikalischen Segment(en)***3.109****sendender BACnet-Benutzer**

(en: sending BACnet-user)

BACnet-Benutzer, der ein *Anforderungs-* oder *Antwort-Dienst*primitiv ausgibt**3.110****Server**

(en: server)

System oder Einrichtung bzw. Gerät, das (die) für einen bestimmten Zweck auf eine Dienstanforderungsinstanz antwortet

Anmerkung 1 zum Begriff: Der Server stellt einen Dienst für einen *Client* bereit.

3.111**signierte Nachricht**

(en: signed message)

Nachricht, die in einen Security Header eingehüllt, signiert, und nicht verschlüsselt ist

3.112

spezieller Datumswert

(en: special date value)

Datumswert, der einem speziellen Wert wie z. B. „gerade Monate“, „letzter Tag des Monats“ usw. entspricht

Anmerkung 1 zum Begriff: Diese speziellen Datumswerte werden in Unterkomponenten (Oktetten) eines Datumswertes verwendet.

3.113

spezifisches Datum

(en: specific date)

vollständig spezifiziertes Datum

BEISPIEL Januar 24, 1991, Wochentag = Donnerstag.

Anmerkung 1 zum Begriff: Es darf das keine nicht spezifischen Oktette oder spezielle Datumswerte enthalten.

3.114

spezifische Datumszeit

(en: specific datetime)

BACnetDateTime-Konstrukt zusammengesetzt aus einem spezifischen Datum und einer spezifischen Zeit

3.115

spezifische Zeit

(en: specific time)

vollständig spezifizierte Zeit

BEISPIEL 17:35:45,17 (= 5:35:45,17 P. M.).

Anmerkung 1 zum Begriff: Darf keine nicht spezifischen Oktette enthalten.

3.116

Standard-Objektyp

(en: standard object type)

durch diese Norm definierter Objektyp, bei dem der numerische Wert im für ASHRAE reservierten Bereich liegt

3.117

Standard-Eigenschaft

(en: standard property)

erforderliche oder optionale Eigenschaft eines Standard-Objektyps, bei der der numerische Wert der Eigenschaftskennung im für ASHRAE reservierten Bereich liegt und die Eigenschaft in der Objektyp-Eigenschafts Tabelle in Abschnitt 12 aufgeführt ist

3.118

Staffelung

(en: stepping)

Zunahme oder Abnahme eines Ausgangswertes in diskreten Schritten

3.119

Synchronisierung

(en: synchronization)

Möglichkeit für Prozesse, bestimmte Stellen in einer Übertragung oder einem Austausch zu definieren und zu identifizieren, die genutzt werden können, um eine Kommunikationssitzung in einen vordefinierten Zustand zurückzusetzen

3.120**Zeitmuster**

(en: time pattern)

Zeit, die ein oder mehrere nicht spezifizierte Oktette enthalten kann

3.121**Zeitstempel**

(en: timestamp)

einem Ereignis oder einer Handlung zugeordneter Eintrag über Datum und Uhrzeit

3.122**vertrauenswürdig**

(en: trusted)

Begriff, der für Geräte oder Netzwerke angewendet wird, deren Nachrichten für authentisch gehalten werden, entweder durch die Verwendung von sicheren Nachrichten oder basierend auf der physischen Sicherheit des Gerätes oder Netzwerkes

3.123**Zeiteinheit**

(en: unit_time)

Länge der Zeit, die erforderlich ist, um ein Oktett mit einem Startbit und einem einzigen Stoppbit zu senden. Zehn Bitintervalle

3.124**nicht spezifiziertes Datum**

(en: unspecified date)

Datum, das ausschließlich aus nicht spezifizierten Oktetten besteht

Anmerkung 1 zum Begriff: Ein Wert von X'FF' = D'255'.

3.125**nicht spezifizierte Datumszeit**

(en: unspecified datetime)

BACnetDateTime Konstrukt zusammengesetzt aus einem nicht spezifizierten Datum und einer nicht spezifizierten Zeit

3.126**nicht spezifiziertes Oktett**

(en: unspecified octet)

Oktett, das im Zusammenhang mit Datum, Zeit oder BACnetWeekNDay Werten verwendet wird und den Wert X'FF' = D'255' beinhaltet

3.127**nicht spezifizierte Zeit**

(en: unspecified time)

Zeit, die ausschließlich aus nicht spezifizierten Oktetten besteht

Anmerkung 1 zum Begriff: Ein Wert von X'FF' = D'255'.

3.128**Upload**

Hochladen

(en: upload)

Prozess, ein Abbild eines ausführbaren Programms oder eine Datenbank von einer abgesetzten Einrichtung so zu übertragen, dass ein anschließender Download erfolgen kann

Abkürzungen in der vorliegenden Norm

Abkürzung (englisch)	Bedeutung (englisch)	Bedeutung (deutsch)
A	application layer	Anwendungsschicht (Präfix)
ABA	American Bankers Association	American Bankers Association
AE	application entity	Anwendungsentität
ANSI	American National Standards Institute	American National Standards Institute
APCI	application protocol control information	Anwendungsprotokoll-Steuerinformationen
APDU	application layer protocol data unit	Protokolldateneinheit der Anwendungsschicht
API	application program interface	Anwendungsprogramm-Schnittstelle
ARCNET	attached resource computer network	Attached Resource Computer Network
ASE	application service element	Anwendungsdienstelement
ASN.1	Abstract Syntax Notation One	Notation Eins für Abstrakte Syntax (ISO 8824)
B' '	denotes that binary notation is used between the single quotes	gibt an, dass zwischen den Anführungszeichen eine Binärschreibweise verwendet wird
BAC	building automation and control	Gebäudeautomation (GA)
BBMD	BACnet/IP broadcast management device	Einrichtung für das BACnet/IP-Broadcast-Management
BDT	broadcast distribution table	Broadcast-Verteilungstabelle
B/IP	BACnet/IP	BACnet/IP
B/IP-M	BACnet/IP multicast	BACnet/IP-Multicast
BVLC	BACnet virtual link control	virtuelle Verbindungsteuerung von BACnet
BVLCI	BACnet virtual link control information	Steuerinformationen der virtuellen Verbindung von BACnet
BVLL	BACnet virtual link layer	virtuelle Verbindungsschicht von BACnet
C	conditional	bedingt
C(=)	conditional (The parameter is semantically equivalent to the parameter in the service primitive to its immediate left in the table.)	bedingt (Der Parameter entspricht semantisch dem Parameter in dem Dienstprimitiv unmittelbar zu seiner Linken in der Tabelle.)
CNF	confirm primitive	Bestätigungsprimitiv
COV	change of value	Wertänderung
CRC	cyclic redundancy check	zyklische Redundanzprüfung
D' '	denotes that decimal notation is used between the single quotes	gibt an, dass zwischen den Anführungszeichen eine Dezimalschreibweise verwendet wird
DA	local destination MAC layer address	MAC-Schicht-Adresse des lokalen Ziels
DADR	ultimate destination MAC layer address	MAC-Schicht-Adresse des endgültigen Ziels

Abkürzung (englisch)	Bedeutung (englisch)	Bedeutung (deutsch)
DER	data expecting reply	Daten erwarten Antwort
DES	Data Encryption Standard (FIPS 46-1)	Datenverschlüsselungsstandard (FIPS 46-1)
DESFire	Data Encryption Standard Fast, Innovative, Reliable and Secure	Datenverschlüsselungsstandard Schnell, Innovativ, Zuverlässig und Sicher
DID	ARCNET destination MAC address	MAC-Adresse des ARCNET-Ziels
DLEN	1-octet length of ultimate destination MAC layer address	1-Oktett-Länge der MAC-Schicht-Adresse des endgültigen Ziels
DNET	2-octet length of ultimate destination MAC layer address	2-Oktett-Länge der MAC-Schicht-Adresse des endgültigen Ziels
DSAP	LLC destination service access point (X'82' for BACnet)	Dienstzugangspunkt des LLC-Ziels (X'82' für BACnet)
EIB	European Installation Bus	Europäischer Installationsbus
EIBA	European Installation Bus Association	European Installation Bus Association
EXEC	capable of executing a service request	fähig, eine Dienstanforderung auszuführen (execute)
FDT	foreign device table	Fremdgerätetabelle
ICI	interface control information	Schnittstellensteuerinformation
IL	ARCNET information length field	ARCNET-Feld Informationslänge
IND	indication primitive	Anzeigeprimitiv
INF	„Infinity“, a unique binary pattern representing positive infinity (see ANSI/IEEE 754-1985)	„Unendlich“, ein eindeutiges Binärmuster, das positiv unendlich darstellt (siehe ANSI/IEEE 754-1985)
-INF	„Negative infinity“, a unique binary pattern representing negative infinity (see ANSI/IEEE 754-1985)	„Negativ unendlich“, ein eindeutiges Binärmuster, das negativ unendlich darstellt (siehe ANSI/IEEE 754-1985)
IEEE	Institute of Electrical and Electronics Engineers	Institute of Electrical and Electronics Engineers
INIT	capable of initiating a service request	fähig, eine Dienstanforderung einzuleiten (initiate)
IP	Internet Protocol – RFC 791	Internet-Protokoll – RFC 791
ISO	International Organization for Standardization	Internationale Organisation für Normung
KNX	Konnex System Specification: EIB is the core protocol of the Konnex standard. The Konnex System Specification reflects the current status for EIB.	Konnex-System-Spezifikation: EIB ist das Kernprotokoll des Konnex-Standards. Die Konnex-System-Spezifikation spiegelt den derzeitigen Stand für EIB wider.
L	data link (prefix)	Datenverbindung (Präfix)
LAN	local area network	Local Area Network
LLC	logical link control (ISO 8802-2)	logische Verbindungssteuerung
LPCI	link protocol control information	Verbindungsprotokoll-Steuerinformation

Abkürzung (englisch)	Bedeutung (englisch)	Bedeutung (deutsch)
LPDU	link protocol data unit	Verbindungsprotokoll-Dateneinheit
LRC	Longitudinal Redundancy Check	Longitudinale Redundanzprüfung
LSAP	link service access point (X'82' for BACnet)	Verbindungsdienstzugriffspunkt (X'82' für BACnet)
LSDU	link service data unit	Verbindungsdienstdateneinheit
M	mandatory	verpflichtend
M(=)	mandatory (The parameter is semantically equivalent to the parameter in the service primitive to its immediate left in the table.)	verpflichtend (Der Parameter entspricht semantisch dem Parameter in dem Dienstprimitiv unmittelbar zu seiner Linken in der Tabelle.)
MA	medium access (prefix)	Medienzugriff (Präfix)
MAC	medium access control	Medienzugriffskontrolle
MPCI	MAC protocol control information	MAC-Protokollsteuerinformation
MPDU	MAC layer protocol data unit	MAC-Schicht-Protokolldateneinheit
MSDU	MAC service data unit	MAC-Dienstdateneinheit
MS/TP	master-slave/token-passing	Master-Slave/Token-Passing
N	network layer (prefix)	Vermittlungsschicht (Präfix)
NaN	„Not a Number“, a unique binary pattern representing an invalid number (see ANSI/IEEE 754-1985)	„Keine Zahl“, ein eindeutiges Binärmuster, das eine ungültige Zahl darstellt (siehe ANSI/IEEE 754-1985)
NAT	Network Address Translation – RFC 2663	Network Address Translation – RFC 2663
NP	network priority	Netzwerkpriorität
NPCI	network protocol control information	Netzwerkprotokoll-Steuerinformationen
NPDU	network layer protocol data unit	Vermittlungsschicht-Protokolldateneinheit
NRZ	non-return to zero	Non-Return-To-Zero
NSAP	network service access point	Netzwerkdienstzugriffspunkt
NSDU	network service data unit	Netzwerkdienstdateneinheit
O	indicates that support of a property is optional	gibt an, dass die Unterstützung einer Eigenschaft optional ist
OSI	open systems interconnection	Kommunikation offener Systeme
P	physical layer (prefix)	physikalische Schicht (Präfix)
PAC	ARCNET data packet header octet	Oktett des ARCNET-Datenpaket-Headers
PCI	protocol control information	Protokollsteuerinformation
PDU	protocol data unit	Protokolldateneinheit
PICS	protocol implementation conformance statement	Konformitätserklärung zur Protokollimplementierung
PK	Private Key	privater Schlüssel
PPCI	physical layer protocol control	Protokollsteuerinformationen der

Abkürzung (englisch)	Bedeutung (englisch)	Bedeutung (deutsch)
	information	physikalischen Schicht
PPDU	physical protocol data unit	physikalische Protokolldateneinheit
PPP	Point-To-Point protocol – RFC 1661	Punkt-zu-Punkt-Protokoll – RFC 1661
PSDU	physical service data unit	physikalische Dienstdateneinheit
PTP	point-to-point	Punkt-zu-Punkt
R	indicates that a property shall be supported and readable using BACnet services	gibt an, dass eine Eigenschaft unterstützt werden und lesbar (readable) sein muss
REQ	request primitive	Anforderungsprimitiv
RFC	request for comment	Request for Comment
RSP	response primitive	Antwortprimitiv
S	selection	Auswahl
S(=)	selection (The parameter is semantically equivalent to the parameter in the service primitive to its immediate left in the table.)	Auswahl (Der Parameter entspricht semantisch dem Parameter in dem Dienstprimitiv unmittelbar zu seiner Linken in der Tabelle.)
SA	local network source MAC layer address	MAC-Schicht-Adresse der lokalen Netzwerkquelle
SAP	service access point	Dienstzugangspunkt
SC	ARCNET system code (X'CD' for BACnet)	ARCNET-Systemcode (X'CD' für BACnet)
SDU	service data unit	Dienstdateneinheit
SIA	Security Industry Association	Security Industry Association
SID	ARCNET source MAC address	MAC-Adresse der ARCNET-Quelle
SK	Session Key	Sitzungsschlüssel
SLEN	1-octet length of original source MAC layer address	1-Oktett-Länge der MAC-Schicht-Adresse der ursprünglichen Quelle
SLIP	Serial Line Internet Protocol	Serial Line Internet Protocol (RFC 1055)
SNET	2-octet original source network number	2-Oktett-Netzwerknummer der ursprünglichen Quelle
SPC	standard project committee	ASHRAE-Ausschuss für Normungsvorhaben
SSAP	LLC source service access point (X'82' for BACnet)	LLC-Quellen-Dienstzugangspunkt (X'82' für BACnet)
TSM	transaction state machine	Transaktionszustandsmaschine
U	user option	Benutzeroption
U(=)	user option (The parameter is semantically equivalent to the parameter in the service primitive to its immediate left in the table.)	Benutzeroption (Der Parameter entspricht semantisch dem Parameter in dem Dienstprimitiv unmittelbar zu seiner Linken in der Tabelle.)
UART	universal asynchronous receiver/transmitter	Universeller Asynchron-Empfänger/-Sender

Abkürzung (englisch)	Bedeutung (englisch)	Bedeutung (deutsch)
UDP	User Datagram Protocol – RFC 768	User Datagram Protocol – RFC 768
UTC	Universal Time Coordinated	Koordinierte Weltzeit
VT	virtual terminal	virtuelles Terminal
W	indicates that a property shall be supported, readable, and writable using BACnet services	gibt an, dass eine Eigenschaft unterstützt werden und lesbar und schreibbar (writable) sein muss
X'	denotes that hexadecimal notation is used between the single quotes	gibt an, dass zwischen den Anführungszeichen eine Hexadezimalschreibweise verwendet wird
XID	eXchange IDentification (ISO 8802-2)	Exchange Identification (ISO 8802-2)

Contents

Page

Foreword	x
Introduction	xi
1 Scope	1
2 Relationship between this part of ISO 16484 and ANSI/ASHRAE 135-2012	1
3 Terms, definitions and abbreviated terms	2
4 BACnet PROTOCOL ARCHITECTURE	20
4.1 The BACnet Collapsed Architecture	21
4.2 BACnet Network Topology	23
4.3 Security	25
5 THE APPLICATION LAYER	26
5.1 The Application Layer Model	26
5.2 Segmentation of BACnet Messages	30
5.3 Transmission of BACnet APDUs	32
5.4 Application Protocol State Machines	36
5.5 Application Protocol Time Sequence Diagrams	53
5.6 Application Layer Service Conventions	61
6 THE NETWORK LAYER	63
6.1 Network Layer Service Specification	63
6.2 Network Layer PDU Structure	65
6.3 Messages for Multiple Recipients	71
6.4 Network Layer Protocol Messages	71
6.5 Network Layer Procedures	75
6.6 BACnet Routers	76
6.7 Point-To-Point Half-Routers	81
7 DATA LINK/PHYSICAL LAYERS: ISO 8802-3 ("Ethernet") LAN	86
7.1 The Use of ISO 8802-2 Logical Link Control (LLC)	86
7.2 Parameters Required by the LLC Primitives	86
7.3 Parameters Required by the MAC Primitives	86
7.4 Physical Media	86
8 DATA LINK/PHYSICAL LAYERS: ARCNET LAN	87
8.1 The Use of ISO 8802-2 Logical Link Control (LLC)	87
8.2 Parameters Required by the LLC Primitives	87
8.3 Mapping the LLC Services to the ARCNET MAC Layer	87
8.4 Parameters Required by the MAC Primitives	87
8.5 Physical Media	87
9 DATA LINK/PHYSICAL LAYERS: MASTER-SLAVE/TOKEN PASSING (MS/TP) LAN	89
9.1 Service Specification	89
9.2 Physical Layer	91
9.3 MS/TP Frame Format	102
9.4 Overview of the MS/TP Network	104
9.5 MS/TP Medium Access Control	104
9.6 Cyclic Redundancy Check (CRC)	121
9.7 Interfacing MS/TP LANs with Other BACnet LANs	122
9.8 Responding BACnet User Processing of Messages from MS/TP	122
9.9 Repeaters	123
10 DATA LINK/PHYSICAL LAYERS: POINT-TO-POINT (PTP)	125
10.1 Overview	125
10.2 Service Specification	125
10.3 Point-to-Point Frame Format	130

10.4	PTP Medium Access Control Protocol	132
11	DATA LINK/PHYSICAL LAYERS: EIA/CEA-709.1 ("LonTalk") LAN	154
11.1	The Use of ISO 8802-2 Logical Link Control (LLC)	154
11.2	Parameters Required by the LLC Primitives	154
11.3	Mapping the LLC Services to the LonTalk Application Layer	154
11.4	Parameters Required by the Application Layer Primitives	154
11.5	Physical Media	155
12	MODELING CONTROL DEVICES AS A COLLECTION OF OBJECTS	156
12.1	Accumulator Object Type	160
12.2	Analog Input Object Type	169
12.3	Analog Output Object Type	174
12.4	Analog Value Object Type	179
12.5	Averaging Object Type	184
12.6	Binary Input Object Type	187
12.7	Binary Output Object Type	193
12.8	Binary Value Object Type	200
12.9	Calendar Object Type	206
12.10	Command Object Type	208
12.11	Device Object Type	212
12.12	Event Enrollment Object Type	221
12.13	File Object Type	229
12.14	Group Object Type	232
12.15	Life Safety Point Object Type	234
12.16	Life Safety Zone Object Type	241
12.17	Loop Object Type	248
12.18	Multi-state Input Object Type	257
12.19	Multi-state Output Object Type	262
12.20	Multi-state Value Object Type	267
12.21	Notification Class Object Type	272
12.22	Program Object Type	275
12.23	Pulse Converter Object Type	281
12.24	Schedule Object Type	289
12.25	Trend Log Object Type	295
12.26	Access Door Object Type	304
12.27	Event Log Object Type	312
12.28	Load Control Object Type	319
12.29	Structured View Object Type	329
12.30	Trend Log Multiple Object Type	332
12.31	Access Point Object Type	341
12.32	Access Zone Object Type	358
12.33	Access User Object Type	366
12.34	Access Rights Object Type	369
12.35	Access Credential Object Type	375
12.36	Credential Data Input Object Type	384
12.37	CharacterString Value Object Type	389
12.38	DateTime Value Object Type	394
12.39	Large Analog Value Object Type	397
12.40	BitString Value Object Type	403
12.41	OctetString Value Object Type	408
12.42	Time Value Object Type	411
12.43	Integer Value Object Type	414
12.44	Positive Integer Value Object Type	420
12.45	Date Value Object Type	426
12.46	DateTimePattern Value Object Type	429
12.47	Time Pattern Value Object Type	432

12.48	Date Pattern Value Object Type	435
12.49	Network Security Object Type	438
12.50	Global Group Object Type	441
12.51	Notification Forwarder Object Type.....	448
12.52	Alert Enrollment Object Type	456
12.53	Channel Object Type	459
12.54	Lighting Output Object Type.....	468
13	ALARM AND EVENT SERVICES	482
13.1	Change of Value Reporting	483
13.2	Event Reporting	486
13.3	Event Algorithms.....	498
13.4	Fault Algorithms.....	527
13.5	AcknowledgeAlarm Service.....	532
13.6	ConfirmedCOVNotification Service	534
13.7	UnconfirmedCOVNotification Service	535
13.8	ConfirmedEventNotification Service	537
13.9	UnconfirmedEventNotification Service.....	540
13.10	GetAlarmSummary Service.....	542
13.11	GetEnrollmentSummary Service	544
13.12	GetEventInformation Service	547
13.13	LifeSafetyOperation Service.....	549
13.14	SubscribeCOV Service	551
13.15	SubscribeCOVProperty Service	554
14	FILE ACCESS SERVICES	557
14.1	AtomicReadFile Service	558
14.2	AtomicWriteFile Service	561
15	OBJECT ACCESS SERVICES	564
15.1	AddListElement Service	564
15.2	RemoveListElement Service	566
15.3	CreateObject Service	568
15.4	DeleteObject Service	571
15.5	ReadProperty Service	572
15.6	Deleted Clause	574
15.7	ReadPropertyMultiple Service.....	575
15.8	ReadRange Service.....	578
15.9	WriteProperty Service	583
15.10	WritePropertyMultiple Service.....	585
15.11	WriteGroup Service	588
16	REMOTE DEVICE MANAGEMENT SERVICES.....	590
16.1	DeviceCommunicationControl Service	590
16.2	ConfirmedPrivateTransfer Service	592
16.3	UnconfirmedPrivateTransfer Service	594
16.4	ReinitializeDevice Service.....	595
16.5	ConfirmedTextMessage Service.....	597
16.6	UnconfirmedTextMessage Service.....	599
16.7	TimeSynchronization Service.....	600
16.8	UTCTimeSynchronization Service.....	601
16.9	Who-Has and I-Have Services.....	602
16.10	Who-Is and I-Am Services	604
17	VIRTUAL TERMINAL SERVICES	606
17.1	Virtual Terminal Model.....	606
17.2	VT-Open Service	610
17.3	VT-Close Service	612
17.4	VT-Data Service	613
17.5	Default-terminal Characteristics	615

18	ERROR, REJECT, and ABORT CODES	619
18.1	Error Class - DEVICE	619
18.2	Error Class - OBJECT	619
18.3	Error Class - PROPERTY	620
18.4	Error Class - RESOURCES	621
18.5	Error Class - SECURITY	622
18.6	Error Class - SERVICES	623
18.7	Error Class - COMMUNICATION	624
18.8	Error Class - VT	626
18.9	Reject Reason	627
18.10	Abort Reason	628
18.11	Confirmed Service Common Errors	628
19	BACnet PROCEDURES	629
19.1	Backup and Restore	629
19.2	Command Prioritization	633
19.3	Device Restart Procedure	637
20	ENCODING BACnet PROTOCOL DATA UNITS	638
20.1	Encoding the Fixed Part of BACnet APDUs	638
20.2	Encoding the Variable Part of BACnet APDUs	650
21	FORMAL DESCRIPTION OF APPLICATION PROTOCOL DATA UNITS	665
22	CONFORMANCE AND INTEROPERABILITY	742
22.1	Conformance to BACnet	742
22.2	BACnet Interoperability	743
23	EXTENDING BACnet TO ACCOMMODATE VENDOR PROPRIETARY INFORMATION	745
23.1	Extending Enumeration Values	745
23.2	Using the PrivateTransfer Services to Invoke Non-Standardized Services	746
23.3	Adding Proprietary Properties to a Standardized Object	746
23.4	Adding Proprietary Object Types to BACnet	747
23.5	Restrictions on Extending BACnet	747
24	NETWORK SECURITY	748
24.1	Overview	748
24.2	Security Wrapper	752
24.3	Security Messages	757
24.4	Securing an APDU	773
24.5	Securing an NPDU	775
24.6	Securing a BVLL	775
24.7	Securing Messages	777
24.8	Network Security Network Trust Levels	780
24.9	Network Security Policies	780
24.10	Network Security	781
24.11	End-to-End Security	782
24.12	Wrapping and Unwrapping Secure Messages	782
24.13	Authenticating Messages	784
24.14	User Authentication	787
24.15	Time Synchronization Requirements	788
24.16	Integrating the Security Layer into the BACnet Stack	789
24.17	BACnet Security In A NAT Environment	796
24.18	BACnet Security Proxy	796
24.19	Deploying Secure Device on Non-Security Aware Networks	796
24.20	Deploying Secure Single Network Installations	797
24.21	Security Keys	797
24.22	Key Server	798
25	REFERENCES	802
	ANNEX A - PROTOCOL IMPLEMENTATION CONFORMANCE STATEMENT (NORMATIVE)	805
	ANNEX B - GUIDE TO SPECIFYING BACnet DEVICES (INFORMATIVE)	808

ANNEX C - Removed	809
ANNEX D - Removed	810
ANNEX E - EXAMPLES OF BACnet APPLICATION SERVICES (INFORMATIVE)	811
E.1 Alarm and Event Services	811
E.2 File Access Services	815
E.3 Object Access Services	817
E.4 Remote Device Management Services	823
E.5 Virtual Terminal Services	826
ANNEX F - EXAMPLES OF APDU ENCODING (INFORMATIVE)	828
F.1 Example Encodings for Alarm and Event Services	828
F.2 Example Encodings for File Access Services	838
F.3 Example Encodings for Object Access Services	840
F.4 Example Encodings for Remote Device Management Services	850
F.5 Example Encodings for Virtual Terminal Services	855
ANNEX G - CALCULATION OF CRC (INFORMATIVE)	858
G.1 Calculation of the Header CRC	858
G.2 Calculation of the Data CRC	864
ANNEX H - COMBINING BACnet NETWORKS WITH NON-BACnet NETWORKS (NORMATIVE)	869
H.1 Mapping Non-BACnet Networks onto BACnet Routers	869
H.2 Multiple "Virtual" BACnet Devices in a Single Physical Device	869
H.3 Using BACnet with the DARPA Internet Protocols	869
H.4 Using BACnet with the IPX Protocol	870
H.5 Using BACnet with EIB/KNX	873
H.6 Using BACnet with the BACnet/WS Web Services Interface (Annex N)	885
H.7 Virtual MAC Addressing	887
ANNEX I - COMMANDABLE PROPERTIES WITH MINIMUM ON AND OFF TIMES (INFORMATIVE)	888
ANNEX J - BACnet/IP (NORMATIVE)	890
J.1 General	890
J.2 BACnet Virtual Link Layer	890
J.3 BACnet/IP Directed Messages	894
J.4 BACnet/IP Broadcast Messages	894
J.5 Addition of Foreign B/IP Devices to an Existing B/IP Network	897
J.6 Routing Between B/IP and non-B/IP BACnet Networks	898
J.7 Routing Between Two B/IP BACnet Networks	900
J.8 Use of IP Multicast within BACnet/IP	905
J.9 Sources for Internet Information	906
ANNEX K - BACnet INTEROPERABILITY BUILDING BLOCKS (BIBBs) (NORMATIVE)	907
K.1 Data Sharing BIBBs	907
K.2 Alarm and Event Management BIBBs	915
K.3 Scheduling BIBBs	923
K.4 Trending BIBBs	926
K.5 Device and Network Management BIBBs	931
ANNEX L - DESCRIPTIONS AND PROFILES OF STANDARDIZED BACnet DEVICES (NORMATIVE)	940
L.1 Operator Interfaces	940
L.2 BACnet Building Controller (B-BC)	942
L.3 BACnet Advanced Application Controller (B-AAC)	942
L.4 BACnet Application Specific Controller (B-ASC)	943
L.5 BACnet Smart Actuator (B-SA)	943
L.6 BACnet Smart Sensor (B-SS)	944
L.7 Profiles of the Standard BACnet Devices	945
ANNEX M - GUIDE TO EVENT NOTIFICATION PRIORITY ASSIGNMENTS (INFORMATIVE)	946
ANNEX N - BACnet/WS WEB SERVICES INTERFACE (NORMATIVE)	951
N.1 Data Model	951
N.2 Paths	952
N.3 Normalized Points	952

N.4 Reference Nodes	953
N.5 Localization.....	953
N.6 Security	954
N.7 Sessions.....	954
N.8 Attributes.....	954
N.9 Standard Nodes	961
N.10 Encodings.....	961
N.11 Service Options	963
N.12 Services	965
N.13 Errors.....	984
N.14 Extending BACnet/WS	985
ANNEX O - BACnet OVER ZigBee AS A DATA LINK LAYER (NORMATIVE).....	986
O.1 General	986
O.2 ZigBee Overview	986
O.3 Definitions.....	987
O.4 Unicast Addressing	987
O.5 Broadcast Addressing.....	987
O.6 BACnet/ZigBee Data Link Layer (BZLL)	988
O.7 Maximum Payload Size	991
O.8 Vendor Specific Commands.....	992
ANNEX P-BACnetENCODING OF STANDARD AUTHENTICATION FACTOR FORMATS(NORMATIVE).....	993
ANNEX Q - XML DATA FORMATS (NORMATIVE)	1000
Q.1 Introduction	1000
Q.2 Document Structure	1003
Q.3 Expressing BACnet Datatypes in XML	1004
Q.4 Expressing BACnet Objects and Properties in XML	1040
Q.5 Definitions, Types, Instances, and Inheritance.....	1040
Q.7 Extensibility	1047
ANNEX R - MAPPING NETWORK LAYER ERRORS (NORMATIVE).....	1051
ANNEX S - EXAMPLES OF SECURE BACnet MESSAGES (INFORMATIVE)	1053

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2. www.iso.org/directives

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received. www.iso.org/patents

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: [Foreword - Supplementary information](#)

The committee responsible for this document is ISO/TC 205, *Building environment design*.

This fifth edition cancels and replaces the fourth edition (ISO 16484-5:2012), of which it forms the subject of a minor revision.

ISO 16484 consists of the following parts, under the general title *Building automation and control systems (BACS) — Data communication conformance testing*:

- *Part 1: Project specification and implementation*
- *Part 2: Hardware*
- *Part 3: Functions*
- *Part 5: Data communication protocol*
- *Part 6: Data communication conformance testing*

Applications and project implementation are to form the subjects of future Parts 4 and 7.

Introduction

BACnet, the ASHRAE building automation and control networking protocol, has been designed specifically to meet the communication needs of building automation and control systems for applications such as heating, ventilating, and air-conditioning control, lighting control, access control, and fire detection systems. The BACnet protocol provides mechanisms by which computerized equipment of arbitrary function may exchange information, regardless of the particular building service it performs. As a result, the BACnet protocol may be used by head-end computers, general-purpose direct digital controllers, and application specific or unitary controllers with equal effect.

The motivation for this standard was the widespread desire of building owners and operators for "interoperability," the ability to integrate equipment from different vendors into a coherent automation and control system — and to do so competitively. To accomplish this, the Standard Project Committee (SPC) solicited and received input from dozens of interested firms and individuals; reviewed all relevant national and international data communications standards, whether de facto or the result of committee activity; and spent countless hours in debate and discussion of the pros and cons of each element of the protocol.

What has emerged from the committee deliberations is a network protocol model with these principal characteristics:

- a) All network devices (except MS/TP slaves) are peers, but certain peers may have greater privileges and responsibilities than others.
- b) Each network device is modeled as a collection of network-accessible, named entities called "objects." Each object is characterized by a set of attributes or "properties." While this Standard prescribes the most widely applicable object types and their properties, implementors are free to create additional object types if desired. Because the object model can be easily extended, it provides a way for BACnet to evolve in a backward compatible manner as the technology and building needs change.
- c) Communication is accomplished by reading and writing the properties of particular objects and by the mutually acceptable execution of other protocol "services." While this Standard prescribes a comprehensive set of services, mechanisms are also provided for implementors to create additional services if desired.
- d) Because of this standard's adherence to the ISO concept of a "layered" communication architecture, the same messages may be exchanged using various network access methods and physical media. This means that BACnet networks may be configured to meet a range of speed and throughput requirements with commensurately varying cost. Multiple BACnet networks can be interconnected within the same system forming an internetwork of arbitrarily large size. This flexibility also provides a way for BACnet to embrace new networking technologies as they are developed.

BACnet was designed to gracefully improve and evolve as both computer technology and demands of building automation systems change. Upon its original publication in 1995, a Standing Standards Project Committee was formed to deliberate enhancements to the protocol under ASHRAE rules for "continuous maintenance." Much has happened since the BACnet standard was first promulgated. BACnet has been translated into Chinese, Japanese, and Korean, and embraced across the globe. BACnet devices have been designed, built and deployed on all seven continents. Suggestions for enhancements and improvements have been continually received, deliberated, and, ultimately, subjected to the same consensus process that

produced the original standard. This publication is the result of those deliberations and brings together all of the corrections, refinements, and improvements that have been adopted.

Among the features that have been added to BACnet are: increased capabilities to interconnect systems across wide area networks using Internet Protocols, new objects and services to support fire detection and other life safety applications, capabilities to backup and restore devices, standard ways to collect trend data, new tools to make specifying BACnet systems easier, a mechanism for making interoperable extensions to the standard visible, and many others. The successful addition of these features demonstrates that the concept of a protocol deliberately crafted to permit extension of its capabilities over time as technology and needs change is viable and sound.

All communication protocols are, in the end, a collection of arbitrary solutions to the problems of information exchange and all are subject to change as time and technology advance. BACnet is no exception. Still, it is the hope of those who have contributed their time, energies, and talents to this work that BACnet will help to fulfill, in the area of building automation and control, the promise of the information age for the public good!

Building automation and control systems (BACS) — Part 5: Data communication protocol

1 Scope

This part of ISO 16484 defines data communication services and protocols for computer equipment used for monitoring and control of heating, ventilation, air-conditioning and refrigeration (HVAC&R) and other building systems. It defines, in addition, an abstract, object-oriented representation of information communicated between such equipment, thereby facilitating the application and use of digital control technology in buildings.

This part of ISO 16484 provides a comprehensive set of messages for conveying encoded binary, analog, and alphanumeric data between devices including, but not limited to,

- a) hardware binary input and output values,
- b) hardware analog input and output values,
- c) software binary and analog values,
- d) text string values,
- e) schedule information,
- f) alarm and event information,
- g) files, and
- h) control logic.

It models each building automation and control computer as a collection of data structures called "objects," the properties of which represent various aspects of the hardware, software, and operation of the device. These objects provide a means of identifying and accessing information without requiring knowledge of the details of the device's internal design or configuration.

2 Relationship between this part of ISO 16484 and ANSI/ASHRAE 135-2012

This part of ISO 16484 comprises, from Clause 4 onwards, the US standard ANSI/ASHRAE 135-2012, *A Data Communication Protocol for Building Automation and Control Networks* (BACnet), published by the American National Standards Institute and the American Society of Heating, Refrigerating and Air-Conditioning Engineers.

3 Terms, definitions and abbreviated terms

For the purposes of this document, the following terms, definitions and abbreviated terms apply.

NOTE Terms and definitions from International Standards for open system interconnection (OSI) are reproduced here with a reference to their source. See Clause 25 for all national and International Standards referenced in this clause and elsewhere in the document.

3.1
abstract syntax
specification of application layer data or *application-protocol-control-information* (3.5) by using notation rules which are independent of the encoding technique used to represent them

[SOURCE: ISO 8822]

3.2
application
set of a USER's information processing requirements

[SOURCE: ISO 8649]

3.3
application-entity
aspects of an *application-process* (3.4) pertinent to OSI

[SOURCE: ISO 7498]

3.4
application-process
element within a *real open system* (3.12) which performs the information processing for a particular *application*

[SOURCE: ISO 7498]

3.5
application-protocol-control-information
information exchanged between *application-entities* (3.3), using presentation services, to coordinate their joint operation

[SOURCE: ISO 9545]

3.6
application-protocol-data-unit
unit of data specified in an application protocol and consisting of *application-protocol-control-information* (3.5) and possibly application-user-data

[SOURCE: ISO 9545]

3.7
application-service-element

that part of an *application-entity* (3.3) which provides an OSI environment capability, using underlying services when appropriate

[SOURCE: ISO 7498]

3.8

concrete syntax

those aspects of the rules used in the formal specification of data which embody a specific representation of that data

[SOURCE: ISO 7498]

3.9

confirm

<primitive>representation of an interaction in which a *service-provider* (3.20) indicates, at a particular *service-access-point* (3.16), completion of some procedure previously invoked, at that service-access-point, by an interaction represented by a *request* (3.14) primitive

[SOURCE: ISO/TR 8509]

3.10

indication

<primitive>representation of an interaction in which a *service-provider* (3.20) either

- a) indicates that it has, on its own initiative, invoked some procedure, or
- b) indicates that a procedure has been invoked by the *service-user* (3.18) at the peer *service-access-point* (3.16)

[SOURCE: ISO TR 8509]

3.11

peer-entities

entities (3.55) within the same layer

[SOURCE: ISO 7498]

3.12

real open system

real system (3.13) which complies with the requirements of OSI standards in its communication with other real systems

[SOURCE: ISO 7498]

3.13

real system

set of one or more computers, the associated software, peripherals, terminals, human operators, physical processes, information transfer means, etc., that forms an autonomous whole capable of performing information processing and/or information transfer

[SOURCE: ISO 7498]

3.14
request

<primitive>representation of an interaction in which a *service-user* (3.18) invokes some procedure

[SOURCE: ISO/TR 8509]

3.15
response

<primitive>representation of an interaction in which a *service-user* (3.18) indicates that it has completed some procedure previously invoked by an interaction represented by an *indication* (3.10) primitive

[SOURCE: ISO/TR 8509]

3.16
(N)-service-access-point

point at which (N)-services are provided by an (N)-*entity* (3.55) to an (N+1)-entity

[SOURCE: ISO 7498].

3.17
(N)-service-data-unit

amount of (N)-interface-data whose identity is preserved from one end of an (N)-connection to the other

[SOURCE: ISO 7498]

3.18
service-user

entity (3.55) in a single open system that makes use of a service through *service-access-points* (3.16)

[SOURCE: ISO TR 8509]

3.19
service-primitive
primitive

abstract, implementation-independent representation of an interaction between the *service-user* (3.18) and the *service-provider* (3.20)

[SOURCE: ISO TR 8509]

3.20
service-provider

abstract of the totality of those entities which provide a service to peer *service-users* (3.18)

[SOURCE: ISO/TR 8509]

3.21
transfer-syntax

concrete syntax (3.8) used in the transfer of data between open systems

[SOURCE: ISO 7498]

3.22

user element

representation of that part of an *application-process* (3.4) which uses those *application-service-elements* (3.7) needed to accomplish the communications objectives of that application-process

[SOURCE: ISO 7498]

3.23

access control

method for regulating or restricting access to *network resources* (3.80)

3.24

access rights

<physical access control> access privileges granted to a credential

3.25

access user

<physical access control> person or asset holding one or more credentials

3.26

alarm

annunciation, either audible or visual or both, that alerts an operator to an off-normal condition that may require corrective action

3.27

alarm

abnormal condition detected by a device or controller that implements a rule or logic specifically designed to look for that condition

3.30

alarm-acknowledgment

process of indicating that a human operator has seen and responded to an event notification

3.31

algorithmic change reporting

detection and reporting of an alarm or event, based on an algorithm specified in an Event Enrollment object

Note 1 to entry: See *intrinsic reporting* (3.72).

3.32

authentication

act of verifying identity

3.33

authentication factor

data element of the credential which is used to verify a credential's identity

3.34

authorization

<network security>control of access to network resources based on known identity and access rules

3.35

authorization

<physical access control> process of determining whether the access user is permitted to enter a protected zone through an access controlled point

3.36

BACnet device

any device, real or virtual, that supports digital communication using the BACnet protocol

3.37

BACnet-user

portion of an *application-process* (3.4) that is represented by the *BACnet user element* (3.22)

3.38

blink-warn

flick warn

flash warn

<lighting control> method of notifying room occupants of an impending automated command to turn off the lights whereby the lights may be blinked, once or multiple times, or an audible signal is generated

Note 1 to entry: After the warning occurs, the room lights are held on for a grace period to allow occupants to either safely leave the room or to initiate a *request* (3.14) to keep the room lights on.

3.39

bridge

device that connects two or more *segments* (3.111) at the physical and data link layers

Note 1 to entry: This device may also perform message filtering based upon MAC layer addresses.

3.40

broadcast

message sent as a single unit, which may apply to more than one device

3.41

change of state

event that occurs when a measured or calculated Boolean or discrete enumerated value changes

3.42

change of value

event that occurs when a measured or calculated analog value changes by a predefined amount

3.43

client

system or device that makes use of another device for some particular purpose via a service *request* instance

Note 1 to entry: A client requests service from a *server* (3.113).

3.44

configurable

capability of property, setting, or value in a device to be changed via BACnet services or some other method

Note 1 to entry: A property, setting, or value that is one-time writable or not changeable *in situ* is not considered to be configurable.

3.45

context

set of data or information that completely describes a particular communication environment at a particular point in time

3.46

controller

device for regulation or management of a system or component

3.47

credential

<physical access control> combination of authentication factors and access rights

3.48

data confidentiality

property that information is not made available or disclosed to unauthorized individuals, entities, or processes

3.49

data integrity

property that data has not been altered or destroyed in an unauthorized manner

3.50

data origin authentication

corroboration that the source of data received is as claimed

3.51

date pattern

date that may contain one or more unspecified octets or special date values

3.52

directly connected network

network that is accessible from a router without messages being relayed through an intervening router

Note 1 to entry: A PTP connection is to a directly connected network if the PTP connection is currently active and no intervening router is used.

3.53

download

particular type of file transfer that refers to the transfer of an executable program or database to a remote device where it may be executed

3.54

encrypted message

message that is wrapped in a security header, signed, and encrypted

3.55

entity

something that has a separate and distinct existence, identifiable item that is described by a set or collection of properties

3.56

error detection

procedure used to identify the presence of errors in a communication

3.57

error recovery

procedure invoked in *response* (3.15) to a detected error that permits the information exchange to continue

3.58

event algorithm

rules that determine when an event-initiating object changes between normal and offnormal states

Note 1 to entry: The event algorithm has no impact on an event-initiating object's transition to or from fault.

3.59

event-initiating object

object that is configured to monitor its event state and can report changes in its event state

3.60

event-notification-distribution

process that a *notification-server* (3.83) performs in the determination of *notification-clients* (3.82) and in the sending of notifications to notification-clients when an event-initiating object changes the event or acknowledgment state

3.61

event notification message

ConfirmedEventNotification or UnconfirmedEventNotification service request used to indicate a change in the event or acknowledgment state of an event-initiating object

3.62

event-state-detection

process of executing an event-initiating object's event algorithm and monitoring the object's Reliability property to detect changes in the object's event state

3.63

event-summarization

querying of event-initiating objects in a device through one of the event summarization services to determine those that meet specific event state or reporting conditions

3.64

fading

gradual increase or decrease of the actual output from one setting to another over a fixed period of time

3.65

gateway

device that connects two or more dissimilar *networks* (3.79), permitting information exchange between them

3.66

global

pertaining to all devices or *nodes* (3.81) on a communication *internetwork* (3.71)

3.67

global broadcast

message addressed to all devices or *nodes* (3.81) on all *networks* (3.79) in a BACnet *internetwork* (3.71)

3.68

half router

device or *node* (3.81) that can participate as one partner in a PTP connection

Note 1 to entry: The two half-router partners that form an active PTP connection together make up a single *router* (3.108).

3.69

incapable device

device that is inherently incapable, or has been configured to appear to be incapable, of producing or consuming secure BACnet messages

Note 1 to entry: All incapable devices are plain devices.

3.70

initialization

process of establishing a known state, usually from a power up condition Initialization may require re-establishment of a *node's* (3.81) logical or physical address

3.71

internetwork

set of two or more *networks* (3.79) interconnected by *routers* (3.108)

Note 1 to entry: In a BACnet *internetwork* (3.71) there exists exactly one message path between any two *nodes* (3.81).

3.72

intrinsic reporting

detection and reporting of an alarm or event, based on an algorithm defined as part of the *object type* specification

Note 1 to entry: No external reference to an Event Enrollment is involved.

Note 2 to entry: See *algorithmic change reporting*.

3.73

inverted network

BACnet *internetwork* (3.71) where two or more *networks* (3.79) are connected by a network with an NPDU size smaller than the networks it joins

3.74

key

sequence of symbols that controls the operations of encipherment and decipherment

3.75

local

pertaining to devices on the same *network* (3.79) as the referenced device

3.76

local broadcast

message addressed to all devices or *nodes* (3.81) on the same *network* (3.79) as the originator

3.77

medium

physical transmission *entity* (3.55)

EXAMPLE Twisted-pair wire, fiber optic cable, and coaxial cable.

3.78

medium access control

process used to maintain order and provide access to the communication *medium* (3.77)

3.79

network

set of one or more *segments* (3.111) interconnected by *bridges* (3.39) that have the same network address

3.80

network resource

any physical or logical *entity* (3.55) that may be accessed via a communication *medium* (3.77)

3.81

node

addressable device connected to the communication *medium* (3.77)

3.82

notification-client

BACnet device that receives and processes event notification messages

3.83

notification-server

BACnet device that contains event-initiating objects and performs event notification distribution

3.84

object

specific instance of an *object type* (3.86)

Note 1 to entry: While an object type is identified by a unique Object_Type property, an object is identified by its Object_Identifier property.

3.85

object profile

means of defining objects beyond those defined in Clause 12

Note 1 to entry: A profile defines the set of *properties* (3.97), behavior, and/or requirements for a proprietary object, or for proprietary extensions to a standard object.

3.86

object type

generic classification of data that is defined by a set of *properties* (3.97)

3.87

operator authentication

corroboration that the operator logging on to a device is as claimed

3.88

peer entity authentication

corroboration that a peer entity in an association is the one claimed

3.89

physical access control

PACS

electronic system that controls the ability of people or vehicles to enter a protected area, by means of authentication and authorization at access control points

3.90

physical segment

single contiguous *medium* (3.77) to which BACnet *nodes* (3.81) are attached

3.91

physically insecure

not physically secure

3.92

physically secure

device or network that is protected from physical access by unauthorized individuals

3.93

plain device

device that does not normally produce or consume secure BACnet messages

Note 1 to entry: All incapable devices are plain devices. However, a plain device that is not an incapable device is capable of producing or consuming secure BACnet messages when communicating with another device that requires it.

3.94

plain network

network that does not require signed or encrypted traffic

3.95

plain message

message that is not secured by a BACnet security wrapper

3.96

printable character

character that represents a printable symbol as opposed to a device control character Printable characters include, but are not limited to, upper-and lowercase letters, punctuation marks, and mathematical symbols

Note 1 to entry: The exact set depends upon the character set being used.

3.97

property

particular characteristic of an *object type* (3.86)

3.98

proprietary

<BACnet>any extension of or addition to *object types* (3.86), *properties* (3.97), PrivateTransfer services, or enumerations specified in this part of ISO 16484

3.99

ramping

gradual increase or decrease of the actual output from one setting to another at a fixed rate of change

3.100

receiving BACnet-user

BACnet-user (3.37) that receives an *indication* (3.10) or *confirm* (3.9) service primitive

3.101

reliability-evaluation

process by which an object determines its reliability and thus the value to set into its Reliability property

3.102

remote

pertaining to devices or *nodes* (3.81) on a different *network* (3.79) than the referenced device

3.103

remote broadcast

message addressed to all devices or *nodes* (3.81) on a different *network* (3.79) than the originator

3.104

repeater

device that connects two or more *physical segments* (3.90) at the physical layer

3.105

requesting BACnet-user

BACnet-user (3.37) that assumes the role of a *client* (3.43) in a confirmed service

3.106

responding BACnet-user

BACnet-user (3.37) that assumes the role of a *server* (3.13) in a confirmed service

3.107

role-based access control

RBAC

access privileges that are assigned to specific roles

Note 1 to entry: Access users acquire privileges through their assigned role.

3.108

router

device that connects two or more *networks* (3.79) at the network layer

3.109

secure network

network on which all traffic is required to be signed or encrypted

3.110

security

any of a variety of procedures used to ensure that information exchange is guarded to prevent disclosure to unauthorized individuals

Note 1 to entry: Security measures are intended to prevent disclosure of sensitive information even to those who have valid access to the communication *network* (3.79).

Note 2 to entry: Security is distinct from access control, although some security can be provided by limiting physical access to the communication medium itself.

3.111

segment

one or more *physical segments* (3.90) interconnected by repeaters

3.112

sending BACnet-user

BACnet-user (3.37) that issues a *request* (3.14) or *response* (3.15) service primitive

3.113

server

system or device that responds to a service *request* (3.14) instance for some particular purpose

Note 1 to entry: The server provides service to a *client* (3.43).

3.114

signed message

message that is wrapped in a security header, signed, and not encrypted

3.115

special date value

date value that is one of the special values such as "even months" or "last day of month"

Note 1 to entry: These special date values are used in subcomponents (octets) of a value of type Date.

3.116

specific date

fully specified date For example, January 24, 1991, Day of week = Thursday

Note 1 to entry: A specific date shall contain no unspecified octets or Special Date Values.

3.117

specific datetime

BACnetDateTime construct composed of a specific date and a specific time

3.118

specific time

fully specified time

EXAMPLE 17:35:4517 (= 5:35:4517 PM).

Note 1 to entry: A specific time shall contain no unspecified octets.

3.119

standard object type

object type (3.86) defined by this standard where the numerical value is within the range reserved for ASHRAE

3.120

standard property

required or optional property of a standard *object type* (3.86) where the numerical value of the property identifier is within the range reserved for ASHRAE and the property is listed in the object type's properties table in Clause 12

3.121

stepping

increase or decrease of an output value in discrete steps

3.122

synchronization

facility that allows processes to define and identify specific places in a transmission or exchange that can be used to reset a communication session to a predefined state

3.123

time pattern

time that may contain one or more unspecified octets

3.124

timestamp

indication of the point in time recorded for and accompanying the record of an event or operation

3.125

trusted

characterising a device or network whose messages are believed to be authentic, either through the use of secure messages or based on the physical security of that device or network

3.126

unit_time

length of time required to transmit one octet with a start bit and a single stop bit Ten bit-times

3.127

unspecified date

date composed entirely of unspecified octets

Note 1 to entry: A value of X'FF' = D'255'.

3.128

unspecified datetime

BACnetDateTime construct composed of an unspecified date and an unspecified time

3.129

unspecified octet

octet used in the context of date, time or BACnetWeekNDay values that contains the value X'FF' = D'255'

3.130

unspecified time

time composed entirely of unspecified octets

Note 1 to entry: A value of X'FF' = D'255'.

3.131

upload

process of transferring an executable program image or a database from a remote device in such a manner as to allow subsequent download

A	application layer (prefix)
ABA	American Bankers Association
AE	application entity
APCI	application protocol control information
APDU	application layer protocol data unit
API	application program interface
ARCNET	attached resource computer network
ASE	application service element
ASN.1	Abstract Syntax Notation One (ISO 8824)
B"	denotes that binary notation is used between the single quotes
BAC	building automation and control
BBMD	BACnet/IP broadcast management device
BDT	broadcast distribution table

B/IP	BACnet/IP
B/IP-M	BACnet/IP multicast
BVLC	BACnet virtual link control
BVLCI	BACnet virtual link control information
BVLL	BACnet virtual link layer
C	conditional
C(=)	conditional (The parameter is semantically equivalent to the parameter in the service primitive to its immediate left in the table.)
CNF	confirm primitive
COV	change of value
CRC	cyclic redundancy check
D''	denotes that decimal notation is used between the single quotes
DA	local destination MAC layer address
DADR	ultimate destination MAC layer address
DER	data expecting reply
DES	Data Encryption Standard (FIPS 46-1)
DESFire	Data Encryption Standard Fast, Innovative, Reliable and Secure
DID	ARCNET destination MAC address
DLEN	-octet length of ultimate destination MAC layer address
DNET	2-octet ultimate destination network number
DSAP	LLC destination service access point (X'82' for BACnet)
EIB	European Installation Bus
EIBA	European Installation Bus Association
EXEC	capable of executing a service request
FDT	foreign device table
ICI	interface control information

IL	ARCNET information length field
IND	indication primitive
INF	"Infinity", a unique binary pattern representing positive infinity (see ANSI/IEEE 754-1985)
-INF	"Negative infinity", a unique binary pattern representing negative infinity (see ANSI/IEEE 754-1985)
IEEE	Institute of Electrical and Electronics Engineers
INIT	capable of initiating a service request
IP	Internet Protocol - RFC 791
KNX	Konnex System Specification: EIB is the core protocol of the Konnex standard. The Konnex System Specification reflects the current status for EIB.
L	data link (prefix)
LAN	local area network
LLC	logical link control (ISO 8802-2)
LPCI	link protocol control information
LPDU	link protocol data unit
LRC	Longitudinal Redundancy Check
LSAP	link service access point (X'82' for BACnet)
LSDU	link service data unit
M	mandatory
M(=)	mandatory (the parameter is semantically equivalent to the parameter in the service primitive to its immediate left in the table.)
MA	medium access (prefix)
MAC	medium access control
MPCI	MAC protocol control information
MPDU	MAC layer protocol data unit
MSDU	MAC service data unit
MS/TP	master-slave/token-passing

N	network layer (prefix)
NaN	"Not a Number", a unique binary pattern representing an invalid number (see ANSI/IEEE 754-1985)
NAT	Network Address Translation - RFC 2663
NP	network priority
NPCI	network protocol control information
NPDU	network layer protocol data unit
NRZ	non-return to zero
NSAP	network service access point
NSDU	network service data unit
O	indicates that support of a property is optional
OSI	open systems interconnection
P	physical layer (prefix)
PAC	ARCNET data packet header octet
PCI	protocol control information
PDU	protocol data unit
PICS	protocol implementation conformance statement
PK	Private Key
PPCI	physical layer protocol control information
PPDU	physical protocol data unit
PPP	Point-To-Point protocol - RFC 1661
PSDU	physical service data unit
PTP	point-to-point
R	indicates that a property shall be supported and readable using BACnet services
REQ	request primitive
RFC	request for comment