
**Building automation and control
systems (BACS) —**

**Part 5:
Data communication protocol**

Systèmes d'automatisation et de gestion technique du bâtiment —

Partie 5: Protocole de communication de données

**iTeh STANDARD PREVIEW
(standards.iteh.ai)**

[ISO 16484-5:2017](https://standards.iteh.ai/catalog/standards/sist/d6b9789e-fc1b-44fa-9b62-c9867af28781/iso-16484-5-2017)

<https://standards.iteh.ai/catalog/standards/sist/d6b9789e-fc1b-44fa-9b62-c9867af28781/iso-16484-5-2017>



iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO 16484-5:2017

<https://standards.iteh.ai/catalog/standards/sist/d6b9789e-fc1b-44fa-9b62-c9867af28781/iso-16484-5-2017>



COPYRIGHT PROTECTED DOCUMENT

© ISO 2017, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

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. International Standards are drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see 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 (see 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 voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 205, *Building environment design*.

This sixth edition cancels and replaces the fifth edition (ISO 16484-5:2014), which has been technically revised. See the detailed list of changes on pages 1 312 to 1 327.

A list of all the parts in the ISO 16484 series, can be found on the ISO website.

CONTENTS

Foreword	iii
Introduction	xii
1 PURPOSE	1
2 SCOPE	1
3 DEFINITIONS	1
3.1 Terms Adopted from International Standards	1
3.2 Terms Defined for this Standard	2
3.3 Abbreviations and Acronyms Used in this Standard	7
4 BACnet PROTOCOL ARCHITECTURE	10
4.1 The BACnet Collapsed Architecture	11
4.2 BACnet Network Topology	13
4.3 Security	15
5 THE APPLICATION LAYER	16
5.1 The Application Layer Model	16
5.2 Segmentation of BACnet Messages	20
5.3 Transmission of BACnet APDUs	21
5.4 Application Protocol State Machines	25
5.5 Application Protocol Time Sequence Diagrams	42
5.6 Application Layer Service Conventions	50
6 THE NETWORK LAYER	51
6.1 Network Layer Service Specification	51
6.2 Network Layer PDU Structure	53
6.3 Messages for Multiple Recipients	58
6.4 Network Layer Protocol Messages	59
6.5 Network Layer Procedures	62
6.6 BACnet Routers	64
6.7 Point-To-Point Half-Routers	69
7 DATA LINK/PHYSICAL LAYERS: Ethernet (ISO 8802-3) LAN	73
7.1 The Use of ISO 8802-2 Logical Link Control (LLC)	73
7.2 Parameters Required by the LLC Primitives	73
7.3 Parameters Required by the MAC Primitives	73
7.4 Physical Media	73
8 DATA LINK/PHYSICAL LAYERS: ARCNET (ATA 878.1) LAN	74
8.1 The Use of ISO 8802-2 Logical Link Control (LLC)	74
8.2 Parameters Required by the LLC Primitives	74
8.3 Mapping the LLC Services to the ARCNET MAC Layer	74
8.4 Parameters Required by the MAC Primitives	74
8.5 Physical Media	74
9 DATA LINK/PHYSICAL LAYERS: MASTER-SLAVE/TOKEN PASSING (MS/TP) LAN	76
9.1 Service Specification	76
9.2 Physical Layer	78
9.3 MS/TP Frame Format	89
9.4 Overview of the MS/TP Network	91
9.5 MS/TP Medium Access Control	91
9.6 Cyclic Redundancy Check (CRC)	110
9.7 Interfacing MS/TP LANs with Other BACnet LANs	111
9.8 Responding BACnet User Processing of Messages from MS/TP	111
9.9 Repeaters	112
9.10 COBS (Consistent Overhead Byte Stuffing) Encoding	113
10 DATA LINK/PHYSICAL LAYERS: POINT-TO-POINT (PTP)	117
10.1 Overview	117
10.2 Service Specification	117
10.3 Point-to-Point Frame Format	121
10.4 PTP Medium Access Control Protocol	124
11 DATA LINK/PHYSICAL LAYERS: LonTalk (ISO/IEC 14908.1) LAN	145
11.1 The Use of ISO 8802-2 Logical Link Control (LLC)	145
11.2 Parameters Required by the LLC Primitives	145
11.3 Mapping the LLC Services to the LonTalk Application Layer	145

11.4	Parameters Required by the Application Layer Primitives	145
11.5	Physical Media	146
12	MODELING CONTROL DEVICES AS A COLLECTION OF OBJECTS	147
12.1	Object Characteristics and Requirements	147
12.2	Analog Input Object Type	152
12.3	Analog Output Object Type	158
12.4	Analog Value Object Type	164
12.5	Averaging Object Type	170
12.6	Binary Input Object Type	174
12.7	Binary Output Object Type	180
12.8	Binary Value Object Type	188
12.9	Calendar Object Type	195
12.10	Command Object Type	197
12.11	Device Object Type	203
12.12	Event Enrollment Object Type	214
12.13	File Object Type	222
12.14	Group Object Type	225
12.15	Life Safety Point Object Type	227
12.16	Life Safety Zone Object Type	234
12.17	Loop Object Type	240
12.18	Multi-state Input Object Type	248
12.19	Multi-state Output Object Type	253
12.20	Multi-state Value Object Type	259
12.21	Notification Class Object Type	265
12.22	Program Object Type	270
12.23	Pulse Converter Object Type	276
12.24	Schedule Object Type	283
12.25	Trend Log Object Type	289
12.26	Access Door Object Type	298
12.27	Event Log Object Type	306
12.28	Load Control Object Type	313
12.29	Structured View Object Type	322
12.30	Trend Log Multiple Object Type	327
12.31	Access Point Object Type	336
12.32	Access Zone Object Type	352
12.33	Access User Object Type	360
12.34	Access Rights Object Type	363
12.35	Access Credential Object Type	369
12.36	Credential Data Input Object Type	378
12.37	CharacterString Value Object Type	384
12.38	DateTime Value Object Type	390
12.39	Large Analog Value Object Type	395
12.40	BitString Value Object Type	402
12.41	OctetString Value Object Type	408
12.42	Time Value Object Type	412
12.43	Integer Value Object Type	417
12.44	Positive Integer Value Object Type	424
12.45	Date Value Object Type	431
12.46	DateTime Pattern Value Object Type	436
12.47	Time Pattern Value Object Type	441
12.48	Date Pattern Value Object Type	446
12.49	Network Security Object Type	451
12.50	Global Group Object Type	454
12.51	Notification Forwarder Object Type	461
12.52	Alert Enrollment Object Type	468
12.53	Channel Object Type	471
12.54	Lighting Output Object Type	480
12.55	Binary Lighting Output Object Type	493
12.56	Network Port Object Type	502

12.57	Timer Object Type	525
12.58	Elevator Group Object Type	537
12.59	Lift Object Type	540
12.60	Escalator Object Type	551
12.61	Accumulator Object Type	558
13	ALARM AND EVENT SERVICES	567
13.1	Change of Value Reporting	568
13.2	Event Reporting	572
13.3	Event Algorithms	583
13.4	Fault Algorithms	612
13.5	AcknowledgeAlarm Service	619
13.6	ConfirmedCOVNotification Service	621
13.7	UnconfirmedCOVNotification Service	623
13.8	ConfirmedEventNotification Service	624
13.9	UnconfirmedEventNotification Service	626
13.10	GetAlarmSummary Service	628
13.11	GetEnrollmentSummary Service	630
13.12	GetEventInformation Service	633
13.13	LifeSafetyOperation Service	635
13.14	SubscribeCOV Service	637
13.15	SubscribeCOVProperty Service	639
13.16	SubscribeCOVPropertyMultiple Service	642
13.17	ConfirmedCOVNotificationMultiple Service	647
13.18	UnconfirmedCOVNotificationMultiple Service	650
14	FILE ACCESS SERVICES	652
14.1	AtomicReadFile Service	653
14.2	AtomicWriteFile Service	656
15	OBJECT ACCESS SERVICES	658
15.1	AddListElement Service	658
15.2	RemoveListElement Service	660
15.3	CreateObject Service	662
15.4	DeleteObject Service	664
15.5	ReadProperty Service	665
15.6	Deleted Clause	667
15.7	ReadPropertyMultiple Service	668
15.8	ReadRange Service	671
15.9	WriteProperty Service	678
15.10	WritePropertyMultiple Service	680
15.11	WriteGroup Service	683
16	REMOTE DEVICE MANAGEMENT SERVICES	685
16.1	DeviceCommunicationControl Service	685
16.2	ConfirmedPrivateTransfer Service	687
16.3	UnconfirmedPrivateTransfer Service	689
16.4	ReinitializeDevice Service	690
16.5	ConfirmedTextMessage Service	692
16.6	UnconfirmedTextMessage Service	694
16.7	TimeSynchronization Service	695
16.8	UTCTimeSynchronization Service	696
16.9	Who-Has and I-Have Services	697
16.10	Who-Is and I-Am Services	699
17	VIRTUAL TERMINAL SERVICES	701
17.1	Virtual Terminal Model	701
17.2	VT-Open Service	705
17.3	VT-Close Service	707
17.4	VT-Data Service	708
17.5	Default Terminal Characteristics	710
18	ERROR, REJECT, and ABORT CODES	714
18.1	Error Class - DEVICE	714
18.2	Error Class - OBJECT	714

IteH STANDARD PREVIEW
(standards.iteh.ai)

<https://standards.iteh.ai/catalog/standards/sist/d6b9789e-fc1b-44fa-9b62-c9867af28781/iso-16484-5-2017>

<https://standards.iteh.ai/catalog/standards/sist/d6b9789e-fc1b-44fa-9b62-c9867af28781/iso-16484-5-2017>

18.3	Error Class - PROPERTY	715
18.4	Error Class - RESOURCES	716
18.5	Error Class - SECURITY	716
18.6	Error Class - SERVICES	718
18.7	Error Class - COMMUNICATION	719
18.8	Error Class - VT	721
18.9	Reject Reason	721
18.10	Abort Reason	722
18.11	Confirmed Service Common Errors	723
19	BACnet PROCEDURES	724
19.1	Backup and Restore	724
19.2	Command Prioritization	727
19.3	Device Restart Procedure	731
19.4	Determining Maximum Conveyable APDU	732
19.5	Value Source Mechanism	733
20	ENCODING BACnet PROTOCOL DATA UNITS	736
20.1	Encoding the Fixed Part of BACnet APDUs	736
20.2	Encoding the Variable Part of BACnet APDUs	746
21	FORMAL DESCRIPTION OF APPLICATION PROTOCOL DATA UNITS	760
22	CONFORMANCE AND INTEROPERABILITY	845
22.1	Conformance to BACnet	845
22.2	BACnet Interoperability	846
23	EXTENDING BACnet TO ACCOMMODATE VENDOR PROPRIETARY INFORMATION	848
23.1	Extending Enumeration Values	848
23.2	Using the Private Transfer Services to Invoke Non-Standardized Services	849
23.3	Adding Proprietary Properties to a Standardized Object	849
23.4	Adding Proprietary Object Types to BACnet	849
23.5	Restrictions on Extending BACnet	850
24	NETWORK SECURITY	851
24.1	Overview	851
24.2	Security Wrapper	855
24.3	Security Messages	859
24.4	Securing an APDU	875
24.5	Securing an NPDU	877
24.6	Securing BVLL Messages	877
24.7	Securing Messages	881
24.8	Network Security Network Trust Levels	884
24.9	Network Security Policies	884
24.10	Network Security	885
24.11	End-to-End Security	886
24.12	Wrapping and Unwrapping Secure Messages	886
24.13	Authenticating Messages	888
24.14	User Authentication	891
24.15	Time Synchronization Requirements	891
24.16	Integrating the Security Layer into the BACnet Stack	893
24.17	BACnet Security In A NAT Environment	900
24.18	BACnet Security Proxy	900
24.19	Deploying Secure Device on Non-Security Aware Networks	900
24.20	Deploying Secure Single Network Installations	900
24.21	Security Keys	900
24.22	Key Server	902
25	REFERENCES	906
	ANNEX A - PROTOCOL IMPLEMENTATION CONFORMANCE STATEMENT (NORMATIVE)	910
	ANNEX B - GUIDE TO SPECIFYING BACnet DEVICES (INFORMATIVE)	913
	ANNEX C - Removed	914
	ANNEX D - Removed	915
	ANNEX E - EXAMPLES OF BACnet APPLICATION SERVICES (INFORMATIVE)	916
	E.1 Alarm and Event Services	916
	E.2 File Access Services	920

E.3 Object Access Services	921
E.4 Remote Device Management Services	927
ANNEX F - EXAMPLES OF APDU ENCODING (INFORMATIVE)	932
F.1 Example Encodings for Alarm and Event Services	932
F.2 Example Encodings for File Access Services	942
F.3 Example Encodings for Object Access Services	944
F.4 Example Encodings for Remote Device Management Services	953
F.5 Example Encodings for Virtual Terminal Services	957
ANNEX G - CALCULATION OF CRC (INFORMATIVE)	960
G.1 Calculation of the Header CRC	960
G.2 Calculation of the Data CRC	965
G.3 Calculation of the Encoded CRC-32K	969
ANNEX H - COMBINING BACnet NETWORKS WITH NON-BACnet NETWORKS (NORMATIVE)	973
H.1 BACnet Gateways	973
H.2 Requirements and Best Practices for BACnet Gateway Implementations	973
H.3 Using BACnet with the DARPA Internet Protocols	975
H.4 Using BACnet with the IPX Protocol	976
H.5 Using BACnet with EIB/KNX	978
H.6 Using BACnet with the Former BACnet/WS Web Services Interface Defined by Annex N	986
H.7 Virtual MAC Addressing	988
ANNEX I - COMMANDABLE PROPERTIES WITH MINIMUM ON AND OFF TIMES (INFORMATIVE)	990
ANNEX J - BACnet/IP (NORMATIVE)	992
J.1 General	992
J.2 BACnet Virtual Link Layer	992
J.3 BACnet/IP Directed Messages	996
J.4 BACnet/IP Broadcast Messages	996
J.5 Addition of Foreign B/IP Devices to an Existing B/IP Network	998
J.6 Routing Between B/IP and non-B/IP BACnet Networks	1000
J.7 Routing Between Two B/IP BACnet Networks	1000
J.8 Use of IP Multicast within BACnet/IP	1006
ANNEX K - BACnet INTEROPERABILITY BUILDING BLOCKS (BIBBs) (NORMATIVE)	1008
K.1 Data Sharing BIBBs	1008
K.2 Alarm and Event Management BIBBs	1022
K.3 Scheduling BIBBs	1033
K.4 Trending BIBBs	1037
K.5 Device and Network Management BIBBs	1040
K.6 Network Security BIBBs	1047
ANNEX L - DESCRIPTIONS AND PROFILES OF STANDARDIZED BACnet DEVICES (NORMATIVE)	1050
L.1 Operator Interface Profiles	1050
L.2 Life Safety Operator Interface Profiles	1052
L.3 Access Control Operator Interface Profiles	1055
L.4 Controller Profiles	1058
L.5 Life Safety Controller Profiles	1061
L.6 Access Control Controller Profiles	1062
L.7 Miscellaneous Profiles	1063
L.8 BACnet General (B-GENERAL) Profile	1066
ANNEX M - GUIDE TO EVENT NOTIFICATION PRIORITY ASSIGNMENTS (INFORMATIVE)	1067
M.1 Life Safety Message Group (0 - 31)	1067
M.2 Property Safety Message Group (32 - 63)	1068
M.3 Supervisory Message Group (64 - 95)	1068
M.4 Trouble Message Group (96 - 127)	1069
M.5 Miscellaneous Higher Priority Message Group (128 - 191)	1069
M.6 Miscellaneous Lower Priority Message Group (192 - 255)	1070
ANNEX N - FORMER BACnet/WS WEB SERVICES INTERFACE (INFORMATIVE)	1071
N.1 Data Model	1071
N.2 Paths	1072
N.3 Normalized Points	1072
N.4 Reference Nodes	1073
N.5 Localization	1073

N.6 Security	1073
N.7 Sessions	1074
N.8 Attributes	1074
N.9 Standard Nodes	1079
N.10 Encodings	1080
N.11 Service Options	1081
N.12 Services	1083
N.13 Errors	1100
N.14 Extending BACnet/WS	1101
ANNEX O - BACnet OVER ZigBee AS A DATA LINK LAYER (NORMATIVE)	1102
O.1 General	1102
O.2 ZigBee Overview	1102
O.3 Definitions	1103
O.4 Unicast Addressing	1103
O.5 Broadcast Addressing	1103
O.6 BACnet/ZigBee Data Link Layer (BZLL)	1104
O.7 Maximum Payload Size	1107
O.8 Vendor Specific Commands	1107
ANNEX P - BACnet ENCODING OF STANDARD AUTHENTICATION FACTOR FORMATS (NORMATIVE)	1108
ANNEX Q - XML DATA FORMATS (NORMATIVE)	1113
Q.1 Introduction	1113
Q.2 XML Document Structure	1116
Q.3 Expressing Data	1119
Q.4 Expressing Metadata	1119
Q.5 Expressing Values	1120
Q.6 Binary Encoding and Access Rules	1122
Q.7 Extensibility	1122
Q.8 BACnet URI Scheme	1124
ANNEX R - MAPPING NETWORK LAYER ERRORS (NORMATIVE)	1125
ANNEX S - EXAMPLES OF SECURE BACnet MESSAGES (INFORMATIVE)	1127
S.1 Example of an Initial Key Distribution	1127
S.2 Example of Device Startup	1130
S.3 Examples of Secured Confirmed Requests	1133
S.4 Security Challenge Example	1139
S.5 Secure-BVLL Example	1141
ANNEX T - COBS (CONSISTENT OVERHEAD BYTE STUFFING) FUNCTIONS (INFORMATIVE)	1142
T.1 Preparing a COBS-Encoded MS/TP Frame for Transmission	1142
T.2 Decoding an Extended MS/TP Frame upon Reception	1144
T.3 Example COBS-Encoded Frame - Who-Has Service	1146
ANNEX U - BACnet/IPv6 (NORMATIVE)	1148
U.1 General	1148
U.2 BACnet/IPv6 BACnet Virtual Link Layer	1149
U.3 BACnet/IPv6 Directed Messages	1153
U.4 BACnet/IPv6 Broadcast Messages	1153
U.5 BACnet /IPv6 VMAc Table Management	1157
ANNEX V - MIGRATION FROM SOAP SERVICES (INFORMATIVE)	1158
V.1 Services	1158
V.2 Service Options	1160
ANNEX W - BACnet/WS RESTful WEB SERVICES INTERFACE (NORMATIVE)	1161
W.1 Data Model	1161
W.2 Paths	1161
W.3 Security	1162
W.4 Sessions	1171
W.5 Standard Data Items	1171
W.6 Metadata	1176
W.7 Functions	1176
W.8 Query Parameters	1177
W.9 Representation of Data	1179
W.10 Representation of Metadata	1180

W.11 Representation of Logs	1180
W.12 Filtering Items	1186
W.13 Limiting Number of Items	1187
W.14 Selecting Children	1188
W.15 Controlling Content of Data Representations	1188
W.16 Specifying Ranges	1191
W.17 Localized Values	1193
W.18 Accessing Individual Tags and Bits	1194
W.19 Semantics	1194
W.20 Links and Relationships	1194
W.21 Foreign XML and Other Media Types	1194
W.22 Logical Modeling	1195
W.23 Mapped Modeling	1195
W.24 Commandability	1196
W.25 Writability and Visibility	1196
W.26 Working with Optional Data	1197
W.27 Working with Optional Metadata	1198
W.28 Creating Data	1198
W.29 Setting Data	1199
W.30 Deleting Data	1201
W.31 Parentally Inherited Values	1201
W.32 Concurrency Control	1202
W.33 Server Support for Data Definitions	1202
W.34 Server Support for Metadata	1202
W.35 Client Implementation Guidelines	1203
W.36 Subscriptions	1204
W.37 Reading Multiple Resources	1205
W.38 Writing Multiple Resources	1206
W.39 Mapping of BACnet Systems	1207
W.40 Errors	1210
W.41 Examples	1212
ANNEX X - EXTENDED DISCOVERY OF DEVICES, PROFILES, AND VIEWS (NORMATIVE)	1241
X.1 Profiles	1241
X.2 xdd Files	1242
X.3 Example of Definition of Objects, Properties, and Datatypes.	1243
X.4 Views	1245
X.5 PICS Declarations	1250
ANNEX Y - ABSTRACT DATA MODEL (NORMATIVE)	1251
Y.1 Model Components	1251
Y.2 Trees	1253
Y.3 Base Types	1255
Y.4 Common Metadata	1255
Y.5 Named Values	1267
Y.6 Named Bits	1270
Y.7 Primitive Values	1271
Y.8 Range Restrictions	1273
Y.9 Engineering Units	1275
Y.10 Length Restrictions	1276
Y.11 Collections	1277
Y.12 Primitive Data	1279
Y.13 Constructed Data	1282
Y.14 Data of Undefined Type	1285
Y.15 Logical Modeling	1286
Y.16 Links	1286
Y.17 Change Indications	1288
Y.18 Definitions, Types, Instances, and Inheritance	1288
Y.19 Data Revisions	1294
Y.20 BACnet-Specific Base Types	1296
Y.21 BACnet-Specific Metadata	1297

IteH STANDARD PREVIEW
(standards.iteh.ai)

[ISO 16484-5:2017](https://standards.iteh.ai/catalog/standards/sist/d6b9789e-fc1b-44fa-9b62-10c523011444/iso-16484-5-2017)

<https://standards.iteh.ai/catalog/standards/sist/d6b9789e-fc1b-44fa-9b62-10c523011444/iso-16484-5-2017>

ANNEX Z - JSON DATA FORMATS (NORMATIVE)	1301
Z.1 Introduction	1301
Z.2 JSON Document Structure	1304
Z.3 Expressing Data	1307
Z.4 Expressing Metadata	1307
Z.5 Expressing Values	1308
Z.6 Extensibility	1310
HISTORY OF REVISIONS	1312

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[ISO 16484-5:2017](https://standards.iteh.ai/catalog/standards/sist/d6b9789e-fc1b-44fa-9b62-c9867af28781/iso-16484-5-2017)

<https://standards.iteh.ai/catalog/standards/sist/d6b9789e-fc1b-44fa-9b62-c9867af28781/iso-16484-5-2017>

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, other life safety applications, lighting, physical access control, and elevator monitoring, 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!

1 PURPOSE

The purpose of this standard is to define data communication services and protocols for computer equipment used for monitoring and control of HVAC&R and other building systems and to define, 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.

2 SCOPE

2.1 This protocol 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.

2.2 This protocol 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.

3 DEFINITIONS

3.1 Terms Adopted from International Standards

The following terms used in this standard are defined by international standards or draft standards for open system interconnection (OSI). The definitions are repeated here and a reference to the appropriate standard is provided. Clause 25 contains the titles of all national and international standards referenced in this clause and elsewhere in this standard. Words or phrases in italics refer to terms defined elsewhere in this clause.

abstract syntax: the specification of application layer data or application-protocol-control-information by using notation rules which are independent of the encoding technique used to represent them (ISO 8822).

application: a set of a USER's information processing requirements (ISO 8649).

application-entity: the aspects of an application-process pertinent to OSI (ISO 7498).

application-process: an element within a real open system which performs the information processing for a particular application (ISO 7498).

application-protocol-control-information: information exchanged between application-entities, using presentation services, to coordinate their joint operation (ISO 9545).

application-protocol-data-unit: a unit of data specified in an application protocol and consisting of application-protocol-control-information and possibly application-user-data (ISO 9545).

application-service-element: that part of an application-entity which provides an OSI environment capability, using underlying services when appropriate (ISO 7498).

concrete syntax: those aspects of the rules used in the formal specification of data which embody a specific representation of that data (ISO 7498).

confirm (primitive): a representation of an interaction in which a service-provider indicates, at a particular service-access-point, completion of some procedure previously invoked, at that service-access-point, by an interaction represented by a request primitive (ISO TR 8509).

ISO 16484-5:2017(E)

3. DEFINITIONS

indication (primitive): a representation of an interaction in which a service-provider 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 at the peer service-access-point (ISO TR 8509).

peer-entities: entities within the same layer (ISO 7498).

real open system: a real system which complies with the requirements of OSI standards in its communication with other real systems (ISO 7498).

real system: a 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 (ISO 7498).

request (primitive): a representation of an interaction in which a service-user invokes some procedure (ISO TR 8509).

response (primitive): a representation of an interaction in which a service-user indicates that it has completed some procedure previously invoked by an interaction represented by an indication primitive (ISO TR 8509).

(N)-service-access-point: the point at which (N)-services are provided by an (N)-entity to an (N+1)-entity (ISO 7498).

(N)-service-data-unit: an amount of (N)-interface-data whose identity is preserved from one end of an (N)-connection to the other (ISO 7498).

service-user: an entity in a single open system that makes use of a service through service-access-points (ISO TR 8509).

service-primitive; primitive: an abstract, implementation-independent representation of an interaction between the service-user and the service-provider (ISO TR 8509).

service-provider: an abstract of the totality of those entities which provide a service to peer service-users (ISO TR 8509).

transfer-syntax: that concrete syntax used in the transfer of data between open systems (ISO 7498).

user element: the representation of that part of an application-process which uses those application-service-elements needed to accomplish the communications objectives of that application-process (ISO 7498).

3.2 Terms Defined for this Standard

access control: a method for regulating or restricting access to network resources.

access rights (physical access control): the access privileges granted to a credential.

access user (physical access control): the person or asset holding one or more credentials.

alarm: 1. An annunciation, either audible or visual or both, that alerts an operator to an off-normal condition that may require corrective action. **2.** An abnormal condition detected by a device or controller that implements a rule or logic specifically designed to look for that condition.

alarm-acknowledgment: the process of indicating that a human operator has seen and responded to an event notification.

algorithmic change reporting: the detection and reporting of an alarm or event, based on an algorithm specified in an Event Enrollment object. See intrinsic reporting.

authentication: the act of verifying identity

authentication factor: a data element of the credential which is used to verify a credential's identity.

authorization (network security): the control of access to network resources based on known identity and access rules.

authorization (physical access control): the process of determining whether the access user is permitted to enter a protected zone through an access controlled point.

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

BACnet-user: that portion of an application-process that is represented by the BACnet user element.

blink-warn: in lighting control, typically a 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. 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 to keep the room lights on. Also known as "flick warn" or "flash warn."

bridge: a device that connects two or more segments at the physical and data link layers. This device may also perform message filtering based upon MAC layer addresses.

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

change of state: an event that occurs when a measured or calculated Boolean or discrete enumerated value changes.

change of value: an event that occurs when a measured or calculated analog value changes by a predefined amount.

client: a system or device that makes use of another device for some particular purpose via a service request instance. A client requests service from a server.

configurable: a property, setting, or value in a device is configurable if it can be changed via BACnet services or some other method. A property, setting, or value that is one-time writable or not changeable in situ is not considered to be configurable.

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

controller: a device for regulation or management of a system or component.

credential (physical access control): the combination of authentication factors and access rights.

data confidentiality: the property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

data integrity: the property that data has not been altered or destroyed in an unauthorized manner.

data origin authentication: the corroboration that the source of data received is as claimed.

date pattern: a date that may contain one or more unspecified octets or special date values.

directly connected network: a network that is accessible from a router without messages being relayed through an intervening router. A PTP connection is to a directly connected network if the PTP connection is currently active and no intervening router is used.

download: a 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.

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

entity: something that has a separate and distinct existence. An identifiable item that is described by a set or collection of properties.

error detection: a procedure used to identify the presence of errors in a communication.

error recovery: a procedure invoked in response to a detected error that permits the information exchange to continue.

event algorithm: the rules that determine when an event-initiating object changes between normal and offnormal states. The event algorithm has no impact on an event-initiating object's transition to or from fault.