BACnet-Server

FSM-8000-BNS

de Technische Beschreibung

Inhaltsverzeichnis

1 Zweck

Dieses Dokument enthält Informationen zur Installation und Konfiguration des AVENAR BACnet-Servers FSM-8000-BNS.
Grundlegende IT-Kenntnisse sind erforderlich, um ein AVENAR panel-Netzwerk einzurichten und zu konfigurieren und es mit dem BACnet-Server zu verbinden.

2 Sicherheit

Der AVENAR BACnet-Server definiert, wie die Sicherheit des Systems während seines gesamten Lebenszyklus gewährleistet wird. Dazu gehören die folgenden Aktivitäten:

- Installation: Sichere Konfigurationseinstellungen und sicheres Betriebssystem verwenden.
- Wartung: Updates durchführen, das System ordnungsgemäß außer Betrieb nehmen und Kundendaten vertraulich behandeln. Löschen Sie sensible Daten (z. B. Passwörter) am Ende der Systemlebensdauer oder während eines Zurücksetzens auf die Werkseinstellungen.

2.1 Sicherheitsvoraussetzungen

- Der Host-Rechner verwendet Windows 11 und erhält regelmäßige Updates.
- Nur autorisierte Personen haben physischen und logischen Zugriff auf den Windows-Rechner und das Brandmeldesystem.
- Die Kunden halten die geltenden Cybersicherheitsstandards ein und ergreifen Maßnahmen, um deren Einhaltung zu gewährleisten.
- Die Endbenutzer werden angewiesen, die Lizenzaktivierungsdatei vertraulich und sicher zu halten.

2.2 Benutzer- und Zugriffsverwaltung

- Nur autorisierte Personen dürfen physischen Zugriff auf den Windows-Host-Rechner oder zum Anlagenverbund Brandmeldesystem haben.
- Der Windows-Host-Rechner muss Rollenberechtigungen nach dem Prinzip der minimalen Berechtigung verwenden.
- Verwenden Sie nur die erforderliche Anzahl von Mitarbeiterkonten auf dem Windows-Host-Rechner.
- Verwenden Sie keine gemeinsam genutzten Konten im System.
- Legen Sie eine Ablaufzeit für Zugriffsrechte der Mitarbeiter fest. Löschen oder ändern Sie Konten, wenn Mitarbeiter nicht mehr an dem Projekt arbeiten oder sich ihre Rolle ändert.
- Legen Sie sichere Verfahren zur Passwortänderung und -zurücksetzung auf dem Windows-Host-Rechner fest.
- Passwörter auf dem Windows-Host-Rechner müssen einer Hardening-Richtlinie folgen. Verwenden Sie z. B. mindestens 12 Zeichen, einschließlich Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen.
- Verwenden Sie standardmäßig keine Gastkonten.

3 Systemübersicht

AVENAR panel ist ein nach EN 54 zertifiziertes analog adressierbares Brandmelde- und Alarmsystem (Fire Detection and Alarm System, FDAS).
Die Programmiersoftware FSP-5000-RPS ermöglicht die Anpassung an projektspezifische und länderspezifische Anforderungen.
Das AVENAR panel-Netzwerk verwendet das BACnet-Protokoll, um mit dem Gebäudemanagementsystem zu kommunizieren.
Das **Zentralennetzwerk** verfügt über Knoten. Ein Knoten kann eine Brandmelderzentrale, eine abgesetzte Bedieneinheit oder ein Server sein (z. B. einen BACnet-Server).
Jeder Knoten im AVENAR panel-Netzwerk verfügt über:

- eine einzigartige physikalische Knotenadresse (Physical Node Address, PNA)
- eine einzigartige logische Knotenadresse

Für die Kommunikation mit dem Gebäudemanagementsystem wird nur die logische Knotenadresse verwendet.
Die logische Knotenadresse verfügt über eine Netzwerkgruppennummer und eine Netzwerkknotennummer. Diese konfigurieren Sie in FSP-5000-RPS.
Eine vollständige Liste der unterstützten Netzwerktopologien finden Sie in Kapitel 9 des Netzwerkhandbuchs.
Die Brand-Peripheriegeräte sind mit den Brandmelderzentralen verbunden.
Die wichtigsten Brand-Peripheriegeräte sind:

- Automatische Brandmelder
- Manuelle Melder
- Signalgeber

Im Brandmeldesystem werden automatische Brandmelder und manuelle Melder werden als Punkt-Sicherheitselement (Security Item, SI) bezeichnet. Signalgeber werden als NAC-Sicherheitselement (SI) bezeichnet.
Jedes Peripheriegerät in einer Zentrale hat eine eindeutige logische Adresse.
Die logische Adresse verfügt über eine Gruppennummer und eine Unteradresse. Diese konfigurieren Sie in FSP-5000-RPS.
Punkte mit der gleichen Gruppennummer in einer Zentrale bilden eine Gruppe.
Signalgeber mit der gleichen Gruppennummer in einer Zentrale bilden eine NAC-Gruppe.
Der BACnet-Server identifiziert jedes Brandmelde-Peripheriegerät mit einem eindeutigen Objektnamen.
Beispiel: `1-2.SI_POINT.3.4`

- `1-2` = Logische Knotenadresse (Netzwerkgruppennummer und Netzwerkknotennummer der Zentrale)
- `SI_POINT` oder `SI_NAC` = Sicherheitselement-Typ
- `3.4` = Logische Adresse (Gruppen- und Unteradresse der Peripheriegeräte)

Life Safety-Objekte
Bei der Verwendung von Life Safety-Objekten fasst der BACnet-Server Life Safety Points zu Life Safety Zones zusammen. Jede Life Safety Zone hat einen einzigartige Kennzeichnung.
Beispiel: `1.2.3 LifeSafetyZone`

- `1.2` = Logische Knotenadresse: Netzwerkgruppennummer und Netzwerkknotennummer der Zentrale
- `3` = Gruppenadresse: Die Punktgruppe und die Signalgebergruppe einer Zentrale mit der gleichen Gruppenadresse werden in einer Life Safety Zone gruppiert.

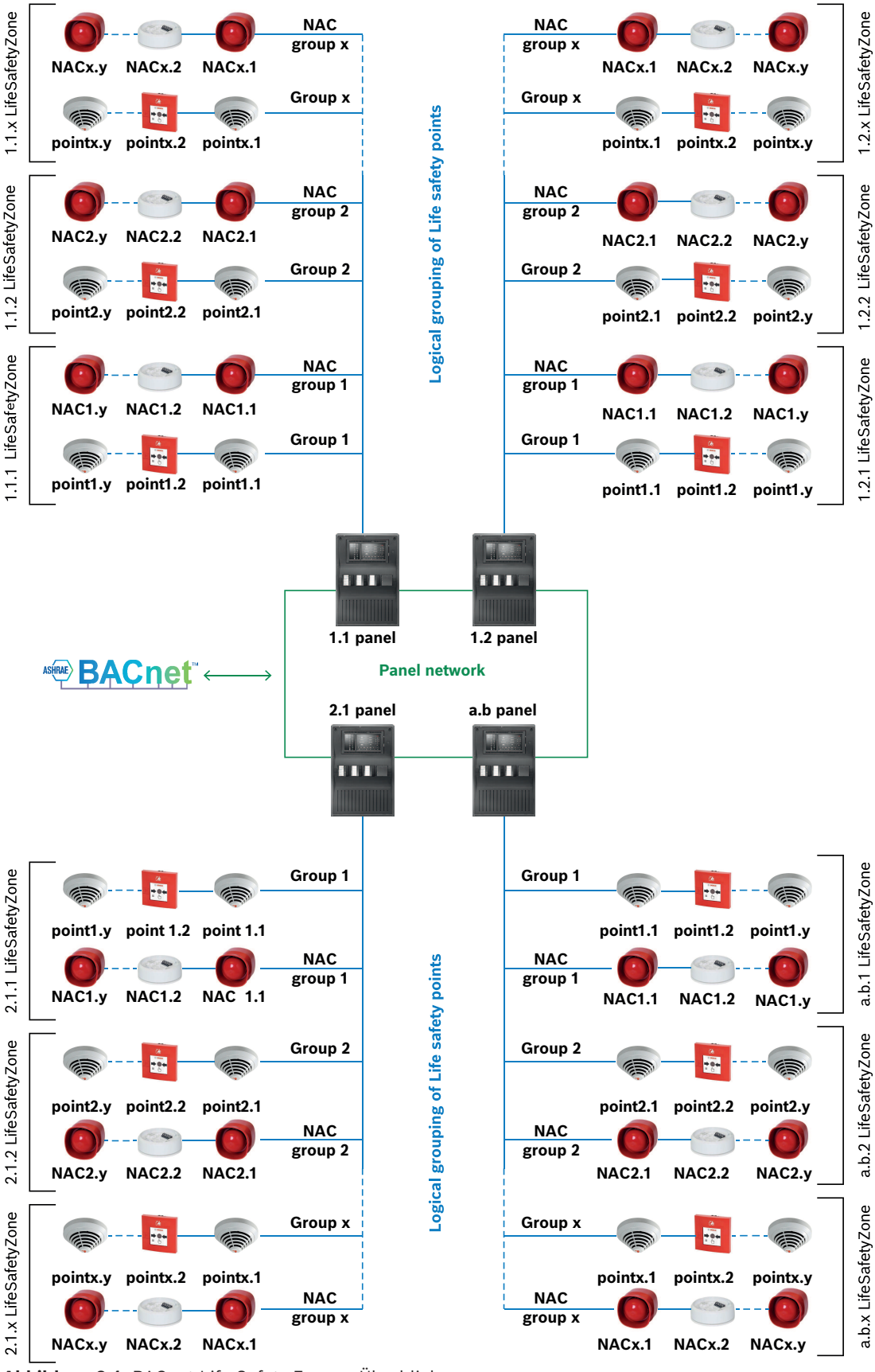

Abbildung 3.1: BACnet Life Safety Zones - Überblick

Der Zustand einer Life Safety Zone hängt vom Zustand des Life Safety Point innerhalb der Zone ab, die die höchste Priorität hat.
Die folgende Tabelle zeigt die Ereignisbedingungen von der höchsten bis zur niedrigsten Priorität:

Bedingung	Prioritätenreihenfolge
FIRE FIRE_DAY FIRE_INT ALARM_DAY SMOKE HEAT WATER	1
FIRE_PRE VERIFY_FIRE	2
SUPERVISORY	3
ACTIVATION	4
TROUBLE TROUBLE_DAY	5
*_BLOCKED *_BYPASS	6
*_WALKTEST	7
INVALID	8
NORMAL NORMAL_DAY	9

4 Produktbeschreibung

Der BACnet-Server für AVENAR panel ist ein Windows-Anwendungs-Gateway, das eine Schnittstelle für Managementsysteme bietet, um AVENAR Brandmeldesystemen zu integrieren.
BACnet ist ein Kommunikationsprotokoll für Gebäudeautomations- und Steuerungsnetzwerke (BACnet) in Gebäudemanagementsystemen.
Das Zielsystem ist ein Windows-Anwendungsserver.
Dieser Server integriert das BACnet-Protokoll mit dem AVENAR panel.
Diese Serveranwendung läuft auf einem Rechner mit Windows 11.
Die BACnet-Spezifikation erlaubt die Verwendung von BACnet-Standardobjekten und -services, um das Brandmeldesystem mit einem größeren Gebäudeautomationssystem zu verbinden.
Die BACnet-Versionshinweise des Servers in `C:\Program Files\Bosch\AVENAR BACnet server\Readme.txt` geben die Kompatibilität zu AVENAR panel-Firmware-Versionen an.
Die Bosch Sicherheitssystem GmbH verwendet Open Source Software für den AVENAR BACnet-Server. Für mehr Informationen siehe `C:\Program Files\Bosch\AVENAR BACnet server\FOSS-Licenses.txt`.

Datum	2024-11-18
Name des Anbieters	Bosch Sicherheitssysteme GmbH
Produktname	AVENAR BACnet-Server
Modellnummer des Produkts	FSM-8000-BNS
BACnet-Protokollversion	23

4.1 Unterstützung von standardisierten BACnet-Geräteprofilen (Annex L)

	BACnet Advanced Workstation	(B-AWS)
	BACnet Operator Workstation	(B-OWS)
	BACnet Operator Display	(B-OD)
	BACnet Building Controller	(B-BC)
	BACnet Advanced Application Controller	(B-AAC)
x	BACnet Life Safety Specific Controller	(B-LSC)
	BACnet Smart Sensor	(B-SS)
	BACnet Smart Actuator	(B-SA)

4.2 Unterstützung von BACnet-Interoperabilitätsbausteinen (Anhang K)

Datenfreigabe
Dazu ist wie folgt vorzugehen:

	Datenfreigabe – Eigenschaft-A lesen	DS-RP-A
x	Datenfreigabe – Eigenschaft-B lesen	DS-RP-B

	Datenfreigabe – Eigenschaft Mehrfach-A lesen	DS-RPM-A
x	Datenfreigabe – Eigenschaft Mehrfach-B lesen	DS-RPM-B
	Datenfreigabe – Eigenschaft Konditionell-A (veraltet) lesen	DS-RPC-A
	Datenfreigabe – Eigenschaft Konditionell-B (veraltet) lesen	DS-RPC-B
	Datenfreigabe – Eigenschaft-A schreiben	DS-WP-A
x	Datenfreigabe – Eigenschaft-B schreiben	DS-WP-B
	Datenfreigabe – Eigenschaft Mehrfach-A schreiben	DS-WPM-A
	Datenfreigabe – Eigenschaft Mehrfach-B schreiben	DS-WPM-B
	Datenfreigabe – Wert -A ändern	DS-COV-A
x	Datenfreigabe – Werteigenschaft -B ändern	DS-COV-B
	Datenfreigabe – Werteigenschaft -A ändern	DS-COVP-A
	Datenfreigabe – Werteigenschaft -B ändern	DS-COVP-B
	Datenfreigabe – Werteigenschaft von -A (unaufgefordert) ändern	DS-COVU-A
	Datenfreigabe – Werteigenschaft von -B (unaufgefordert) ändern	DS-COVU-B
	Datenfreigabe – Ansicht-A	DS-V-A
	Datenfreigabe – Erweiterte Ansicht-A	DS-AV-A
	Datenfreigabe – Ändern-A	DS-M-A
	Datenfreigabe – Erweitertes Ändern-A	DS-AM-A

Zeitplanung

	Zeitplanung – A	SCHED-A
	Zeitplanung – Internal-B	SCHED-I-B
	Zeitplanung – Extern-B	SCHED-E-B
	Zeitplanung – Erweiterte Ansicht Ändern-A	SCH-AVM-A
	Zeitplanung – Ansicht Ändern-A	SCH-VM-A
	Zeitplanung – Wochenplan-A	SCH-WS-A
	Zeitplanung – Wochenplan Intern-B	SCH-WS-I-B
	Zeitplanung – Auslesbar-B	SCH-R-B

Alarm- und Ereignismanagement

	Alarm und Ereignis – Benachrichtigung-A	AE-N-A
	Alarm und Ereignis – Benachrichtigung Intern-B	AE-N-I-B

	Alarm und Ereignis – Benachrichtigung Extern-B	AE-N-E-B
	Alarm und Ereignis – ACK-A	AE-ACK-A
x	Alarm und Ereignis – ACK-B	AE-ACK-B
	Alarm und Ereignis – Alarmzusammenfassung-A	AE-ASUM-A
	Alarm und Ereignis – Alarmzusammenfassung-B	AE-ASUM-B
	Alarm und Ereignis – Bekanntmachungszusammenfassung-A	AE-ESUM-A
	Alarm und Ereignis – Bekanntmachungszusammenfassung-B	AE-ESUM-B
	Alarm und Ereignis – Information-A	AE-INFO-A
x	Alarm und Ereignis – Information-B	AE-INFO-B
	Alarm und Ereignis – Schutz von Menschenleben-A	AE-LS-A
x	Alarm und Ereignis – Schutz von Menschenleben-B	AE-LS-B
	Alarm und Ereignis – Ansicht Benachrichtigungen-A	AE-VN-A
	Alarm und Ereignis – Erweiterte Ansicht Benachrichtigungen-A	AE-AVN-A
	Alarm und Ereignis – Anzeigen und Ändern-A	AE-VM-A
	Alarm und Ereignis – Erweiterte Anzeige und Ändern-A	AE-AVM-A
	Alarm und Ereignis – Alarmübersicht Anzeige-A	AE-AS-A
	Alarm und Ereignis – Ereignisprotokoll anzeigen-A	AE-ELV-A
	Alarm und Ereignis – Ereignisprotokoll anzeigen und ändern-A	AE-ELVM-A
	Alarm und Ereignis – Internes Ereignisprotokoll-B	AE-EL-I-B
	Alarm und Ereignis – Externes Ereignisprotokoll-B	AE-EL-E-B

Trends

	Trendaufzeichnung – Trends anzeigen und ändern-A	T-VMT-A
	Trendaufzeichnung – Intern anzeigen und ändern-B	T-VMT-I-B
	Trendaufzeichnung – Extern anzeigen und ändern-B	T-VMT-E-B
	Trendaufzeichnung – Mehrfachwerte anzeigen und ändern-A	T-VMMV-A
	Trendaufzeichnung – Mehrfachwerte intern anzeigen und ändern-B	T-VMMV-I-B
	Trendaufzeichnung – Mehrfachwerte extern anzeigen und ändern-B	T-VMMV-E-B
	Trendaufzeichnung – Automatisierte Mehrfachwertabfrage-A	T-AMVR-A

	Trendaufzeichnung – Automatisierte Mehrfachwertabfrage-B	T-AMVR-B
	Trendaufzeichnung – Anzeige-A	T-V-A
	Trendaufzeichnung – Erweiterte Anzeige und Änderung-A	T-AVM-A
	Trendaufzeichnung – Archivierung-A	T-A-A
	Trendaufzeichnung – Automatisierte Trendabfrage-A	T-ATR-A
	Trendaufzeichnung – Automatisierte Trendabfrage-B	T-ATR-B

Geräte- und Netzwerkmanagement

x	Gerätemanagement – Dynamische Gerätebindung-A	DM-DDB-A
x	Gerätemanagement – Dynamische Gerätebindung-B	DM-DDB-B
	Gerätemanagement – Dynamische Objektbindung-A	DM-DOB-A
x	Gerätemanagement – Dynamische Objektbindung-B	DM-DOB-B
	Gerätemanagement – Steuerung der Gerätekommunikation-A	DM-DCC-A
x	Gerätemanagement – Steuerung der Gerätekommunikation-B	DM-DCC-B
	Gerätemanagement – Private Übertragung-A	DM-PT-A
	Gerätemanagement – Private Übertragung-B	DM-PT-B
	Gerätemanagement – Textnachricht-A	DM-TM-A
	Gerätemanagement – Textnachricht-B	DM-TM-B
	Gerätemanagement – Zeitsynchronisierung-A	DM-TS-A
	Gerätemanagement – Zeitsynchronisierung-B	DM-TS-B
	Gerätemanagement – UTC-Zeitsynchronisierung-A	DM-UTC-A
	Gerätemanagement – UTC-Zeitsynchronisierung-B	DM-UTC-B
	Gerätemanagement – Gerät neu initialisieren-A	DM-RD-A
	Gerätemanagement – Gerät neu initialisieren-B	DM-RD-B
	Gerätemanagement – Backup und Wiederherstellung-A	DM-BR-A
	Gerätemanagement – Backup und Wiederherstellen-B	DM-BR-B
	Gerätemanagement – Neustart-A	DM-R-A
	Gerätemanagement – Neustart-B	DM-R-B
	Gerätemanagement – Listenmanipulation-A	DM-LM-A
	Gerätemanagement – Listenmanipulation-B	DM-LM-B
	Gerätemanagement – Objekt erstellen und löschen-A	DM-OCD-A
	Gerätemanagement – Objekt erstellen und löschen-B	DM-OCD-B

	Gerätemanagement – Virtuelles Terminal-A	DM-VT-A
	Gerätemanagement – Virtuelles Terminal-B	DM-VT-B
	Gerätemanagement – Automatische Netzwerkkartierung-A	DM-ANM-A
	Gerätemanagement – Automatische Gerätezuordnung-A	DM-ADM-A
	Gerätemanagement – Automatische Zeitsynchronisierung-A	DM-ATS-A
	Gerätemanagement – Manuelle Zeitsynchronisierung-A	DM-MTS-A

4.3 Segmentierungsfähigkeit

x	Kann segmentierte Meldungen übertragen	Standardfenstergröße = 3
x	Kann segmentierte Meldungen empfangen	Standardfenstergröße = 3

4.4 Unterstützte Standardobjekttypen

Objekttyp	Unterstützt	Objekttyp	Unterstützt
Zugangsdaten		Datei	
Zugangstür		Globale Gruppe	
Zugangspunkt		Gruppe	
Zugriffsrechte		Laststeuerung	
Zugriffsbenutzer		Ring	
Akkumulator		Life Safety Point	x
Analogeingang		Life Safety Zone	x
Analogausgang		Multi-State Input	x
Analogwert		Multi-State-Ausgang	
Mittelwertbildung		Multi-State-Wert	
Binärer Eingang		Netzwerkanschluss	x
Binärer Ausgang		Benachrichtigungsklasse	
Binärer Wert		Programm	
Kalender		Pulsumsetzer	
Befehl		Planung	
Gerät	x	Strukturierte Ansicht	
Ereignisanmeldung		Trend-Protokoll	
Ereignisprotokoll		Mehrere Trendprotokolle	

4.5 Optionen der BACnet-Datenverbindungsschicht

x	BACnet IP, (Anhang J)	
	BACnet IP, (Anhang J), Fremdgerät	
	ISO 8802-3, Ethernet (Abschnitt 7)	
	ANSI/ATA 878.1, 2,5 Mb. ARCNET (Abschnitt 8)	
	ANSI/ATA 878.1, RS-485 ARCNET (Abschnitt 8), Baudrate(n)	
	MS/TP-Master (Abschnitt 9), Baudrate(n)	
	MS/TP-Slave (Abschnitt 9), Baudrate(n)	
	Punkt-zu-Punkt, EIA 232 (Abschnitt 10), Baudrate(n)	38400
	Punkt-zu-Punkt, Modem (Abschnitt 10), Baudrate(n)	38400
	LonTalk, (Abschnitt 11), mittel	TP/FT-10
	Andere	

4.6 Bindung der Geräteadresse

Wird die statische Gerätebindung unterstützt?	Ja	**Nein**

4.7 Vernetzungsmöglichkeiten

	Router, Abschnitt 6 (Funktion zur Fernverwaltung/BACnet PTP)
	Anhang H, BACnet-Tunneling-Router über IP

4.8 Unterstützte Zeichensätze

x	UTF-8		IBM/Microsoft DBCS		ISO 8859-1
	ISO 10646 (UCS-2)		ISO 10646 (UCS-4)		JIS X 0208

5 Objektzuordnung

Für die Brandmelde-Peripheriegeräte unterstützt der BACnet-Server zwei verschiedene Objekte:

– Life Safety
– Multi-State Input

In der Konfiguration des BACnet-Servers müssen Sie auswählen, welches Objekt Sie verwenden möchten. Für mehr Informationen siehe *BACnet-Serverkonfiguration, Seite 19*.

5.1 Life Safety-Objekte

Die folgende Tabelle enthält eine Liste aller unterstützten Bedingungen für Brandmelde-Peripheriegeräte und deren Zuordnung für Life Safety Points und Life Safety Zones.

Bedingung	PresentValue/ TrackingValue property	StatusFlags property	Event_State property	Out_Of_Service property	Reliability property	Mode property
FIRE FIRE_DAY FIRE_INT ALARM_DAY SMOKE HEAT WATER	alarm (2)	1000	life-safety-alarm (5)	false	no-fault-detected (0)	on (1)
FIRE_PRE VERIFY_FIRE	pre-alarm (1)	1000	life-safety-alarm (5)	false	no-fault-detected (0)	on (1)
SUPERVISORY	supervisory (22)	0000	normal (0)	false	no-fault-detected (0)	enabled (11)
ACTIVATION	active (7)	1000	life-safety-alarm (5)	false	no-fault-detected (0)	on (1)
TROUBLE TROUBLE_DAY	fault (3)	0100	fault (1)	false	monitored-object-fault (14	disabled (12)
*_BLOCKED *_BYPASS	blocked (19)	0001	normal (0)	true	no-fault-detected (0)	disabled (12)
*_WALKTEST	test-alarm (9)	0000	normal (0)	false	no-fault-detected (0)	test (2)
INVALID	not-ready (6)	0000	normal (0)	false	no-fault-detected (0)	default (14)

Bedingung	PresentValue/ TrackingValue property	StatusFlags property	Event_State property	Out_Of_Service property	Reliability property	Mode property
NORMAL NORMAL_DAY	quiet (0)	0000	normal (0)	false	no-fault-detected (0)	enabled (11)

5.2 Multi-State-Input-Objekte

Die folgende Tabelle enthält eine Liste aller unterstützten Bedingungen für Brandmelde-Peripheriegeräte und deren Zuordnung für Multi-State Inputs.

Bedingung	PresentValue property
FIRE FIRE_DAY FIRE_INT ALARM_DAY SMOKE HEAT WATER	1
FIRE_PRE VERIFY_FIRE	2
SUPERVISORY	3
ACTIVATION	4
TROUBLE TROUBLE_DAY	5
*_BLOCKED *_BYPASS	6
*_WALKTEST	7
INVALID	8
NORMAL NORMAL_DAY	9

6 Technische Information

Voraussetzungen

Die folgenden Elemente werden benötigt, um einen BACnet-Server in einem Zentralennetzwerk einzurichten:

- AVENAR panel mit Premium-Lizenz
- Kompatible FSP-5000-RPS-Software
- FSM-8000-BNS-Serverversion, die mit der Zentralenversion kompatibel ist
- Windows 11 auf dem Host-Rechner, um FSM-8000-BNS zu installieren. Dadurch wird die Zuverlässigkeit und Integrität des BACnet-Servers gewährleistet.
- Windows-Firewall-Konfiguration: Fehlende Firewall-Regeln aktualisieren (TBU)
- Das vom BACnet-Server verwendete Netzwerksegment muss sicher und nur für vertrauenswürdige BACnet-Clients verfügbar sein.

6.1 Hardwareanforderungen

Bosch empfiehlt für den Betrieb des BACnet-Servers folgende Hardwareeinstellungen:

Prozessor	12th Gen Intel® Core™ i5-1240P 1.70 GHz
RAM	8.0 GB
Systemtyp	64-Bit-Betriebssystem, x64-basierter Prozessor
Betriebssystem	Windows 11 Enterprise
Version	23H2

6.2 Softwareanforderungen

Das System muss die folgenden Mindestanforderungen erfüllen:

- Windows 11 als unterstütztes Windows-Betriebssystem

Die zur Einrichtung des BACnet-Servers erforderliche Software umfasst:

- BACnet-Server-Installationspaket

Zur Überprüfung der Funktionsfähigkeit des BACnet-Servers und zur Validierung der Protokolldaten empfiehlt Bosch die Verwendung des Open-Source-Tools YABE (Yet Another BACnet Explorer). Sie können YABE von SourceForge.net herunterladen.

7 Installation und Konfiguration

7.1 Installation des BACnet-Servers

Der BACnet-Server wird als Installationspaket bereitgestellt, das für Windows 11 digital signiert ist.

1. Laden Sie die neueste Version des BACnet-Servers aus dem Extranet für Brandmeldesysteme herunter:
   https://www.boschsecurity.com/en/extranet/fire-alarm-systems/
2. Führen Sie das Installationspaket als Administrator aus.
3. Wenn Sie das Paket öffnen, wird ein Installationsassistent gestartet.
4. Der BACnet-Serverordner wird am Standardspeicherort erstellt:
   `C:\Program Files\Bosch\AVENAR BACnet server.`

Gehen Sie folgendermaßen vor, um den Standardordnerspeicherort zu ändern:

1. Klicken Sie im Installationsassistenten auf **Optionen**.
2. Klicken Sie im Fenster **Einrichtungsoptionen** auf **Durchsuchen**.
3. Wählen Sie den gewünschten Ordner aus.

7.2 BACnet-Serverlizenz

Für die Aktivierung des AVENAR BACnet-Servers ist eine Lizenzdatei erforderlich.
Nach der Installation des BACnet-Servers müssen Sie den Fingerabdruck des Rechners abrufen, auf dem der Server gehostet wird.
Senden Sie den Fingerabdruck an Bosch, um die Lizenzdatei zu erhalten.

Abrufen des Fingerabdrucks

1. Installieren Sie den BACnet-Server.
2. Öffnen Sie den Datei-Explorer und gehen Sie zu dem Ordner, in dem der Server installiert ist.
   Standardordner: `C:\Program Files\Bosch\AVENAR BACnet server.`
3. Klicken Sie oben auf die Adressleiste, geben Sie `cmd` ein und drücken Sie die **Eingabetaste**, um die Eingabeaufforderung zu öffnen.
4. Geben Sie den folgenden Befehl ein und drücken Sie die **Eingabetaste**:
   `Bosch.BT.BacnetServer /fingerprint`
   (Hinweis: Es gibt ein Leerzeichen nach `Server`)
5. Die Host-IDs werden in der Eingabeaufforderung angezeigt.
   Zum Beispiel: `98fa9bbb1001 04ed3315168e`
6. Kopieren Sie die Host-ID(s) aus der Eingabeaufforderung.
7. Fügen Sie die Host-IDs in das Lizenzanforderungsformular ein und senden Sie das Formular an Bosch unter: st-fir-emea.clp-Plan@de.bosch.com.

Aktivierung der Lizenz

1. Bosch sendet Ihnen die Aktivierungslizenzdatei per E-Mail zu.
2. Verschieben Sie die Lizenzdatei in den Lizenzordner.
   Standardordner: `C:\Program Files\Bosch\AVENAR BACnet server\License`

Hinweise

– Wenn der BACnet-Server läuft, kann die Umstellung der Uhr zu Softwarefehlern führen.
– Die Host-ID ist an die Netzwerkkarte des Rechners gebunden. Bei einem Wechsel der Netzwerkkarte ist eine neue Lizenz erforderlich.
– Eine abgelaufene Lizenz stoppt den BACnet-Server, auch wenn sich eine neue Lizenz im Ordner befindet.

– Um die Lizenz zu erneuern, ersetzen Sie die alte Lizenz durch die neue im Lizenzordner und starten Sie den BACnet-Serverdienst neu.

7.3 BACnet-Serverkonfiguration

Der BACnet-Server enthält eine `JSON`-Datei, in der Benutzer Netzwerkeinstellungen und allgemeine Anwendungskonfigurationen eingeben müssen:

```
{
  "ApplicationSettings": {
    "FSI": {
      "MPNetGroup": 2,
      "MPNetNode": 1,
      "PNA": 20,
      "LocalIPAddress": "192.168.1.20",
      "MulticastIpAddress": "239.192.0.1",
      "PortNumber": "25001"
    },
    "Bacnet": {
      "Ip": "192.168.1.20",
      "Port": 47808,
      "DeviceId": 1001
    },
    "CultureCode": "en-US",
    "Profile": "LifeSafety"
  }
}
```

Der Standardinstallationspfad des BACnet-Servers ist: `C:\Program Files\Bosch\AVENAR BACnet server\Settings`, Dateiname: `appsettings.json`.

Der Installationsprozess legt den Speicherort dieser Konfigurationsdatei fest. Führen Sie einen Texteditor (z. B. Notepad++) als Administrator aus, um die Konfigurationsdatei zu bearbeiten.

Die Konfigurationsdatei besteht aus zwei Teilen:

– FSI
– BACnet

Der BACnet-Server und der FSI-Server müssen in FSP-5000-RPS konfiguriert werden, damit sie wie vorgesehen funktionieren.

FSI

Die folgenden Einstellungen müssen in FSP-5000-RPS und in der `JSON`-Datei gleich sein:

Logische Knotenadresse:

– MPNetGroup=Net Group
– MPNetNode=Net Node

Physikalische Knotenadresse:

– PNA=PNA/RSN

IP-Einstellungen:

– LogicalIPAddress=IP Address
– MulticastIpAddress=Multicast: Es wird empfohlen, die Adresse 239.192.0.1 zu verwenden.
– PortNumber=Port: Es wird empfohlen, den Ethernetport 25001 zu verwenden.

BACnet

Die folgenden Einstellungen müssen im Gebäudemanagementsystem und in der `JSON`-Datei identisch sein:

– IP: IP-Adresse des Gebäudemanagementsystems. Falls das Gebäudemanagementsystem und der BACnet-Server auf demselben Rechner installiert sind, muss die IP-Adresse identisch sein.

– Port: Es wird empfohlen, den Ethernetport 47808 zu verwenden.
– DeviceId: Es wird empfohlen, die Geräte-ID 1001 zu verwenden.

Life Safety / **Multi-State**

In der JSON-Datei können Sie auswählen, welches BACnet-Objekt Sie verwenden möchten:

– Life Safety Standard
– Multi-State

Um Multi-State zu verwenden, ändern Sie den Wert von **Profile** zu **MultiState**.
Um Life Safety zu verwenden, behalten Sie den Wert von **Profile** bei als **LifeSafety**.

Vorsicht!
Risiko einer Fehlfunktion des Systems
Ändern Sie nicht die Struktur der JSON-Datei.

7.4 Inbetriebnahme des BACnet-Servers

Der BACnet-Server wird als automatisch gestarteter Dienst mit dem Namen AVENAR BACnet-Server ausgeführt, der auf dem Zielsystem installiert ist.
Wenn sich die Anwendungseinstellungen ändern, starten Sie den BACnet-Dienst jedes Mal neu:

1. Geben Sie **Dienste** in das Windows-Suchfeld ein, um den BACnet-Server zu starten oder zu stoppen.
2. Führen Sie das Fenster „Dienste“ als Administrator aus und suchen Sie nach AVENAR BACnet-Server.
3. Wählen Sie den AVENAR BACnet-Server aus und klicken Sie oben auf die Schaltfläche **Start** oder **Stop**.

8 Störungsbehebung

Wenn die Konfiguration des FSM-8000-BNS-Servers im Zentralennetzwerk nicht funktioniert, versuchen Sie die folgenden Verfahren:

- Vergewissern Sie sich, dass der BACnet-Server eine zugewiesene IP-Adresse hat und pingen Sie die Zentralensteuerung an.
- Falls der Ping-Befehl beantwortet wird, aber die Konfiguration noch immer nicht funktioniert, prüfen Sie:
  - Alle Einstellungen der Zentrale
  - Alle Einstellungen in der FSM-8000-BNS-Datei appsettings.json
  - Die Einstellungen des Ethernetadapters in der Systemkonfiguration von Windows
- Stellen Sie sicher, dass die Microsoft-Firewallregeln die Kommunikation zulassen:
  - Erlauben Sie eingehenden UDP-Verkehr für den FSI-Portbereich plus 7 im IP-Subnetz der Zentrale. Wenn der Port zum Beispiel als 25001 konfiguriert ist, reicht der Bereich von 25001 bis 25008. Zusätzlich muss Multicast-Verkehr für 239.192.0.1 erlaubt sein.
  - Erlauben Sie eingehenden UDP-Verkehr für BACnet-Meldungen auf dem konfigurierten BACnet-Server-Port von einer beliebigen IP und einem beliebigen Port (empfohlen 47808).
  - Wenn der Fehler weiterhin auftritt, deaktivieren Sie die Firewall, um zu prüfen, ob sie das Problem verursacht.
- Führen Sie diese Schritte aus:
  - Beenden Sie BACnet (siehe die Registerkarte **Dienste** im Configuration Editor).
  - Löschen Sie die bin-Dateien in `C:\Program Files\Bosch\AVENAR BACnet server\Repository`.
  - Starten Sie BACnet: Für jeden Knoten wird eine neue Datei angelegt.
- Falls keine Elemente angezeigt werden, kontrollieren Sie, ob der Ordner „Repository“ vorhanden ist und eine bin-Datei für jeden Knoten enthält. Die Dateien befinden sich in `C:\Program Files\Bosch\AVENAR BACnet server\Repository`.
- Stellen Sie sicher, dass die Zentralensteuerung keine Probleme im Zusammenhang mit dem BACnet-Serverknoten oder der Netzwerkkommunikation anzeigt.
- Vergewissern Sie sich, dass der BACnet-Server über eine gültige Lizenz verfügt. Öffnen Sie die Lizenzdatei, um das Ablaufdatum zu überprüfen. Folgendes kann dazu führen, dass die Lizenz nicht gültig ist:
  - Änderung der Uhr des Host-Rechners
  - Änderung der Netzwerkkarte des Host-Rechners
- Vergewissern Sie sich, dass die Zentralensteuerung über eine AVENAR-Premium-Lizenz mit Firmware-Kompatibilität verfügt, wie beschrieben in der Datei: `C:\Program Files\Bosch\AVENAR BACnet server\Readme.txt`.
- Öffnen Sie die Protokolldateien in `C:\Program Files\Bosch\AVENAR BACnet server\Logs\`, um die Fehlerprotokolle des FSI-Servers (fsi.log) und des BACnet-Servers (server.log) zu überprüfen.

Gebäudelösungen für ein besseres Leben

202505281036