



**Politecnico
di Torino**

III Facoltà di Ingegneria
Corso di Laurea in Ingegneria Informatica

Tesi di Laurea Magistrale

**Sicurezza e Interoperabilità nei
BEMS: Valutazione del Rischio e
Scenari di Protezione tra VPN,
Segregazione e BACnet/SC**
Security Assessment di architetture reali in ambienti
convergenti IT/OT

Relatori

prof. Fulvio Valenza

prof. ssa Maria Ferrara

Candidato

Antonio CATALANO

ANNO ACCADEMICO 2024-2025

Sommario

In un contesto in cui gli edifici intelligenti diventano sempre più interconnessi e data-centrici, i sistemi BEMS (Building Energy Management Systems) rappresentano un nodo nevralgico tra infrastrutture operative (OT) e reti informative (IT). Questa interconnessione, se da un lato abilita l'interoperabilità e l'ottimizzazione in tempo reale, dall'altro espone l'intero ecosistema edificio e servizi connessi a nuove superfici di attacco informatico.

La tesi si propone di affrontare in modo strutturato il tema della Cybersecurity nei sistemi BEMS, con particolare riferimento ai protocolli di comunicazione BACnet (ISO 16484-5) e alla loro evoluzione verso BACnet Secure Connect (BACnet/SC).

L'approccio seguito si indirizza a quello del *Security Assessment*, articolato su un'analisi comparativa di architetture reali, valutazione di rischi specifici e strategie di mitigazione, confrontando soluzioni tradizionali e moderne in termini di sicurezza, scalabilità e resilienza.

Viene inoltre proposto un possibile workflow di validazione tecnica, con criteri basati su interoperabilità, efficienza e resilienza, applicato a delle architetture reali e distinte.

Uno degli obiettivi è anche fornire un riferimento concreto per professionisti, progettisti e integratori di sistemi che operano in ambiti che stanno diventando sempre più critici.

Lungo tutto il percorso, la tesi evidenzia la centralità del dato come risorsa da proteggere e valorizzare, evidenziando come la Cybersecurity non sia solo un'esigenza tecnica, ma un fattore abilitante per l'affidabilità e la sostenibilità degli edifici del futuro (Intelligent Building).

Ringraziamenti

"Il futuro appartiene a coloro che credono nella bellezza dei propri sogni"

— Eleanor Roosevelt

Giunto al termine di questo lavoro di tesi, sento il dovere e il piacere di esprimere la mia profonda gratitudine a tutte le persone che, con il loro sostegno, la loro vicinanza, il loro incoraggiamento e, non da ultimo, la loro pazienza, mi hanno accompagnato nel tempo fino al raggiungimento di questo importante traguardo, nonostante il lungo percorso affrontato.

Desidero innanzitutto rivolgere un sentito ringraziamento al *Prof. Fulvio Valenza*, relatore di questa tesi, e alla *Prof.ssa Maria Ferrara*, correlatrice, per la loro disponibilità, competenza e guida preziosa. Grazie al loro costante supporto ho potuto trasformare le conoscenze acquisite durante il percorso di studi in esperienze concrete, applicate quotidianamente nel mio ambito professionale, dando forma e valore a questo lavoro di ricerca.

Un infinito ringraziamento va a *Tutte le Famiglie*, da quella di nascita, a quella che nel tempo si è allargata con *Teresa*, la sua famiglia e la nascita di *Davide*; a chi non c'è più ma è sempre con me. Con la loro presenza quotidiana, la loro storia di vita, in modi diversi ma soprattutto con il loro appoggio, mi hanno sempre aiutato ad affrontare ogni difficoltà e fin dall'inizio hanno creduto in me e in questo importante obiettivo.

Un Grazie particolare va anche a *Carmelo*, per l'aiuto, la pazienza, gli incoraggiamenti, l'affetto, la fiducia, la stima, l'esempio che ha saputo darmi. La sua presenza costante e il suo supporto quotidiano hanno rappresentato un punto di riferimento fondamentale nell'ultimo miglio di percorso.

Un caloroso ringraziamento va anche agli *amici*, ai *colleghi* ai *collaboratori*, incontrati in questi anni, con cui ho condiviso indimenticabili esperienze e che, con il loro affetto, mi sono sempre stati vicini e a cui devo tanto anche come esperienze di vita.

In ultimo vorrei ringraziare *tutte le persone* vicine e lontane che, con il loro contributo, mi hanno aiutato e sostenuto in questo lavoro di tesi.

Indice

| | |
|--|-----------|
| Elenco delle figure | 8 |
| Elenco delle tabelle | 9 |
| 1 Obiettivi e Percorso di Ricerca | 11 |
| 1.1 Motivazioni e contesto tecnologico | 11 |
| 1.2 Scopo della tesi e problemi affrontati | 12 |
| 1.3 Domande di ricerca e ipotesi operative | 13 |
| 1.4 Metodologia adottata | 14 |
| 2 Background: Reti IT/OT, Sistemi BEMS e Architetture di Auto- mazione | 15 |
| 2.1 Reti OT e IT: differenze, convergenza, sfide | 15 |
| 2.2 Architettura a livelli nei sistemi BMS/BEMS | 16 |
| 2.3 Dispositivi tipici: DDC, PLC, gateway, supervisori | 17 |
| 2.4 Reti di campo, protocolli e topologie fisiche | 18 |
| 3 Background: Standard di Comunicazione per l’Integrazione nei BEMS | 19 |
| 3.1 Protocolli aperti vs proprietari | 19 |
| 3.2 BACnet, Modbus, KNX, OPC UA – confronto tecnico-funzionale . | 20 |
| 3.3 Standardizzazione e interoperabilità secondo ISO 16484-5 | 21 |
| 3.4 Ruolo dei gateway e problematiche di traduzione semantica | 23 |
| 4 BACnet e BACnet Secure Connect (SC): Struttura, Logica e Ap- plicazioni | 25 |
| 4.1 Fondamenti di BACnet: oggetti, servizi, modelli dati | 26 |
| 4.2 Tipologie di rete: MS/TP, IP, Ethernet, BBMD, NAT | 26 |
| 4.3 Limiti del BACnet “classico” in ottica cybersecurity | 27 |
| 4.4 Evoluzione a BACnet/SC: struttura, TLS, CA | 27 |
| 4.5 Applicazioni reali nei sistemi di automazione | 30 |

| | | |
|----------|--|-----------|
| 5 | Proprietà di Sicurezza nei Sistemi BACnet | 32 |
| 5.1 | Limiti strutturali del BACnet “classico” | 32 |
| 5.2 | Sicurezza applicativa in BACnet/SC: autenticazione, crittografia, trust | 33 |
| 5.3 | Strategie di protezione: reti segregate, VPN, firewall | 33 |
| 5.4 | BACnet SC vs approcci infrastrutturali: confronto | 34 |
| 5.5 | Scenari di implementazione BACnet/SC | 35 |
| 5.5.1 | Scenario A - Accesso Sicuro dall'esterno della Struttura . . . | 35 |
| 5.5.2 | Scenario B - Accesso Sicuro all'interno dell'edificio | 36 |
| 5.5.3 | Scenario C – Accesso sicuro all'esterno e all'interno della struttura con aree isolate | 37 |
| 5.5.4 | Scenario D – Accesso Sicuro via Internet a diverse strutture | 38 |
| 5.6 | Raffronti Architetture BACnet IP Vs BACnet/SC | 39 |
| 6 | Rischi e Criticità nei Sistemi BEMS Interconnessi | 45 |
| 6.1 | Superfici di attacco e minacce in ambienti OT | 47 |
| 6.2 | Discovery, spoofing, broadcast storm, man-in-the-middle | 47 |
| 6.3 | Interoperabilità incompleta e versioning | 48 |
| 6.4 | Limiti degli approcci tradizionali alla sicurezza | 48 |
| 7 | Validazione della Sicurezza nei BEMS: Metodologia Proposta e Casi Studio | 50 |
| 7.1 | Obiettivi della validazione | 50 |
| 7.2 | Struttura della metodologia | 52 |
| 7.3 | Griglia di validazione e punteggio | 54 |
| 7.4 | Integrazione con audit e compliance | 55 |
| 7.5 | Esempio applicativo semplificato | 55 |
| 7.6 | Casi Studio Reali | 56 |
| 7.6.1 | Caso Studio A – Edificio Direzionale con rete segregata e BACnet/IP | 56 |
| 7.6.2 | Caso Studio A-Bis – Edificio Direzionale con rete segregata e BACnet/IP+SC | 58 |
| 7.6.3 | Caso Studio B – Super Condomini: BEMS distribuito e ac- cesso remoto via VPN | 60 |
| 7.6.4 | Caso Studio C – Insediamento Industriale Multivendor: su Private-Cloud Cliente e accesso remoto via VPN con MFA . | 61 |
| 7.6.5 | Caso Studio D – Connessione di edificio Residenziale e Ufficio con architettura full BACnet/SC | 63 |
| 7.7 | Riepilogo - Lezioni apprese e buone pratiche | 64 |

| | | |
|----------|--|-----------|
| 8 | Linee Guida e Raccomandazioni Operative | 65 |
| 8.1 | Principi per l'integrazione sicura di sistemi BEMS | 65 |
| 8.2 | Strumenti di progettazione e configurazione dei dispositivi | 66 |
| 8.3 | Gestione sicura degli aggiornamenti, dei certificati e degli accessi . . | 67 |
| 8.4 | Logging, auditing, monitoraggio e reazione agli incidenti | 68 |
| 9 | Conclusioni e Sviluppi Futuri | 69 |
| 9.1 | Sintesi dei risultati | 69 |
| 9.2 | Riflessioni conclusive | 70 |
| 9.3 | Limiti del lavoro | 70 |
| 9.4 | Sviluppi futuri | 71 |
| | Bibliografia | 72 |

Elenco delle figure

| | | |
|------|---|----|
| 4.1 | Schema di connessione BACnetSC | 28 |
| 4.2 | Confronto layer BACnet/IP vs BACnet/SC | 29 |
| 4.3 | BACnetSC nel modello ISO/OSI | 30 |
| 5.1 | Canale sicuro Nodo-HUB o HUB-Nodo | 34 |
| 5.2 | Architettura tipo con BACnet/SC | 35 |
| 5.3 | Scenario A BACnet/SC | 36 |
| 5.4 | Scenario B BACnet/SC | 37 |
| 5.5 | Scenario C BACnet/SC | 38 |
| 5.6 | Scenario D BACnet/SC | 39 |
| 5.7 | BACnet via BACnet-SC | 40 |
| 5.8 | BACnet IP via BBMD | 40 |
| 5.9 | Architettura BACnet/IP in piccole reti | 41 |
| 5.10 | Architettura BACnet/SC in piccole reti | 42 |
| 5.11 | Architettura BACnet/IP in reti di dimensioni sostenute | 42 |
| 5.12 | Architettura BACnet/SC in reti di dimensioni sostenute | 43 |
| 5.13 | Confronto architetture BACnet e BACnet/SC in reti piccole e gradi | 44 |

Elenco delle tabelle

| | | |
|-----|---|----|
| 2.1 | Caratteristiche a confronto nella gestione di Reti IT e Reti OT . . . | 16 |
| 3.1 | Caratteristiche a confronto nei protocolli Aperti e Proprietari | 20 |
| 3.2 | Caratteristiche a confronto nei diversi protocolli standard | 21 |
| 3.3 | Caratteristiche tecniche del protocollo BACnet | 23 |
| 4.1 | Tabella di recap funzionamento Hub-Nodi | 31 |
| 5.1 | Confronto caratteristiche di sicurezza IT e BACnet/SC | 34 |
| 6.1 | Tabella criteri di valutazione rischi e validazione | 49 |
| 7.1 | Tabella di valutazione con score per validazione | 54 |
| 7.2 | Ripilogo comparativo casi di studio | 64 |

Capitolo 1

Obiettivi e Percorso di Ricerca

1.1 Motivazioni e contesto tecnologico

I sistemi di Building Automation (BMS) stanno diventando sempre più sofisticati trasformandosi in BEMS e sempre più spesso devono esser integrati con altre infrastrutture IT; i Proprietari e gli Utilizzatori richiedono sempre più informazioni operative e anche sui costi che si riflettono sugli edifici il che genera che i Facility Manager chiedano ai sistemi di Building Automation sempre più dati ed il prima possibile (in real-time) il che implica anche più dispositivi e informazioni in rete da governare, addirittura trasferendoli direttamente da un sistema ad un altro; i Reparti IT sono già sovraccarichi dell'ordinaria operatività per l'infrastruttura IT ed hanno poca capacità di apprendere e gestire sistemi di Building Automation che non rispondono a degli standard.

Il concetto di edificio intelligente, un tempo prerogativa esclusiva dell'edilizia di alta fascia o delle applicazioni industriali, è oggi al centro di una trasformazione strutturale e tecnologica che investe l'intero comparto edilizio. Questa evoluzione è guidata da fattori convergenti: da un lato la necessità di ridurre i consumi energetici e le emissioni climalteranti, dall'altro la crescente attenzione al comfort abitativo, alla qualità dell'aria indoor, alla sicurezza e alla continuità dei servizi, il tutto si trasduce nella necessità di maggiori dati provenienti dal campo e le relative conseguenze legate alla loro trattazione.

In questo scenario, i **Building Energy Management Systems (BEMS)** rappresentano l'infrastruttura digitale fondamentale per la gestione intelligente degli impianti tecnologici degli edifici, comprendendo climatizzazione, ventilazione, illuminazione, controllo accessi, sicurezza e monitoraggio energetico. I BEMS moderni non si limitano a registrare dati, ma sono in grado di elaborare informazioni in tempo reale, ottimizzare comportamenti dinamici, reagire a condizioni ambientali variabili e garantire livelli costanti di comfort e performance implementando molteplici processi.

Tuttavia, questi benefici dipendono in larga misura dalla **capacità dei sistemi di comunicare in modo efficiente e sicuro**. L'**interoperabilità** tra dispositivi eterogenei, la **scalabilità** delle architetture e la **protezione** delle reti sono diventati requisiti centrali per garantire affidabilità, continuità operativa e rispetto delle normative.

Un elemento determinante nel cambiamento in atto è la **convergenza tra il mondo dell'Information Technology (IT)** e quello, storicamente separato, dell'**HVAC e della building automation**. Fino a pochi anni fa, i sistemi HVAC erano progettati e gestiti come compartimenti stagni, supervisionati da soluzioni **SCADA locali** o da interfacce grafiche dedicate, con comunicazioni basate su bus seriali o segnali analogici, spesso chiusi e proprietari.

Con l'evoluzione delle reti IP, dei protocolli standard e delle piattaforme software, è emersa una nuova generazione di sistemi BMS/BEMS capaci di **integrarsi nativamente** con le infrastrutture IT. I controllori DDC, i sensori intelligenti e i gateway multi-protocollo oggi operano all'interno di **reti IP convergenti**, parlano protocolli aperti come **BACnet/IP**, supportano aggiornamenti remoti, logging crittografato, gestione cloud e interfacce RESTful.

Questa **sovrapposizione tra dominio impiantistico e informatico** ha portato notevoli vantaggi in termini di automazione, scalabilità, accessibilità da remoto, gestione centralizzata e supporto ai modelli **"data-driven"**. Tuttavia, ha anche introdotto **nuove superfici di attacco**: intrusioni, compromissione delle credenziali e/o dei processi, intercettazione dei pacchetti, spoofing e denial of service sono minacce reali anche per un sistema di regolazione HVAC.

In parallelo, la regolamentazione internazionale (es. **NIS2, ENISA, ISO 27001**) e nazionale (es. linee guida ACN, framework AGID) impone oggi requisiti stringenti anche per l'automazione edilizia, in particolare nei settori pubblico, sanitario, industriale e terziario avanzato.

In questo contesto, il protocollo **BACnet**, ampiamente adottato come standard di comunicazione nei BEMS, mostra **limiti progettuali** legati alla sua origine "intranet-oriented". Per colmare questo gap, il comitato ASHRAE ha sviluppato **BACnet Secure Connect (BACnet/SC)**, un'estensione del protocollo che introduce nativamente meccanismi di **TLS, autenticazione mutua e gestione dei certificati digitali**, superando la necessità di protezioni infrastrutturali esterne come VPN o firewall complessi.

Questa tesi si inserisce all'interno di questa trasformazione, proponendo un'analisi critica e comparativa delle architetture di comunicazione per BEMS, mettendo a confronto approcci classici e moderni, con l'obiettivo di definire **un modello di riferimento sicuro, interoperabile, efficiente e scalabile**.

1.2 Scopo della tesi e problemi affrontati

Il principale obiettivo della tesi è offrire un contributo metodologico e applicativo alla progettazione e alla valutazione di **architetture di comunicazione sicura per sistemi BEMS**, con particolare riferimento a **BACnet** e alla sua evoluzione **BACnet/SC**.

Le domande a cui si intende rispondere includono:

- Come si può garantire una **vera interoperabilità** in un sistema multivendor basato su dispositivi eterogenei?

- Quali sono i **limiti di sicurezza** dei protocolli di comunicazione BEMS tradizionali?
- È possibile realizzare una **sicurezza end-to-end** nativa senza ricorrere a soluzioni infrastrutturali pesanti come le VPN?
- Come confrontare, in modo oggettivo, diverse architetture di rete BEMS in termini di efficienza, sicurezza e scalabilità?
- Quali **criteri tecnici** possono guidare la selezione della migliore configurazione architetturale in funzione del contesto operativo?

L'ambizione della tesi è duplice:

1. Da un lato, **esaminare criticamente** le soluzioni tecnologiche esistenti, le loro potenzialità e i loro limiti.
2. Dall'altro, **proporre un metodo di validazione tecnica**, utile a progettisti, integratori e gestori per selezionare e implementare architetture BEMS più robuste e sicure.

1.3 Domande di ricerca e ipotesi operative

La tesi adotta un approccio guidato da **ipotesi di lavoro** e da **domande di ricerca strutturate**, che verranno validate nei capitoli finali:

Domande di ricerca:

- Quali elementi abilitano l'interoperabilità reale nei sistemi BEMS?
- In quali condizioni BACnet/SC può sostituire o semplificare le soluzioni tradizionali di sicurezza perimetrale?
- Quali sono i costi architetturali (tecnici, gestionali) connessi all'introduzione di protocolli sicuri a livello applicativo?
- Quali sono i limiti normativi rispettati in materia di GDPR e come rispettarli
- Qual è il trade-off tra **semplicità infrastrutturale** e **complessità crittografica**?

Ipotesi operative:

- **H1:** BACnet SC può garantire un livello di sicurezza superiore, semplificando le architetture
- **H2:** Un approccio “application-layer security” è più scalabile in ambienti distribuiti rispetto alla segregazione fisica.
- **H3:** È possibile definire criteri tecnici oggettivi per valutare la qualità architetturale di una rete BEMS.

- **H4:** : La gestione dei dati intesi come aggregato di informazione per alimentare sistemi terzi superiori e non è impossibile se gestita in modo strutturato e ad oggetti con funzioni e proprietà.

Queste ipotesi saranno validate attraverso un confronto strutturato tra architetture di rete reali, simulazioni logiche e scenari applicativi concreti.

1.4 Metodologia adottata

La metodologia adottata è di tipo **tecnico-comparativa**, con un'impostazione **multi-dimensionale** che combina:

- Analisi normativa e tecnica di BACnet e BACnet SC.
- Ricognizione delle architetture reali adottate nel settore (impianti civili, industriali, sanitari, altro).
- Valutazione dei rischi legati alla sicurezza OT.
- Valore Aggiunto della disponibilità del Dato ex-post
- Proposta di modelli architetturali e criteri di confronto (funzionali, operativi, di sicurezza).
- Strumento di validazione dei vari modelli

Capitolo 2

Background: Reti IT/OT, Sistemi BEMS e Architetture di Automazione

2.1 Reti OT e IT: differenze, convergenza, sfide

Le reti IT (Information Technology) e OT (Operational Technology) hanno storicamente rappresentato due mondi distinti per obiettivi, tecnologie e approccio progettuale.

- Le **reti IT** sono orientate alla **gestione delle informazioni**, alla **comunicazione tra persone e sistemi**, e privilegiano **velocità, scalabilità, flessibilità e connettività globale**.
- Le **reti OT**, al contrario, sono progettate per **monitorare e controllare processi fisici**, come impianti HVAC, sistemi elettrici, illuminazione, controllo degli accessi e altre gestioni sottomesse o funzionali all'edificio o alle strutture in generale. L'obiettivo primario non è la connettività, bensì la **continuità operativa**, la **deterministicità** e l'**affidabilità in tempo reale**. Nel contesto della digitalizzazione degli edifici, queste due tipologie di reti si stanno **progressivamente fondendo**, portando a nuove sfide. Il BEMS moderno vive all'intersezione tra questi due mondi: riceve dati da dispositivi OT (tramite DDC, sensori e attuatori, altri sottosistemi), li elabora su infrastrutture IT (server, virtual machine, cloud) e li distribuisce in molteplici forme e modalità, dalla presentazione agli utenti tramite interfacce web al trasferimento a sistemi aziendali integrati che occupano di successive analisi in molteplici contesti.

Questa convergenza genera importanti benefici ma introduce anche **nuove criticità**.

Una attività di sintesi delle caratteristiche differenti tra reti IT e OT viene riassunta nella Tabella [2.1](#)

| Aspetto | Reti IT | Reti OT |
|----------------------|------------------------------|--|
| Obiettivo | Gestione dati e servizi | Controllo di processo fisico |
| Priorità | Riservatezza e integrità | Disponibilità e continuità |
| Protocolli | TCP/IP, HTTP, FTP | BACnet, Modbus, KNX |
| Aggiornamenti | Continui e automatizzati | Pianificati e vincolati alla stabilità |
| Sicurezza | Consolidata (firewall, SIEM) | Storicamente trascurata |

Tabella 2.1. Caratteristiche a confronto nella gestione di Reti IT e Reti OT

La fusione delle reti IT e OT richiede l'introduzione di nuove **architetture segmentate**, con firewall industriali, VLAN, DMZ, monitoraggio attivo e isolamento dei dispositivi critici e quanto altro necessario e funzionale alle diverse operatività in sicurezza di tutte le componenti dei sistemi coinvolti.

2.2 Architettura a livelli nei sistemi BMS/BEMS

I moderni sistemi di Building Management (BMS) e Building Energy Management (BEMS) sono strutturati secondo un modello **a livelli gerarchici**, che riflette la separazione funzionale tra i componenti.

Livello di campo (Field Level)

Comprende sensori (temperatura, umidità, CO₂, pressione) e attuatori (valvole, motori, attuatori), connessi direttamente agli impianti. La comunicazione avviene attraverso I/O digitali, analogici o bus seriali su RS485 (su svariati mezzi trasmissivi).

Livello di automazione (Controller Level)

Include dispositivi programmabili come DDC (Direct Digital Controller) o PLC (Programmable Logic Control), che eseguono logiche di regolazione (Control), raccolgono segnali e attuano comandi. Quasi sempre sono in grado di funzionare autonomamente anche in assenza di supervisione.

Livello di supervisione (Supervision Level)

Comprende software SCADA, BEMS o HMI, Applicazioni, che consentono il monitoraggio in tempo reale, la gestione di allarmi, la visualizzazione di dati storici e l'interazione con gli operatori. È il cuore del sistema di monitoraggio e gestione.

Livello enterprise / IT

Rappresenta l'integrazione del sistema con le infrastrutture informatiche aziendali: database, piattaforme di analisi energetica, sistemi ERP, servizi cloud e accesso remoto. Favorisce un approccio data-driven alla gestione dell'edificio.

La comunicazione tra i livelli avviene mediante protocolli standard (ad esempio BACnet, Modbus TCP, MQTT, XML-SOAP) e interfacce aperte, consentendo interoperabilità tra dispositivi e sistemi eterogenei.

L'interazione verticale consente automazione avanzata e visibilità operativa.

2.3 Dispositivi tipici: DDC, PLC, gateway, supervisori

Il cuore funzionale di ogni BEMS è costituito da un insieme di dispositivi elettronici programmabili, configurabili e organizzati secondo funzione e livello.

DDC (Direct Digital Controller)

Controllori digitali progettati specificamente per il mondo HVAC. Offrono:

- Logiche programmabili (PID, logiche condizionali, sequenze)
- Ingressi e uscite digitali/analogici
- Comunicazione via BACnet MS/TP o BACnet/IP
- Capacità di funzionamento autonomo e distribuito

PLC (Programmable Logic Controller)

Più diffusi in ambito industriale. Offrono:

- Maggiore robustezza e modularità
- Ampia gamma di moduli I/O e funzioni avanzate
- Maggiore complessità nella programmazione rispetto ai DDC HVAC-oriented

Gateway e router

Dispositivi di interfaccia tra protocolli diversi (Modbus-BACnet, KNX-BACnet, ecc.). Fondamentali per:

- Integrazione di dispositivi legacy
- Collegamento tra sotto-reti diverse (es. BBMD per BACnet/IP)
- Traduzione di indirizzamenti o conversioni semantiche

Supervisori e HMI

Software installati su Server o Dispositivi Embedded che forniscono:

- Visualizzazione dei dati in tempo reale
- Monitoraggio degli allarmi e notifiche
- Logging e trend energetici
- Accesso remoto da desktop o mobile

2.4 Reti di campo, protocolli e topologie fisiche

Le **reti di campo** rappresentano l'infrastruttura su cui viaggiano i segnali e i dati dei sistemi BEMS. La loro progettazione è cruciale per garantire:

- affidabilità
- scalabilità
- facilità di manutenzione

Protocolli di comunicazione

- **BACnet MS/TP**: funziona su RS-485, è robusto ma limitato in velocità e numero di nodi (64 o 99 device a seconda delle tecnologie impiegate dai diversi vendor).
- **BACnet/IP**: sfrutta Ethernet e TCP/IP, supporta reti IT ed è molto più veloce.
- **Modbus RTU / TCP**: semplice e molto diffuso, ma non orientato a oggetti.
- **KNX**: usato in ambito residenziale e terziario leggero.
- **MQTT**: indicato per scenari IoT o cloud-based.

Topologie fisiche

- **Bus (RS485)**: semplice ed economico, ma sensibile ai guasti fisici.
- **Stella (Ethernet)**: tipica delle reti IP con switch, offre flessibilità e facilità di diagnostica.
- **Anello / Mesh**: offre resilienza a guasti, usata in impianti critici o con fibra ottica.

Mezzi trasmissivi

- Cavo schermato twisted pair (RS-485)
- Cavi Ethernet CAT5/6/7
- Fibra ottica per lunghe distanze o ambienti ad alto disturbo EMI
- Wireless (Wi-Fi, Zigbee, 5G) per scenari senza cablaggio

L'evoluzione del settore porta a una migrazione progressiva verso reti IP-native, che abilitano soluzioni cloud, accessi sicuri, protocolli criptati e funzioni avanzate di diagnostica e logging distribuito.

A questo punto si è delineato il **contesto tecnico-operativo** all'interno del quale si muove la tesi. Dalla distinzione tra reti IT e OT, passando per la struttura a livelli dei BEMS, l'analisi dei dispositivi e la panoramica sui protocolli e sulle reti di campo, si è costruita una base solida per affrontare il cuore della trattazione: l'interoperabilità e la sicurezza nei sistemi BEMS basati su BACnet.

Capitolo 3

Background: Standard di Comunicazione per l'Integrazione nei BEMS

L'efficace integrazione dei sistemi di automazione negli edifici intelligenti si fonda sulla capacità di comunicazione tra dispositivi eterogenei. In questo capitolo vengono analizzati i **principali standard di comunicazione utilizzati nei BEMS**, con particolare attenzione al protocollo **BACnet**, alla sua evoluzione **BACnet Secure Connect (SC)** e al confronto con altri protocolli diffusi, evidenziandone punti di forza, limiti e implicazioni per la **sicurezza informatica** e l'**interoperabilità**.

3.1 Protocolli aperti vs proprietari

Una distinzione fondamentale nei sistemi di automazione è quella tra **protocolli aperti** e **protocolli proprietari**.

- **Protocolli proprietari** sono sviluppati e mantenuti da singoli produttori. Offrono spesso integrazione ottimale all'interno del proprio ecosistema, ma presentano **forti limiti di interoperabilità** verso dispositivi di terze parti. L'accesso alle specifiche tecniche è generalmente limitato o soggetto a licenza. Esempi: Siemens P1/P2, Trend, Honeywell C-Bus.
- **Protocolli aperti**, invece, sono pubblici, documentati e orientati a favorire l'**interoperabilità tra dispositivi eterogenei**. Sono mantenuti da consorzi o enti di standardizzazione e adottati in contesti dove apertura e scalabilità sono fondamentali. Esempi: BACnet, Modbus, KNX, OPC UA.

Una attività di sintesi delle caratteristiche differenti tra Protocolli Aperti (Standard) e Protocolli Proprietari viene riassunta nella Tabella [3.1](#)

| Caratteristica | Protocollo Aperto | Protocollo Proprietario |
|---------------------|-------------------|-------------------------|
| Accessibilità | Pubblica | Riservata |
| Interoperabilità | Alta | Limitata |
| Vendor lock-in | Basso | Alto |
| Supporto tecnico | Comunità aperta | Centralizzato |
| Evoluzione standard | Collaborativa | Dipendente dal vendor |

Tabella 3.1. Caratteristiche a confronto nei protocolli Aperti e Proprietari

3.2 BACnet, Modbus, KNX, OPC UA – confronto tecnico-funzionale

Nel tempo e sin dai primi arbori si sono susseguiti diversi protocolli di comunicazione che hanno tentato di imporsi come standard nel mondo della Building Automation, alcuni sono ormai tramontati (come Lonworks di Echelon[®]).

I protocolli di comunicazione più diffusi nei BEMS includono:

- **BACnet:** protocollo orientato agli **oggetti**, con molteplici **proprietà** e standardizzato secondo **ISO 16484-5**, progettato per la **Building Automation**. Supporta numerose funzioni integrate: allarmi, scheduling, trending, gestione eventi e si adatta a diversi layer di rete (MS/TP, IP, Ethernet).
- **Modbus:** protocollo industriale semplice, basato su registri e architettura master/slave. Manca di semantica, ma resta molto diffuso per la sua semplicità (che non sempre è sinonimo di compatibilità) e larga diffusione a basso costo.
- **KNX:** protocollo europeo nato per automazione residenziale e terziaria (dove il controllo non è di fatto un must). Utilizza una semantica a gruppi e supporta media come TP, IP e RF. Diffuso per funzioni legate a **comfort, illuminazione, tapparelle** e HVAC diciamo “Light”.
- **MQTT: Protocollo IoT-oriented**, ottimo per comunicazione cloud e logging distribuito. Sicuro se usato con TLS, ma non progettato per il controllo diretto di attuatori ha una funzione di interscambio.
- **OPC UA:** protocollo orientato all’interoperabilità a livello enterprise/IT. Pur non essendo nativo nei BEMS, viene utilizzato nei layer di supervisione e interfaccia IT/OT per la sua **modellazione semantica avanzata e sicurezza TLS**.
 - OPC UA è incluso come riferimento comparativo. La sua adozione nei BEMS è limitata a componenti middleware, mentre non è impiegato nei dispositivi di campo (es. DDC, sensori, attuatori).

Nella tabella 3.2 le caratteristiche individuate per la classificazione sono:

| Caratteristica | BACnet | Modbus | KNX | MQTT | OPC UA |
|-----------------------------|-------------|----------|------------|--------------------------------|-------------------|
| Modello dati | Oggetti | Registri | Gruppi | Topic/pub-sub (payload libero) | Modelli semantici |
| Sicurezza nativa | BACnet/SC | Assente | Limitata | TLS/X.509 | TLS/X.509 |
| Livello di interoperabilità | Alto | Basso | Medio | Alto | Molto alto |
| Topologie supportate | IP, MS/TP | RTU, TCP | TP, IP, RF | TCP/IP, WebSocket | TCP, MQTT |
| Standard di riferimento | ISO 16484-5 | De facto | EN 50090 | ISO/IEC 20922 | IEC 62541 |

Tabella 3.2. Caratteristiche a confronto nei diversi protocolli standard

- *Modello dati*: indica la struttura logica delle informazioni scambiate. I modelli orientati agli oggetti o semantici favoriscono l'interoperabilità.
- *Sicurezza nativa*: evidenzia la presenza (o meno) di meccanismi di autenticazione, cifratura e integrità integrati nel protocollo.
- *Livello Interoperabilità*: misura la capacità di integrazione trasparente tra dispositivi di vendor diversi.
- *Topologie*: elenca le reti fisiche e logiche supportate dal protocollo.
- *Standard di riferimento*: presenza di uno standard formale riconosciuto a livello internazionale che assevera quanto deve essere seguito.

L'evoluzione dei protocolli di comunicazione nei BEMS segue due direttrici principali:

- **Interoperabilità crescente** → standard aperti, oggetti comuni, servizi condivisi.
- **Sicurezza by design** → cifratura, autenticazione, segmentazione e gestione centralizzata.

BACnet/SC si pone come sintesi ideale poiché mantiene la struttura progettuale di BACnet, ma la integra con paradigmi IT contemporanei, rendendo i BEMS adatti a operare in contesti sempre più integrati e a **rischio cyber**.

3.3 Standardizzazione e interoperabilità secondo ISO 16484-5

BACnet (Building Automation and Control Network) è uno standard sviluppato da ASHRAE e formalizzato nella norma **ISO 16484-5**, pensato per **garantire l'interoperabilità tra dispositivi di automazione** appartenenti a produttori differenti.

Lo standard **ISO 16484-5** definisce BACnet come **protocollo standard** per i sistemi BEMS, specificando:

- Struttura a oggetti con proprietà e servizi definiti

- Comunicazione peer-to-peer
- Supporto a diverse topologie (MS/TP, Ethernet, IP)
- Conformità e certificazione tramite laboratori BTL

Caratteristiche chiave:

- **Modello a oggetti:** ogni dispositivo espone “oggetti” standardizzati (Analog Input, Binary Output, Schedule, ecc.).
- **Neutralità di trasporto:** supporta diversi media fisici e protocolli (RS-485, Ethernet, Wi-Fi, Zigbee).
- **Servizi applicativi standard:** lettura/scrittura di proprietà, scheduling, trending, gestione allarmi.
- **BIBBs** (BACnet Interoperability Building Blocks): definiscono i requisiti minimi per le funzionalità di interoperabilità.

Questa struttura rende BACnet particolarmente adatto ad ambienti BEMS, dove è necessario gestire un numero elevato di dispositivi eterogenei (valvole, sensori, attuatori, controllori, supervisori) con linguaggio comune.

L'obiettivo dello standard è garantire che **dispositivi di produttori differenti possano cooperare senza personalizzazioni proprietarie**, favorendo un'integrazione **flessibile, aperta e scalabile**. BACnet certificato secondo ISO 16484-5 è oggi requisito centrale in molti capitolati di gara pubblici e privati.

Di fatto possiamo assumere come definizione che BACnet è pensato per essere **agnostico rispetto al mezzo trasmissivo**. I due standard più diffusi sono:

BACnet MS/TP (Master-Slave/Token-Passing)

- Funziona su **RS-485** (bus seriale).
- Topologia a **bus lineare**, fino a 64/99 nodi.
- Velocità: 9.6–115.2 kbps.
- Nessuna sicurezza nativa.
- Ancora usato in impianti locali e retrofit.

BACnet/IP

- Funziona su **Ethernet o Wi-Fi**, usando il protocollo IP.
- Topologia a **stella o mesh**.
- Velocità: 100 Mbps – 1 Gbps.
- Integrabile con reti aziendali, virtualizzazione, VLAN.

- Prevede l'uso di **BBMD** per il superamento delle subnet IP.

Una attività di sintesi delle caratteristiche tecniche della comunicazione BACnet via RS485 e quella IP riassunta nella Tabella 3.3

| Parametro | BACnet MS/TP | BACnet/IP |
|-------------------------|------------------------------|------------------------------|
| <i>Mezzofisico</i> | RS-485/FibraOggetti | Ethernet/Wi-Fi/FibraRegistri |
| <i>Topologia</i> | Bus | Stella/Mesh |
| <i>Velocità</i> | ≤ 115.2 kbps | ≥ 100 Mbps |
| <i>Diagnostica</i> | Limitata e con grande effort | Avanzata (SNMP, Wireshark) |
| <i>Sicurezza nativa</i> | Nessuna | Nessuna (\rightarrow SC) |
| <i>Scalabilità</i> | Limitata | Elevata |

Tabella 3.3. Caratteristiche tecniche del protocollo BACnet

La transizione da MS/TP a IP è una delle principali direzioni evolutive del settore, favorita dalla convergenza tra mondo OT e IT.

3.4 Ruolo dei gateway e problematiche di traduzione semantica

In contesti eterogenei, l'integrazione tra protocolli diversi (BACnet, KNX, Modbus...) avviene spesso tramite **gateway**, che traducono i messaggi da un protocollo all'altro. BACnet si è affermato sin dall'inizio e viene utilizzato oggi poiché è in grado di coprire tutti i 7 livelli della Pila ISO/OSI, in quanto il livello Applicazione è definito nello standard.

Di fatto è noto che i gateway possono introdurre diverse problematiche:

- **Perdita di semantica:** oggetti BACnet complessi possono ridursi a registri generici in Modbus
- **Incoerenza** nei tipi di dato o nella scala di valori
- **Latenze** dovute a polling o a traduzioni lente
- **Mancanza di supporto** a funzionalità avanzate (trending, allarmi, eventi)

L'utilizzo dei gateway deve quindi essere progettato con cura, valutando anche alternative basate su middleware o soluzioni che impiegano protocolli con **modelli informativi compatibili**, per questo la volontà di riportare su BACnet tutto quello lato BMS che non lo è nell'altro protocollo (Standard o proprietario che sia)

Fino a questo punto abbiamo delineato il panorama tecnico degli standard di comunicazione più diffusi nei BEMS. La conoscenza delle caratteristiche, delle differenze e delle implicazioni di sicurezza di ciascun protocollo rappresenta il prerequisito per poter progettare architetture realmente interoperabili e sicure, in linea con i requisiti dell'edificio intelligente moderno.

Capitolo 4

BACnet e BACnet Secure Connect (SC): Struttura, Logica e Applicazioni

BACnet Secure Connect (BACnet/SC) è una caratteristica significativa verso la creazione di un protocollo di comunicazione dati sicuro per reti di automazione degli edifici e che fornisce una infrastruttura di Building Automation che utilizza un protocollo Internet Standard e metodi di Sicurezza Standard ampiamente utilizzati, eliminando gran parte delle preoccupazioni e del lavoro di un reparto IT. BACnet/SC è un'aggiunta alle specifiche BACnet esistenti e utilizza il protocollo TLS per autenticare i dispositivi sulla rete di automazione degli edifici e crittografare le loro comunicazioni. La sicurezza TLS è tra i protocolli di sicurezza più recenti e porta il BACnet a un livello di sicurezza crittografica considerato affidabile da governi e istituzioni finanziarie in tutto il mondo.

Ogni dispositivo sulla rete BACnet/SC viene verificato nella propria identità prima di poter accedere alla comunicazione in rete. Senza autenticazione, i dispositivi non verificati non possono accedere alla rete e non possono comunicare con altri dispositivi verificati. Grazie a questo meccanismo, tutte le informazioni che attraversano la rete BACnet/SC sono crittografate end-to-end, impedendo a malintenzionati di intercettare e decodificare il traffico. Ciò impedisce agli hacker di alterare le prestazioni e il funzionamento del sistema. Le informazioni inviate tramite una connessione BACnet/SC vengono verificate come dati autentici e inalterati provenienti dalla fonte originale.

BACnet/SC è un nuovo Data Link Layer BACnet, che offre un altro modo per inviare il traffico BACnet tra due reti. Il routing BBMD tradizionale è efficace nel connettere dispositivi BACnet che risiedono su reti separate. Tuttavia, richiede eccezioni firewall per consentire la comunicazione bidirezionale e il traffico tra i dispositivi BBMD è completamente aperto e non crittografato. BACnet/SC sostituisce la necessità di dispositivi BBMD, colmando così una significativa lacuna di sicurezza presente da molti anni nel mondo dell'automazione degli edifici.

L'interoperabilità di prodotti BACnet tra diversi produttori è garantita da BACnet. Una rete può contenere un mix di controllori BACnet/SC e non BACnet/SC, consentendo un percorso di aggiornamento graduale per portare l'intero sistema ai

più recenti standard di sicurezza. Pochi produttori hanno sviluppato ad oggi questa caratteristica distintiva.

4.1 Fondamenti di BACnet: oggetti, servizi, modelli dati

A differenza di altri protocolli storici nati in ambito industriale, BACnet è stato progettato fin dall'inizio con una struttura orientata agli oggetti, riflettendo una visione in cui ogni componente del sistema – sensori, attuatori, dispositivi di controllo, supervisor – è rappresentato secondo un modello logico coerente, indipendente dal costruttore o dal livello della rete.

Questa struttura si articola attorno a:

- **Oggetti BACnet**, come Analog Input, Binary Output, Schedule, Trend Log, ognuno dei quali incapsula specifiche proprietà (valore presente, unità di misura, stato di affidabilità, ecc.).
- Un insieme di **Servizi Standardizzati** che permettono di interrogare, modificare o ricevere notifiche in tempo reale sulle proprietà degli oggetti: ReadProperty, WriteProperty, SubscribeCOV, Alarm Acknowledgment, e così via.

Questa modellazione consente una **coerenza semantica** nell'interazione tra dispositivi diversi. Un controllore BACnet può dialogare con un sensore BACnet di un altro vendor, purché entrambi aderiscano allo standard ISO 16484-5.

4.2 Tipologie di rete: MS/TP, IP, Ethernet, BBMD, NAT

La flessibilità di BACnet si manifesta anche nella varietà di tipologie di rete che supporta. A seconda della scala del sistema, della topologia fisica e dei vincoli infrastrutturali, è possibile scegliere tra diversi layer di trasporto.

BACnet MS/TP è una soluzione seriale su RS-485, molto comune per il collegamento di dispositivi di campo. Basata su un meccanismo di token-passing, garantisce un controllo ordinato dell'accesso al mezzo.

BACnet/IP è oggi la soluzione predominante per reti moderne. Consente l'uso di infrastrutture Ethernet standard, l'integrazione in VLAN, l'accesso remoto tramite VPN e l'interconnessione di edifici distribuiti.

BBMD consente la propagazione dei messaggi broadcast BACnet tra subnet IP diverse, mentre NAT pone problemi che richiedono soluzioni come VPN o tunneling.

4.3 Limiti del BACnet “classico” in ottica cybersecurity

BACnet è nato in un contesto e in un momento storico in cui la sicurezza informatica **non era una priorità**, in quanto i sistemi di automazione erano progettati per lavorare in **reti isolate (air-gapped)**. Nel tempo l'esigenza crescente di accesso remoto alla struttura o ai sistemi ha reso sempre più necessaria l'interconnessione della rete segmentata BACnet con le reti aziendali. Questo lo rende oggi sempre più vulnerabile in ambienti connessi.

Principali limiti:

- **Dati in chiaro:** il traffico BACnet può essere intercettato e analizzato facilmente, perché non criptato .
- **Assenza di autenticazione forte:** ogni dispositivo sulla rete può inviare richieste, anche non autorizzate.
- **Possibilità di spoofing:** un attore malevolo può impersonare un altro dispositivo.
- **Scarsa tracciabilità:** difficile identificare l'origine delle richieste maligne.
- **Broadcast indiscriminato:** utile per il discovery, ma utilizzabile anche a fini malevoli.

Tali limiti non sono trascurabili, soprattutto in architetture in cui la rete BEMS è connessa alla rete aziendale o accessibile da remoto.

4.4 Evoluzione a BACnet/SC: struttura, TLS, CA

L'evoluzione di BACnet verso una maggiore sicurezza e compatibilità IT ha portato allo sviluppo di BACnet Secure Connect (SC).

Con l'introduzione di **BACnet/SC**, approvato nel 2019 Annex bj del 135-2016 come estensione ufficiale dello standard, si è colmata la mancanza di sicurezza strutturale nel protocollo.

BACnet/SC abbandona i broadcast e il trasporto UDP, adottando HTTP con TLS 1.3, rendendolo compatibile con le infrastrutture IT moderne. Utilizza una topologia hub-and-spoke, con relay centralizzati che redistribuiscono il traffico BACnet.

Ogni nodo BACnet/SC utilizza certificati X.509 per garantire autenticazione, integrità e riservatezza. La gestione centralizzata dei certificati rende BACnet/SC una soluzione altamente scalabile e sicura per ambienti complessi. Tra le caratteristiche principali:

- **Uso di HTTP over TLS 1.3** → cifratura end-to-end.

- **Mutua autenticazione tramite certificati digitali X.509.**
- **Trasporto nativo su IP** (porta TCP 443 configurabile).
- **Eliminazione del broadcast** → riduzione della superficie d'attacco.
- **Modelli di topologia: Hub & Spoke o Failover Mesh.**

Uno schema di connessione tipico tramite BACnet/SC può essere rappresentato dalla Figura 4.1

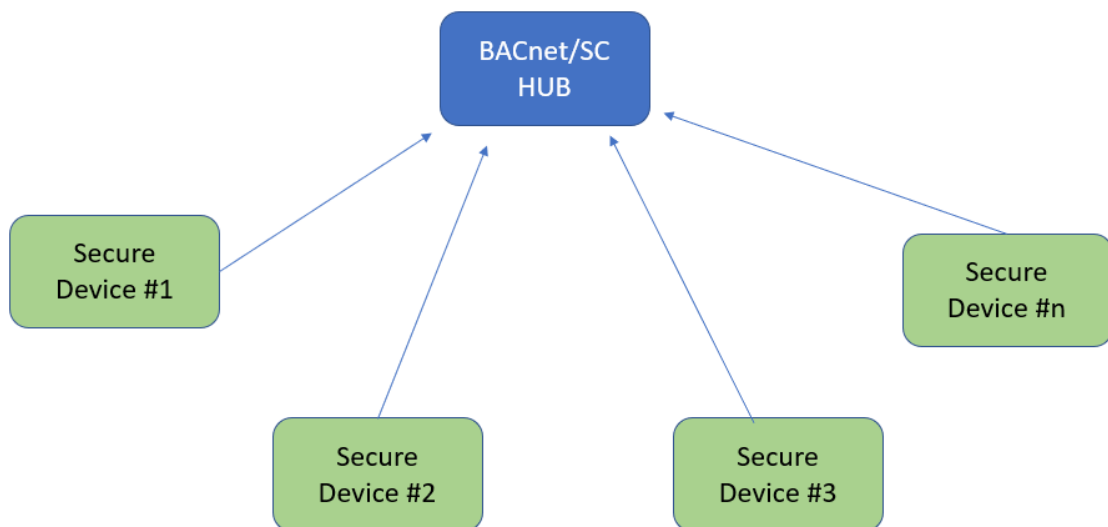


Figura 4.1. Schema di connessione BACnetSC

dove si mostra la struttura tipica (di una rete BACnet/SC), in cui tutti i dispositivi sicuri si connettono a un **Hub centrale** che gestisce l'autenticazione, la crittografia e il routing TLS.

Mentre il secondo diagramma nella Figura 4.2 mostra l'evoluzione dello stack di protocolli in cui abbiamo:

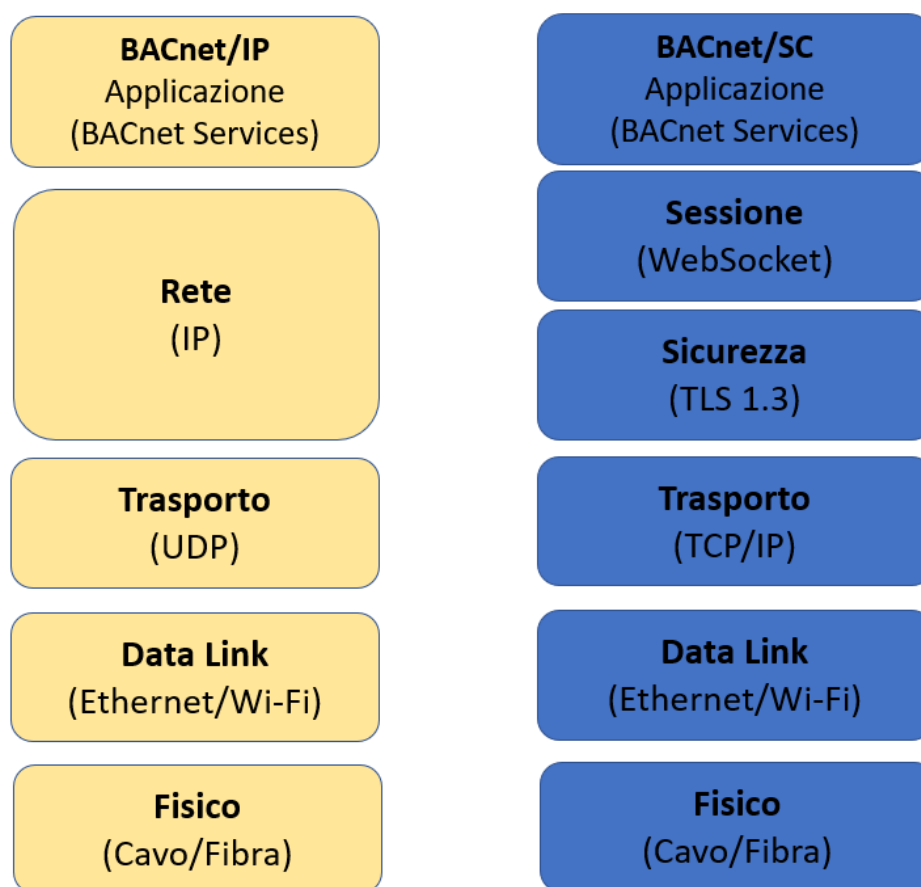


Figura 4.2. Confronto layer BACnet/IP vs BACnet/SC

BACnet/IP si basa su UDP e senza strato di sicurezza nativo, mentre **BACnet/SC** introduce livelli aggiuntivi HTTP, TLS 1.3, TCP, permettendo una comunicazione sicura e conforme alle moderne architetture IT.

Pertanto si ottiene con questo una sorta di topologia orientata all'IP, dove

- Tutto il BACnet è un "Application", incluso il BACnet/SC BACnet Datalink
- WebSockets è l' "Application Layer"
- TLS e TCP costituiscono il "Transport Layer"
- IPv4 o IPv6 è il "Internet Layer"
- Al "link Layer", qualsiasi tecnologia di collegamento dati possibile che support IPv4 o IPv6: Ethernet, WLAN, 4G/5G, ...

BacnetSC opera da Virtual Data Link per incapsulare i dati BACnet nativi utilizzando i protocolli sopra indicati.

Qui di seguito si presenta una tabella riassuntiva degli scenari descritti [4.3](#)

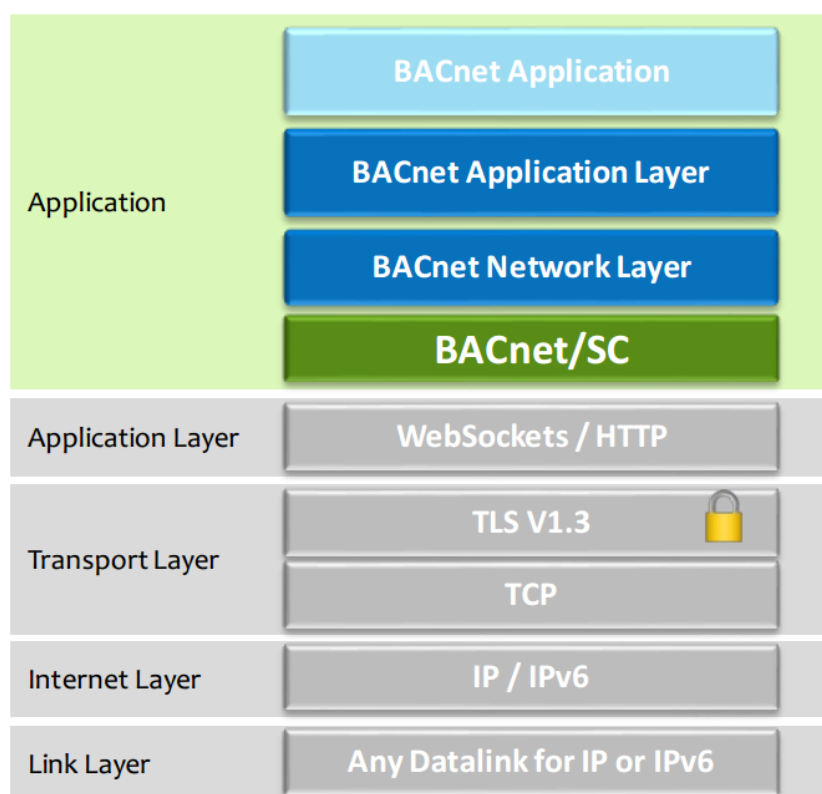


Figura 4.3. BACnetSC nel modello ISO/OSI

4.5 Applicazioni reali nei sistemi di automazione

BACnet e BACnet/SC trovano applicazione in una vasta gamma di contesti, dagli edifici intelligenti agli impianti industriali critici. L'implementazione di BACnet/SC può avvenire in molteplici modi seguendo diversi approcci per proteggere l'infrastruttura BACnet. In alcuni casi queste soluzioni possono risultare difficili da configurare e comportano un onere non trascurabile per la parte IT, è in questi casi che grazie a BACnet/SC si contribuirà a rendere l'uso di una infrastruttura di Building Automation sicura e standardizzata, pienamente compatibile con le implementazioni BACnet esistenti e conforme alle best practice IT che sono anche abilitanti per il cloud.

Nei sistemi HVAC avanzati, BACnet consente regolazioni dinamiche e ottimizzazione del comfort. In infrastrutture multisistema, agisce da backbone per l'integrazione di altri protocolli come KNX o Modbus.

La transizione verso BACnet/SC è spesso motivata da esigenze normative (NIS2, ISO 27001) e dall'esigenza di integrazione con reti IT. BACnet/SC rappresenta così una piattaforma per l'integrazione sicura e scalabile in edifici orientati al futuro.

La topologia impiegata da BACnet/SC è di tipo **hub-and-spoke**, dove abbiamo al centro un Hub che dirige il traffico tra gli n Nodi a questo collegati.

Il compito dell'Hub è quello di analizzare il traffico per determinare se deve essere inoltrato a un nodo diretto, ad un nodo terzo, o deve essere invece inoltrato a tutti i Nodi della rete.

Un nodo può essere controllore basico (ad esempio un attuatore o un termostato) o complesso (ad esempio un regolatore di una AHU o di un processo specifico) collegato direttamente alla rete BACnet esistente oppure attraverso un controllore padre che si interfaccia direttamente con la postazione di supervisione dell'intero impianto (B-AWS/B-OWS)

Come ben noto, un Hub può rappresentare un single point of failure, ecco perché i Nodi BACnet/SC supportano un meccanismo di Failover per garantire che il sistema rimanga operativo in caso di guasto o manutenzione preventiva. In fase di configurazione di ogni nodo, verrà stabilita se si tratta di un nodo Master o di Failover. Nella tabella 4.1 presentiamo un riepilogo del funzionamento Hub-Nodi.

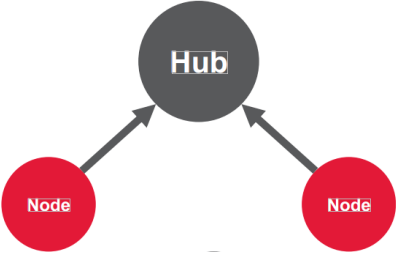
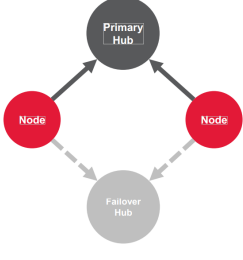
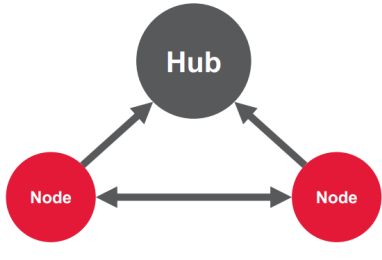
| | | |
|--|---|---|
|  |  |  |
| <p>L'Hub deve essere accessibile dai nodi. (necessario che abbia un IP raggiungibile dai nodi direttamente a lui connessi). Nella fase di discovery i singoli nodi contattano l'HUB Principale. Se si trovano interamente su una rete privata, non è necessario alcun indirizzo IP pubblico.</p> | <p>Lo standard consente l'uso di un hub di failover; così che il dispositivo di backup subentri se quello primario smette di funzionare o non risulta accessibile a livello network. I Nodi devono conoscere i hostname/ip dell'hub primario e di quello di failover.</p> | <p>Inizialmente, i Nodi si collegheranno all'Hub e inizieranno a comunicare con esso. Successivamente possono instaurare una comunicazione diretta tra loro in specifiche condizioni, sempre in modo crittografato/autenticato, riducendo il carico sull'hub, e il traffico di rete, ecc.</p> |

Tabella 4.1. Tabella di recap funzionamento Hub-Nodi

Capitolo 5

Proprietà di Sicurezza nei Sistemi BACnet

L'evoluzione dei Building Energy Management Systems (BEMS) verso ambienti sempre più connessi e intelligenti ha reso evidente la necessità di affrontare in modo sistematico i temi della **cybersecurity**. In questo contesto, BACnet – lo standard di comunicazione più diffuso nella building automation – è oggi al centro di una profonda trasformazione. Questo capitolo analizza i limiti strutturali della versione “classica” del protocollo, le innovazioni introdotte da **BACnet Secure Connect (SC)** e le strategie di protezione applicabili a livello di rete e di sistema.

5.1 Limiti strutturali del BACnet “classico”

Il BACnet originario, concepito negli anni '90, riflette un paradigma di sicurezza fisica e isolamento della rete, tipico delle infrastrutture OT tradizionali. In questo modello, i dispositivi di campo non erano esposti a reti pubbliche né a minacce cyber esterne. Tuttavia, la crescente integrazione con ambienti IT e l'adozione di BACnet/IP in scenari distribuiti rendono evidenti diverse criticità:

- **Assenza di autenticazione:** qualunque dispositivo sulla rete può inviare comandi a un altro, in assenza di meccanismi di identificazione affidabile.
- **Trasmissione in chiaro:** i messaggi BACnet/IP sono tipicamente non cifrati, esponendo i dati a sniffing e manipolazione.
- **Uso massivo di broadcast:** i messaggi Who-Is e I-Am, alla base della discovery, si basano su broadcast UDP, vulnerabili a exploit e attacchi DoS.
- **Mancanza di auditing nativo:** non esistono funzionalità standard di logging per operazioni di sicurezza o accesso.

Questi limiti richiedono un ripensamento architetturale per garantire **integrità, riservatezza e controllo degli accessi** nei moderni ambienti BEMS interconnessi.

5.2 Sicurezza applicativa in BACnet/SC: autenticazione, crittografia, trust

BACnet/SC, introdotto dallo standard **ASHRAE 135-2020**, affronta in modo nativo le esigenze di sicurezza attraverso un'architettura modernizzata basata su tecnologie consolidate nel mondo IT.

Le innovazioni chiave includono:

- **Comunicazione cifrata end-to-end:** l'utilizzo del protocollo TLS 1.3 su HTTP garantisce confidenzialità e integrità dei dati.
- **Autenticazione tramite certificati digitali X.509:** ogni nodo della rete deve essere autorizzato da una CA (Certification Authority) interna o esterna.
- **Sessioni persistenti:** le connessioni sono state concepite per mantenere stabilità, ridurre il traffico di discovery e mitigare i rischi di intercettazione.
- **Gestione centralizzata della fiducia (PKI):** è possibile controllare, aggiornare o revocare i certificati in modo centralizzato, seguendo un modello "zero trust" adattabile al contesto OT.

Con BACnet/SC, la sicurezza non è più demandata solo all'infrastruttura di rete ma diventa parte integrante del protocollo stesso, promuovendo una maggiore scalabilità e semplicità operativa.

5.3 Strategie di protezione: reti segregate, VPN, firewall

In scenari in cui BACnet SC non è ancora adottato, la protezione dei sistemi BEMS viene garantita attraverso misure di tipo infrastrutturale e perimetrale, tipiche della convergenza IT/OT. Le più comuni includono:

- **Segregazione fisica o logica delle reti OT:** separazione netta dei segmenti di rete che ospitano i dispositivi di automazione dagli ambienti IT, mediante VLAN o air-gap.
- **Firewall con regole applicative:** filtraggio del traffico BACnet/IP basato su porte UDP specifiche (in genere 47808) e segmentazione dei flussi.
- **VPN site-to-site:** utilizzate per connettere edifici remoti al supervisore centrale, mantenendo un canale cifrato attraverso Internet.
- **Sistemi di monitoraggio OT-aware (IDS/IPS):** dispositivi o software in grado di rilevare attività anomale o non autorizzate nel traffico BACnet.

Tali approcci sono utili ma non affrontano la sicurezza a livello di payload applicativo. L'adozione combinata di misure fisiche, logiche e protocollari diventa oggi indispensabile.

5.4 BACnet SC vs approcci infrastrutturali: confronto

Il confronto tra BACnet SC e le tecniche tradizionali di protezione OT evidenzia un cambio di paradigma. Mentre firewall e VPN operano “dall’esterno”, BACnet SC interna la sicurezza nel cuore della comunicazione. La tabella 5.1 riepiloga le differenze tra sicurezza IT e BACnet/SC.

| Criterio | Firewall / VPN / Segregazione | BACnet Secure Connect (SC) |
|----------------------------------|-------------------------------|--------------------------------------|
| Protezione del traffico interno | No | Sì (HTTP cifrato con TLS) |
| Gestione accessi dei dispositivi | Limitata | Certificati X.509 + CA |
| Complessità operativa | Alta | Media (PKI, automazione) |
| Visibilità e audit | Limitata | Possibile con TLS logging |
| Scalabilità multi-sito/cloud | Critica | Ottimizzata per ambienti distribuiti |

Tabella 5.1. Confronto caratteristiche di sicurezza IT e BACnet/SC

BACnet SC si configura quindi non solo come un’estensione del protocollo, ma come un’infrastruttura di sicurezza di nuova generazione, integrata e progettata per i BEMS del futuro. Dalla trattazione riteniamo anche utile specificare meglio con un elevato grado di sintesi, cosa NON è BACnet /SC ovvero:

- Non è una autorizzazione: tutti parlano con tutti
- Non è un tramite per instradare/routare altro traffico, ma solo BACnet
- Non è una strada per proteggere i device, ma solamente il collegamento di questi
- Non è disponibile su altri supporti
- Non è un set di strumenti per la crittografia



Figura 5.1. Canale sicuro Nodo-HUB o HUB-Nodo

Una rappresentazione di rete che riassume quest’ultimo concetto può essere riassunta nell’architettura di rete sintetica della Figura 5.2

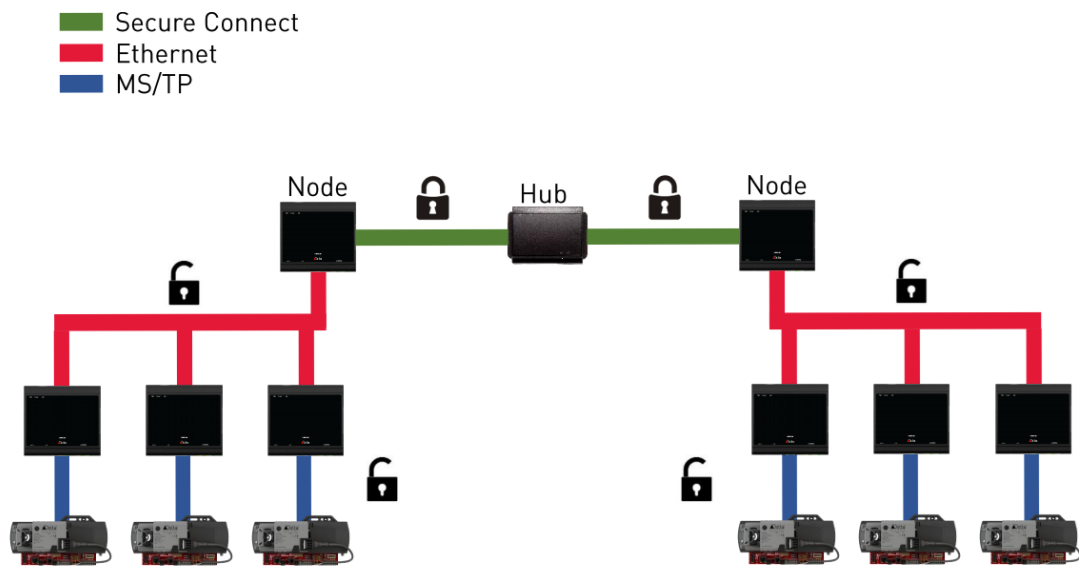


Figura 5.2. Architettura tipo con BACnet/SC

5.5 Scenari di implementazione BACnet/SC

Possiamo certamente affermare che BACnet/SC può essere implementato con diverse topologie architetture a seconda delle necessità di sicurezza da implementare e delle architetture BACnet presenti/disponibili. A scopo illustrativo riportiamo 4 possibili scenari astratti che possono essere affrontati in modo sicuro grazie a BACnet/SC

5.5.1 Scenario A - Accesso Sicuro dall'esterno della Struttura

Un edificio con un sistema BACnet esistente in cui il responsabile delle strutture deve accedere al sistema da remoto tramite Internet pubblico e non può consentire connessioni in entrata attraverso il firewall della rete dell'edificio.

In questo caso, viene aggiunto all'edificio un singolo nodo BACnet/SC che include un router BACnet per il routing al sistema BACnet legacy, viene implementato un hub BACnet/SC basato su cloud e viene utilizzato il software della workstation del nodo BACnet/SC.

Il nodo BACnet/SC dell'edificio avvia una connessione all'hub BACnet/SC nel cloud e, poiché il nodo dell'edificio avvia la connessione dall'interno dell'edificio, non è necessaria alcuna configurazione specifica nel firewall dell'edificio, ad eccezione delle connessioni HTTPS in uscita, che sono in genere già abilitate. Il responsabile della struttura utilizza il software della workstation per avviare una connessione con l'hub nel cloud e, una volta connesso, è in grado di gestire il sistema dell'edificio.

Nuove apparecchiature

- Router BACnet che supporta BACnet/SC
- Hub BACnet/SC - Primary Hub all'esterno della struttura
- Hub di failover BACnet/SC – Failover Hub (Opzionale) anch'esso all'esterno della Struttura
- B-OWS che supporta BACnet/SC

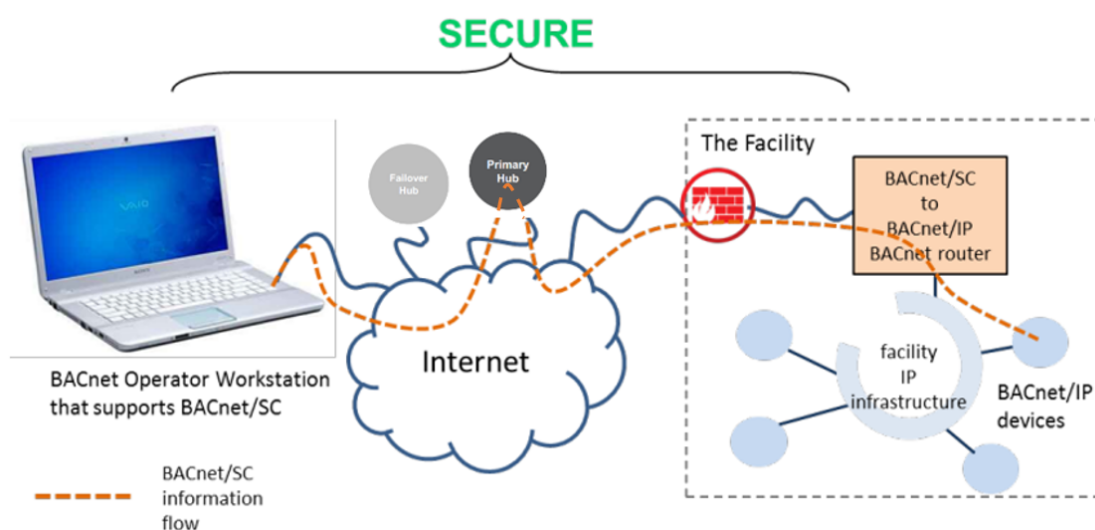


Figura 5.3. Scenario A BACnet/SC

5.5.2 Scenario B - Accesso Sicuro all'interno dell'edificio

Un nuovo edificio in cui le politiche IT non consentono il traffico BACnet non protetto su una rete IP condivisa.

In questo caso, tutti i dispositivi BACnet basati su IP dovranno supportare BACnet/SC. Sarà necessario installare un Hub BACnet/SC primario e di failover come parte della rete.

Nuove apparecchiature

- Dispositivi BACnet che supportano BACnet/SC
- Hub BACnet/SC – **Primary HUB**
- Hub di failover BACnet/SC - **Failover Hub**
- B-OWS che supporta BACnet/SC

The Facility

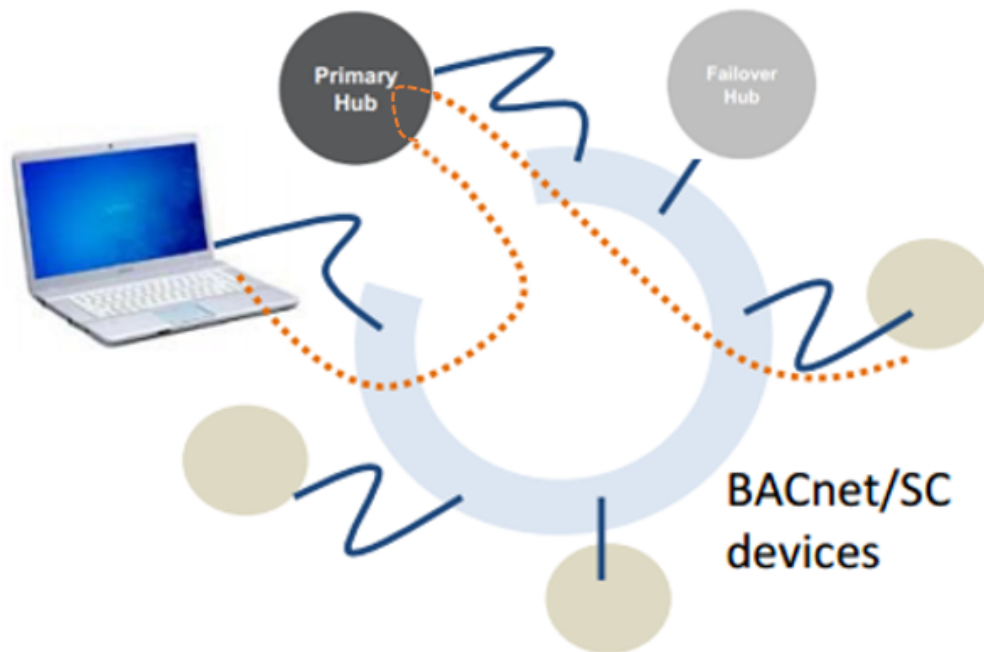


Figura 5.4. Scenario B BACnet/SC

5.5.3 Scenario C – Accesso sicuro all'esterno e all'interno della struttura con aree isolate

Un edificio che utilizza dispositivi misti sicuri e non sicuri/legacy.

In questo esempio, gli hub primario e di failover si trovano a valle del firewall e vengono utilizzati per proteggere i dispositivi BACnet/SC all'interno della struttura. È incluso un router da BACnet/SC a BACnet/IP per consentire la connettività tra la rete sicura BACnet/SC e le reti BACnet legacy. Sebbene sia possibile utilizzare un router tradizionale da BACnet/IP a MS/TP, l'esempio mostra anche un router da BACnet/SC a MS/TP che estende l'accesso sicuro al limite di un determinato trunk MS/TP. Si noti che ciò non protegge il trunk MS/TP stesso da soggetti con accesso fisico al trunk, ma protegge il trunk dall'accesso esterno dall'infrastruttura IP e da Internet. In questo esempio, l'accesso esterno (remoto) è fornito abilitando il firewall a inoltrare la porta BACnet/SC utilizzando un nome DNS pubblico o un indirizzo IP statico pubblico, in alternativa è possibile utilizzare una VPN Client-To-Site instaurata verso il Firewall per raggiungere l'HUB BACnet/SC.

Nuove apparecchiature

- Dispositivi BACnet che supportano BACnet/SC
- Hub BACnet/SC - Primary Hub

- Hub di failover BACnet/SC – Failover Hub (Opzionale)
- Router da BACnet/SC a BACnet/IP e/o MS/TP per connessioni legacy
- B-OWS che supporta BACnet/SC

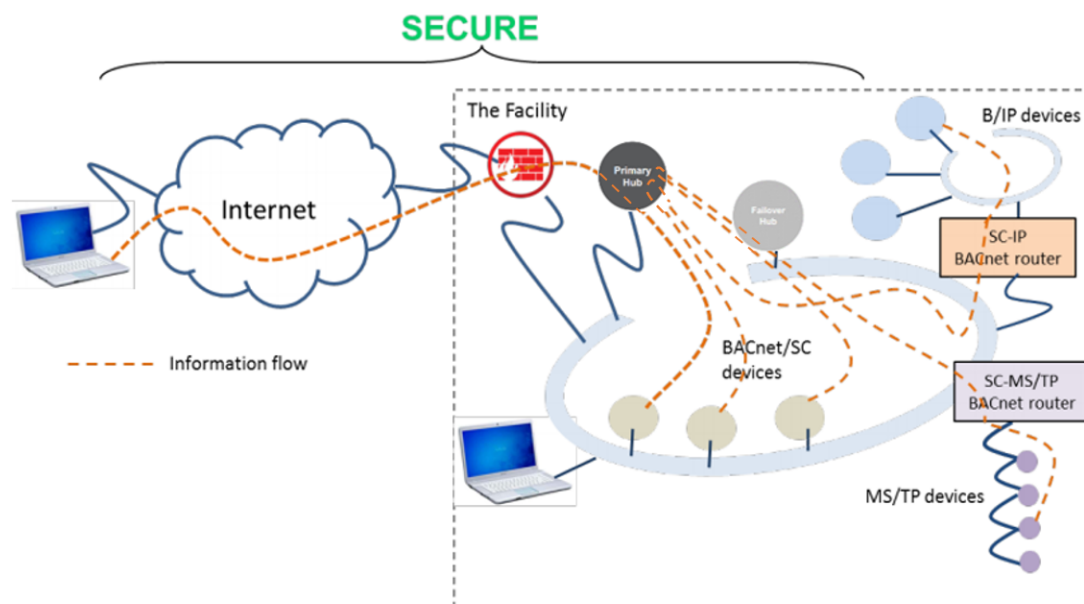


Figura 5.5. Scenario C BACnet/SC

5.5.4 Scenario D – Accesso Sicuro via Internet a diverse strutture

Una catena regionale di grandi magazzini gestita da un centro di gestione regionale con connettività tramite Internet pubblico o WAN. In questo esempio, gli hub primari e di failover si trovano nel cloud e ogni negozio dispone di una propria collezione di dispositivi BACnet/SC o di un router BACnet/SC-to-some other BACnet. Il diagramma mostra un router SC to-MS/TP, ma potrebbe trattarsi di un router SC-to-BACnet/IP o semplicemente di dispositivi BACnet/SC.

Nuove apparecchiature

- Dispositivi BACnet che supportano BACnet/SC e/o router BACnet da SC a MS/TP o IP
- Hub BACnet/SC - Primary Hub
- Hub di failover BACnet/SC – Failover Hub (Opzionale)
- B-OWS che supporta BACnet/SC

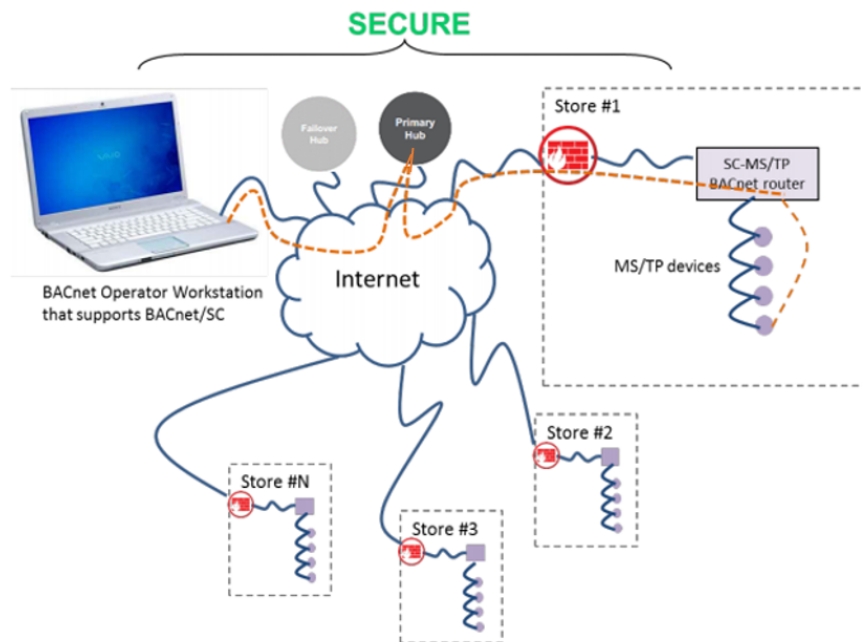


Figura 5.6. Scenario D BACnet/SC

5.6 Raffronti Architetture BACnet IP Vs BACnet/SC

Si ritiene utile offrire un parallelo in termini di organizzazioni di architetture di reti BACnet dove il parallelo BACnet SC e IP viene messo a confronto 1:1 prima di procedere poi in modo avanzato su alcuni casi studio che saranno elementi caratterizzanti di questo lavoro.

Qui di seguito due rappresentazioni possibili di architetture in cui è la postazione B-AWS/OWS a fungere da HUB oppure esiste effettivamente un Device che assolve questo compito (dentro o fuori l'architettura di rete locale).

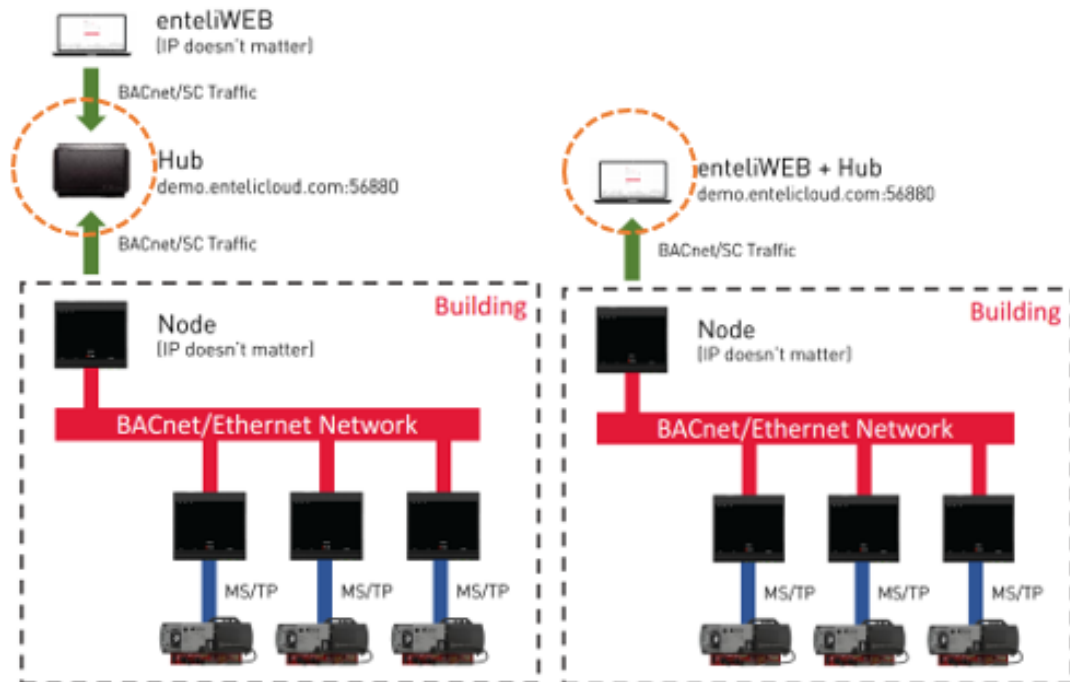


Figura 5.7. BACnet via BACnet-SC

Nella figura 5.7 viene riassunto la diversa collocazione dell'HUB che può essere sia il Software Applicativo BACnet oppure un controllore a cui il Software Applicativo BACnet si collega al pari dei controllori lato impianto.

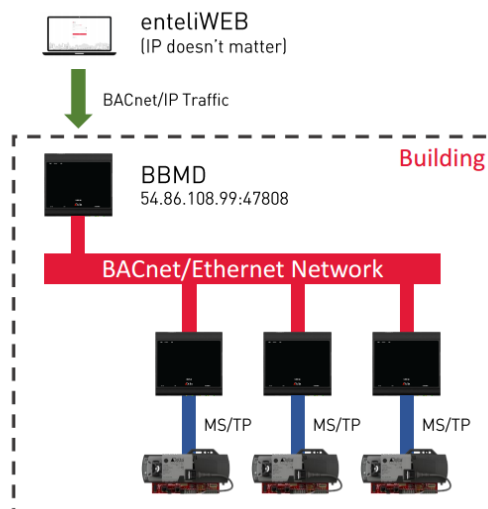


Figura 5.8. BACnet IP via BBMD

Nella figura 5.8 invece viene rappresentata la connessione tradizionale del software via BBMD, quando questo non è presente direttamente nella rete dei dispositivi in locale.

Da questa sintesi di distribuzione quindi può risultare utile fare un collegamento confrontando soluzioni di piccoli e grandi impianti BACnet più o meno distribuiti e che sfruttano BACnet a solo livello di protocollo o altresì anche a livello di sicurezza, al fine di mostrare i flussi informativi e la relativa sicurezza/implementazione.

A scopo illustrativo di dettaglio e per chiarire a livello di architettura le possibili metodologie di connessione via BACnet applicate in pratica, si immagina una soluzione di una piccola rete WAN e una più articolata, al fine di illustrare un approccio “classico” BACnet IP di riflesso a uno sicuro BACnet/SC in modo comparativo.

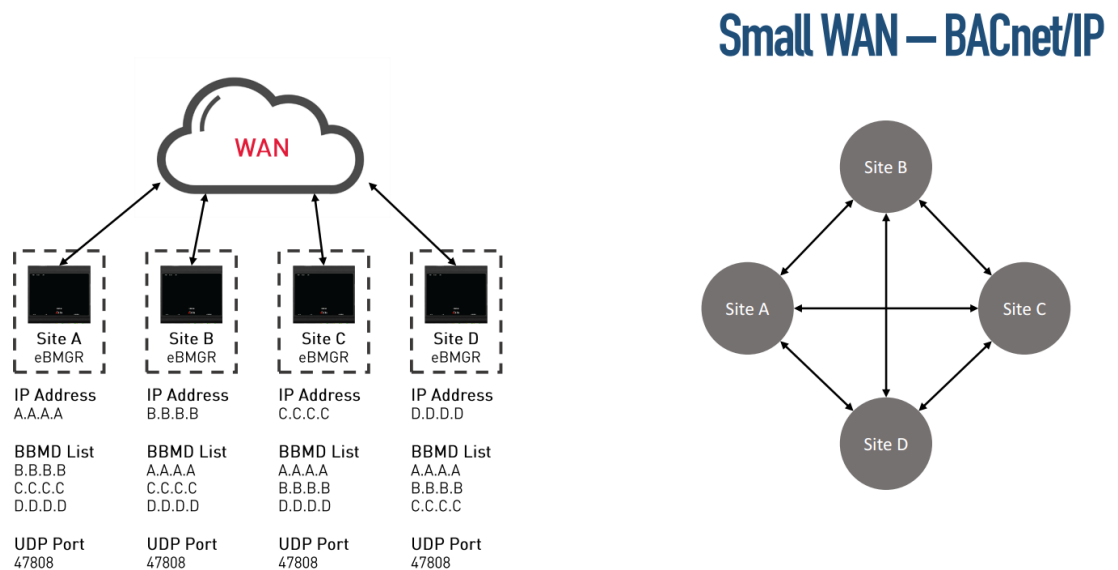


Figura 5.9. Architettura BACnet/IP in piccole reti

La architettura rappresentata figura 5.9 instrada una serie di connessioni di piccoli siti ad una WAN via BBMD classiche dove la connessione è bidirezionale, per cui sono necessarie le configurazioni lato IT adeguate per la gestione del protocollo UDP.

Small WAN – BACnet/SC

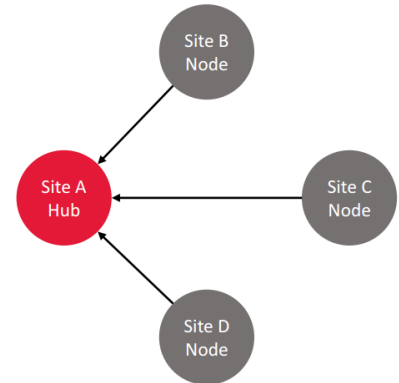
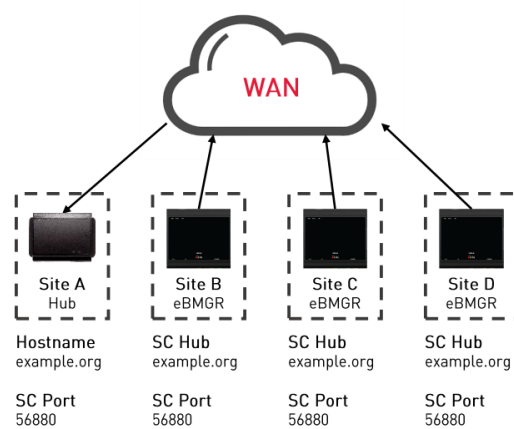


Figura 5.10. Architettura BACnet/SC in piccole reti

La architettura rappresentata figura 5.10 ricalca la necessità di connessione precedente ma solo che utilizza BACnet SC, per cui sono i nodi che raggiungono l'HUB, qui al contrario non sono necessarie rilevanti configurazioni lato IT ad eccezione dell'accesso HTTPS.

Large WAN – BACnet/IP

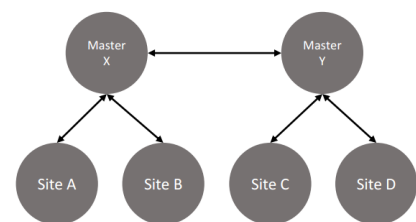
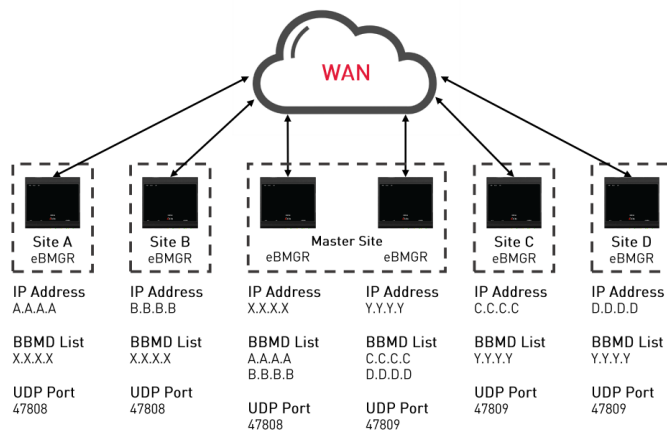


Figura 5.11. Architettura BACnet/IP in reti di dimensioni sostenute

La architettura rappresentata figura 5.11 instrada una serie di connessioni di siti con una struttura più complessa ad una WAN via BBMD classiche dove la connessione è bidirezionale, ma sono necessari dei Router aggiuntivi per lo scambio dati tra i siti, per cui sono necessarie le configurazioni lato IT adeguate per la

gestione del protocollo UDP su diverse porzioni della rete, infatti abbiamo diverse porte UDP attive.

Large WAN – BACnet/SC

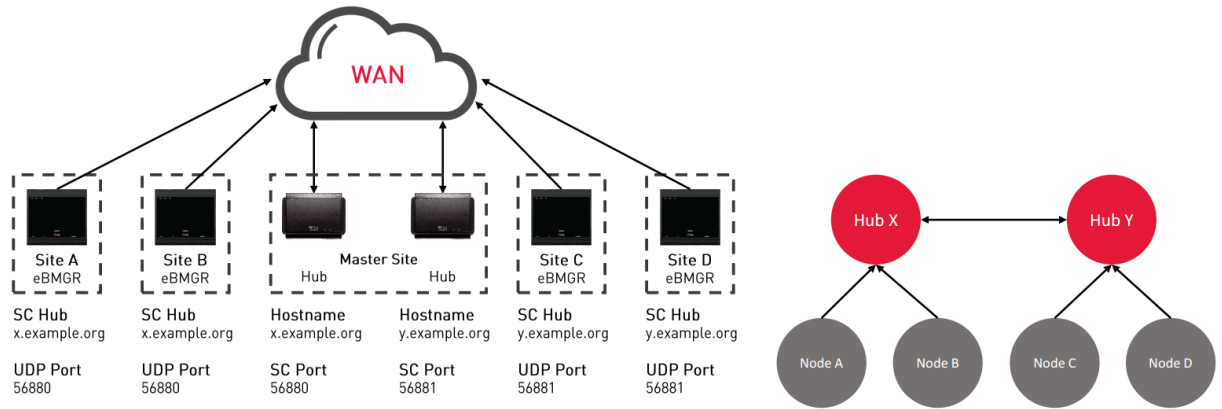


Figura 5.12. Architettura BACnet/SC in reti di dimensioni sostenute

La architettura rappresentata figura 5.12 ricalca la necessità di connessione precedente ma solo che utilizza anche in questo caso BACnet SC, per cui sono i nodi che raggiungono l'HUB, qui al contrario non sono necessarie rilevanti configurazioni lato IT ad eccezione dell'accesso HTTPS e la configurazione di rete è simile a quella rappresentata nella 5.10

Visti singolarmente i quattro scenari simili per coppia, si riporta in figura 5.13, un raffronto sintetico ed 1:1 dei casi BACnet IP VCs BACnet/SC dei due modelli di connessione affrontati a titolo di esempio.

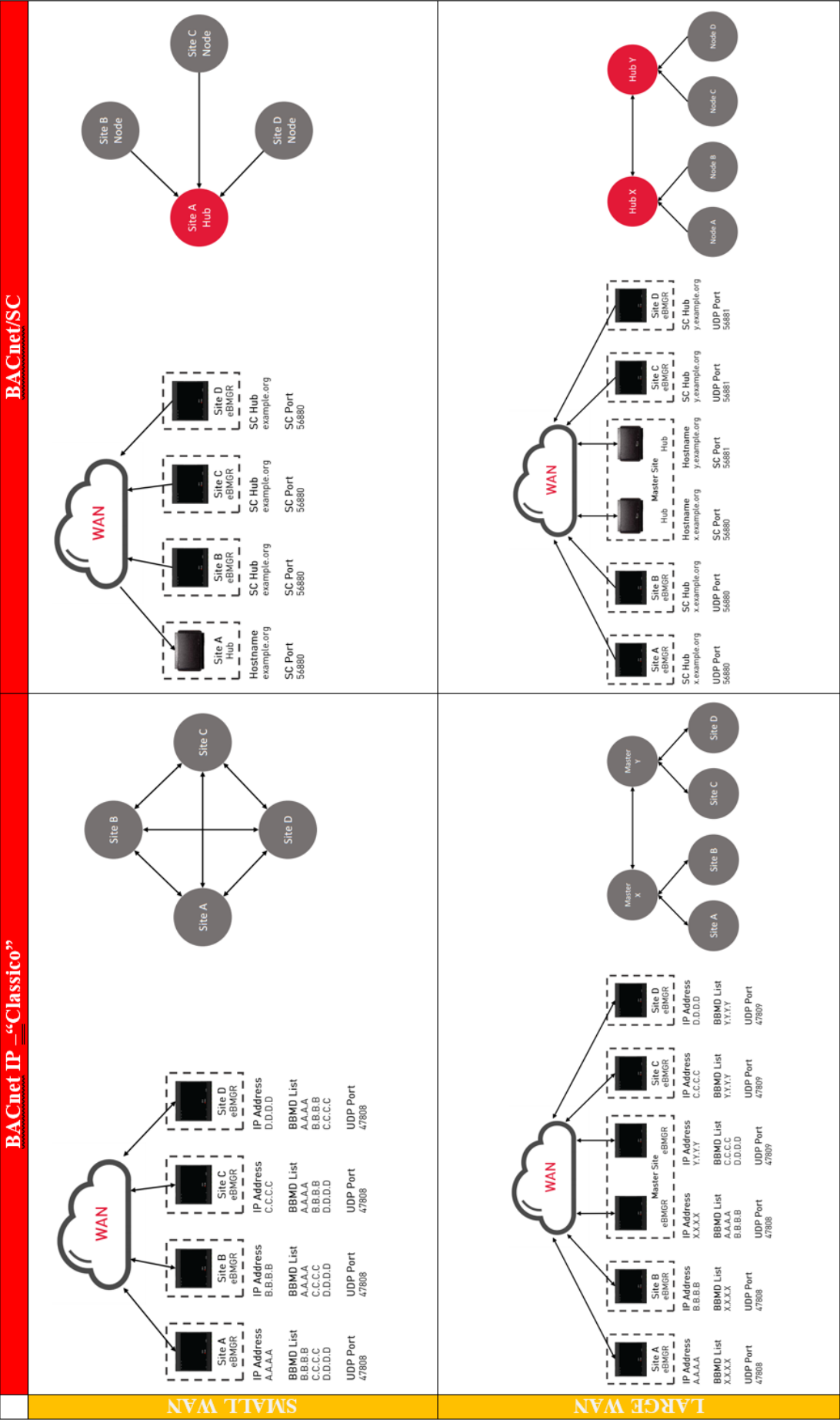


Figura 5.13. Confronto architetture BACnet e BACnet/SC in reti piccole e grandi

Capitolo 6

Rischi e Criticità nei Sistemi BEMS Interconnessi

I Building Energy Management Systems (BEMS), sempre più interconnessi e data-centrici, sono esposti a nuove minacce informatiche che possono compromettere non solo l'integrità dei dati, ma anche la continuità operativa degli impianti critici. In questo capitolo vengono analizzati i principali vettori di attacco, le debolezze architetturali più comuni, le pratiche consolidate per la mitigazione e i criteri professionali per la **validazione della sicurezza** dei sistemi BEMS.

L'interconnessione dei sistemi BEMS con reti aziendali, cloud e dispositivi intelligenti ha trasformato radicalmente il profilo di rischio di questi ambienti. Dall'accesso fisico si è passati a una molteplicità di **vettori digitali** che espongono gli impianti a minacce persistenti, complesse e spesso non visibili con strumenti tradizionali OT.

La trasformazione digitale degli edifici ha reso i sistemi BEMS obiettivi sempre più esposti ad attacchi informatici. Le minacce possono essere classificate in base al **vettore d'ingresso**, al **tipo di impatto** e alla **motivazione**.

Alcuni tra i principali vettori di minaccia possono essere ricondotti a:

- **Accessi remoti non protetti** (VPN mal configurate, porte aperte verso Internet)
- **Dispositivi obsoleti** (firmware vulnerabili, patch mancanti)
- **Protocolli non sicuri** (es. BACnet classico in chiaro)
- **Fornitori terzi** con accesso alla rete (manutenzione, cloud, diagnostica)
- **Attacchi interni** (malware su dispositivi o operatori malintenzionati)

Da una analisi progressiva gli impatti potenziali di queste minacce, nella normalità imprevedibile possono sfociare in

- **Interruzione dei servizi:** HVAC, illuminazione, antincendio e molto altro

- **Manomissione dei dati:** falsificazione letture o comandi
- **Esfiltrazione di dati energetici o sensibili**
- **Compromissione della reputazione o responsabilità legale**

Quanto appena epilogato mette in evidenza rischi e nuove necessità emergenti per porre rimedio a quelle che sono le vulnerabilità comuni delle architetture BEMS. Di fatto sappiamo che le reti BEMS sono spesso progettate per l'affidabilità operativa, ma non per **la resilienza informatica**. Questo le rende vulnerabili a diverse problematiche strutturali, infatti questo rappresentano storicamente

- **Architetture piatte e non segmentate:** Tutti i dispositivi condividono la stessa subnet → facilità di propagazione malware.
- **Possibilità di accesso diretto a livello di Automazione:** Supervisor esposti senza proxy o gateway → superficie d'attacco ampia e disarmata anche di fronte a principianti malintenzionati (hacker).
- **Assenza di logging e monitoraggio eventi/accessi:** Nessun controllo su eventi anomali, accessi remoti o configurazioni sospette.
- **Protocollo BACnet in chiaro:** Scambi leggibili, modificabili o intercettabili senza alcuna cifratura.
- **Mancanza di policy di aggiornamento:** Firmware e software non aggiornati → vulnerabilità note sfruttabili facilmente solitamente gli impianti vengono dimenticati fino a quando non sono obsoleti, tanto questi sono più complessi tanto il fenomeno + più eclatante e pari-merito pericoloso

Questo scenario in prima approssimazione ha reso la necessità di trovare le prime soluzioni “empiriche” per attuare le mitigazioni dei rischi descritti in precedenza, ed è per questo che i primi approcci classici applicati alle architetture BEMS hanno puntato ad **Rete Segregate** e **VPN**.

Prima dell'introduzione di BACnet/SC, i meccanismi classici per mitigare i rischi erano principalmente **infrastrutturali**:

- **Rete segregata (air-gapped o VLAN isolate):**
 - Separazione fisica o logica tra reti IT e OT.
 - Uso di firewall industriali tra segmenti.
 - Limitazione dei protocolli inter-VLAN (es. solo BACnet/IP).
- **VPN e accesso remoto sicuro:**
 - Autenticazione multi-fattore per accessi da esterno.
 - Tunnel cifrati con gestione centralizzata dei certificati.
 - Logging di accessi e autorizzazioni granulari.

Questi metodi **restano validi** e sono spesso **complementari a BACnet/SC**, specie in contesti legacy o ibridi.

6.1 Superfici di attacco e minacce in ambienti OT

Le architetture BEMS moderne integrano una vasta gamma di componenti: controllori, sensori, attuatori, gateway multi-protocollo, interfacce HMI, server SCADA, portali cloud, ecc. Ciascun elemento rappresenta un possibile **entry point** per un “attaccante”.

Tra le principali superfici d’attacco:

- **Connessioni remote mal configurate** (VPN, port forwarding, accessi diretti ai supervisori o anche ai controllori o gateway in campo)
- **Dispositivi legacy con firmware obsoleto**
- **Gateway multi-protocollo esposti con regole firewall permissive**
- **Supervisori o dashboard con credenziali deboli o predefinite**
- **Mancanza di segmentazione interna**

Queste vulnerabilità sono sfruttate da malware, botnet, ransomware o attacchi mirati a impianti critici, che in modo molto semplice, per non dire spesso banale, si rivelano “distruttivi” (perdite di dati, blocchi di processi, alto).

6.2 Discovery, spoofing, broadcast storm, man-in-the-middle

I protocolli OT, inclusi quelli per Building Automation, sono stati progettati per ambienti “fidati”, con **modelli di comunicazione basati sull’affidabilità implicita**.

Le vulnerabilità tipiche includono:

- **Service Discovery non autenticato** (Who-Is / I-Am in BACnet): mappatura semplice dell’intera topologia di rete.
- **Spoofing di dispositivo**: un attaccante può impersonare un controllore o un attuatore, influenzando direttamente il funzionamento dell’impianto.
- **Broadcast Storm**: l’eccesso di messaggi broadcast può saturare la rete, causando ritardi, time-out o blocchi.
- **Man-in-the-Middle (MITM)**: in assenza di crittografia, il traffico può essere intercettato, alterato o registrato senza lasciare tracce visibili.

Queste tecniche sono sempre più automatizzate all’interno di toolkit di attacco (es. BACNet Exploiter, ScapyBACnet).

6.3 Interoperabilità incompleta e versioning

L'interoperabilità dichiarata tra dispositivi BACnet può rivelarsi problematica in ambienti reali. I fattori critici includono:

Versioni dello standard diverse: un supervisore recente potrebbe non riconoscere correttamente oggetti di un controllore più vecchio, “Backward Compatibility” non sempre garantita dai produttori.

Implementazioni parziali: alcuni dispositivi supportano solo un sottoinsieme di oggetti o servizi, senza notificarlo esplicitamente. La profondità dell'implementazione dello standard dipende dal produttore e non è insita nello standard stesso.

Ambiguità semantiche nella rappresentazione dei valori: es. “temperatura setpoint” codificata in modi differenti.

Gateway multi-protocollo che eseguono mappature errate o approssimative dovendo ricostruire informazioni non sempre complete all'origine.

Questi problemi possono compromettere l'affidabilità del sistema, generare **fault silenziosi** e ostacolare il monitoraggio.

6.4 Limiti degli approcci tradizionali alla sicurezza

Sebbene le difese infrastrutturali abbiano rappresentato per anni un valido primo livello di protezione, oggi rischiano sempre di più di esse non sono sufficienti. I principali limiti includono:

- **Protezione perimetrale fragile:** un singolo ingresso compromesso (es. VPN) può esporre l'intero sistema.
- **Assenza di visibilità profonda nel traffico OT**
- **Rigidità architetturale:** difficile integrazione con sistemi cloud, analisi predittive o piattaforme AI.
- **Dipendenza da competenze IT elevate** per configurare correttamente firewall, VLAN, tunnel, ecc.

Serve dunque un nuovo approccio alla sicurezza: distribuito, nativo nei protocolli, adattivo e in grado di rispondere in tempo reale alle minacce emergenti. E di questo i produttori e le associazioni che supportano lo standard se ne sono resi conto, spesso anche a duro prezzo, tanto da decidere di elevare dall'interno del protocollo una parte di sicurezza della gestione di dati e processi.

Con l'adozione di BACnet Secure Connect, la sicurezza viene gestita a livello applicativo, con un modello nativamente conforme agli standard IT.

Elementi chiave del modello SC:

- **TLS 1.3:** cifratura end-to-end tra dispositivi autorizzati.
- **Mutua autenticazione:** solo dispositivi dotati di certificato valido possono partecipare.
- **Eliminazione del broadcast:** riduzione del traffico visibile in rete.
- **Trust group centralizzati:** gestione scalabile delle identità digitali.

BACnet/SC abilita anche l'**integrazione con SIEM (Security Information and Event Management)** e sistemi di monitoraggio IT standard, migliorando la visibilità e la risposta agli incidenti.

Quanto affrontato in questa sezione ci porta a concludere che vi sia la necessità di criteri professionali di validazione della sicurezza. Possiamo quindi affermare che un sistema BEMS sicuro deve essere valutato secondo **criteri tecnici oggettivi**.

Di seguito la tabella 6.1, presenta una sintesi dei principali ambiti da verificare:

| Criterio | Descrizione |
|---------------------------------|---|
| <i>Segmentazione della rete</i> | Presenza di VLAN/DMZ per separare traffico IT e OT o SW Applicativo |
| <i>Accesso remoto sicuro</i> | VPN con MFA, log accessi e gestione certificati |
| <i>Patch Management</i> | Aggiornamenti programmati e periodici a Firmware e Applicativi su rilasci dei produttori - FixCVE |
| <i>Logging & auditing</i> | Supervisione continua, monitoraggio traffico e registrazione eventi |
| <i>Sicurezza dei protocolli</i> | Uso di BACnet/SC o altri protocolli cifrati |
| <i>Autenticazione forte</i> | Autenticazione di dispositivi e utenti tramite certificati o MFA |
| <i>Backup e ripristino</i> | Piano di disaster recovery documentato e testato |
| <i>Security Audit</i> | Analisi proattiva delle vulnerabilità e penetration test (opzionale) tramite strumenti automatici |

Tabella 6.1. Tabella criteri di valutazione rischi e validazione

Questi criteri possono essere **formalizzati in check-list** e audit periodici per garantire **conformità normativa** (es. ISO 27001, IEC 62443) o semplicemente **buone pratiche operative**.

I sistemi BEMS, in quanto elementi centrali dell'edificio intelligente, devono essere progettati e gestiti con attenzione alla sicurezza informatica. Il passaggio da architetture isolate a modelli connessi e interoperabili impone un cambio di paradigma: dalla semplice protezione perimetrale alla **sicurezza nativa dei protocolli**, come BACnet/SC. La valutazione periodica della **postura di sicurezza**, basata su criteri strutturati e misurabili, rappresenta il fondamento per garantire affidabilità, continuità e fiducia negli ambienti costruiti digitali.

Capitolo 7

Validazione della Sicurezza nei BEMS: Metodologia Proposta e Casi Studio

L'adozione di standard di comunicazione sicuri come **BACnet/SC** non è sufficiente, da sola, a garantire la **sicurezza effettiva** dei Building Energy Management Systems. Occorre infatti disporre di una **metodologia di validazione** che consenta di valutare in modo sistematico l'efficacia delle contromisure adottate, identificare eventuali lacune e supportare processi di miglioramento continuo.

In questo capitolo si propone una metodologia di validazione **tecnico-procedurale**, pensata per essere applicata a sistemi BEMS in esercizio o in fase di progettazione, con focus su interoperabilità, sicurezza e compliance normativa.

7.1 Obiettivi della validazione

L'obiettivo della validazione della sicurezza nei sistemi BEMS non è semplicemente quello di verificare la presenza di tecnologie aggiornate o protocolli sicuri, ma piuttosto di **valutare l'intero sistema in termini di resilienza, affidabilità e capacità di risposta alle minacce informatiche**, in un contesto integrato IT/OT.

La metodologia proposta si basa su una visione **funzionale e strutturata**, che mira a rispondere a specifici interrogativi professionali riguardo alla “**postura/livello**” di **sicurezza dell'impianto**, sia in fase di esercizio che di progetto. Gli obiettivi principali sono i seguenti:

1. Misurare il livello di esposizione al rischio informatico

Questa attività serve a comprendere quanto un determinato sistema BEMS sia realmente **vulnerabile** agli attacchi esterni o interni. La valutazione si concentra sulla **facilità con cui un potenziale attaccante** potrebbe accedere, manipolare o interrompere le funzioni chiave del sistema. Si tiene conto della presenza (o assenza) di:

- segmentazione di rete
- autenticazioni
- protocolli cifrati
- protezioni fisiche e logiche

L'obiettivo è fornire una **fotografia del rischio effettivo**, supportata da dati tecnici e osservazioni dirette.

2. Valutare la coerenza architetturale tra progetto e implementazione

Molti impianti, pur essendo progettati con criteri moderni, vengono poi implementati con **scostamenti significativi** che ne compromettono l'efficacia. Questa fase della validazione mira a confrontare la **documentazione di progetto** (planimetrie, schemi di rete, dichiarazioni funzionali) con la **configurazione reale** dei dispositivi, delle reti e delle politiche di accesso.

L'obiettivo è evidenziare discrepanze e **non conformità operative**, al fine di correggere eventuali deviazioni o consolidare la coerenza del sistema.

3. Supportare decisioni su interventi correttivi e migliorativi

La validazione non ha un valore puramente **diagnostico**, ma anche decisionale. I risultati ottenuti devono fornire al responsabile dell'impianto, al progettista o al gestore un **quadro chiaro delle priorità tecniche**, utile a:

- pianificare aggiornamenti tecnologici,
- ottimizzare la gestione degli accessi remoti,
- decidere se e come adottare protocolli sicuri come BACnet/SC,
- bilanciare esigenze di sicurezza, comfort e continuità operativa.

L'obiettivo è quello di **orientare gli investimenti** verso azioni ad alto impatto sulla resilienza del sistema.

4. Favorire la conformità a standard di settore

In un contesto sempre più regolamentato, le infrastrutture BEMS possono rientrare tra i sistemi critici ai sensi di normative come:

- **ISO/IEC 27001** (gestione della sicurezza informatica),
- **IEC 62443** (sicurezza dei sistemi di controllo industriale),
- **GDPR** (protezione dei dati),
- **Linee guida AgID/ENISA** (per la PA o impianti strategici).

Attraverso la metodologia proposta, la validazione supporta anche un percorso verso la **compliance normativa**, tracciabile e "auditabile".

7.2 Struttura della metodologia

La metodologia proposta per la validazione della sicurezza nei BEMS si articola in **cinque fasi operative**, ciascuna delle quali è finalizzata a individuare specifici aspetti di rischio e a predisporre le basi per un intervento correttivo o di miglioramento. L'approccio è **sequenziale ma modulare**, per consentire applicazioni flessibili anche su impianti esistenti o solo parzialmente documentati.

1. Fase - Mappatura del sistema BEMS

In questo punto l'obiettivo è ottenere una **visione completa e documentata dell'infrastruttura attuale**, identificando tutti gli elementi coinvolti nella comunicazione e gestione energetica dell'edificio.

In questa fase si raccolgono le informazioni essenziali per comprendere la struttura del sistema:

- Identificazione dei componenti fisici e logici (controllori, sensori, gateway, server di supervisione).
- Censimento dei protocolli di comunicazione impiegati (es. BACnet/IP, MS/TP, Modbus).
- Mappatura dei flussi di dati tra dispositivi OT e sistemi IT.
- Individuazione dei percorsi di accesso remoto (VPN, desktop remoto, portali web).

Questa attività è fondamentale per delineare il perimetro della validazione e localizzare i punti di possibile vulnerabilità.

2. Fase - Valutazione architetturale

In questo punto l'obiettivo è analizzare **l'organizzazione topologica e la segmentazione della rete**, evidenziando eventuali incoerenze con le best practice in ambito IT/OT.

La valutazione riguarda:

- La presenza (o assenza) di segmentazione tra rete IT e OT (es. VLAN dedicate, DMZ industriali).
- Le modalità di instradamento e visibilità tra dispositivi (routing, NAT, proxy).
- Il bilanciamento tra disponibilità operativa e isolamento logico.
- La capacità della rete di contenere la propagazione di minacce in caso di compromissione.

Questa fase consente di giudicare la **robustezza strutturale** della rete e la sua predisposizione a gestire in sicurezza il traffico BEMS.

3. Fase - Verifica dei protocolli e della sicurezza applicativa

In questo punto l'obiettivo invece è analizzare i **meccanismi applicativi di sicurezza** adottati per la trasmissione dei dati e il controllo degli accessi all'interno del sistema BEMS.

In particolare, si verifica:

- Se il protocollo in uso supporta la **cifratura end-to-end** (es. TLS 1.3 per BACnet/SC).
- L'utilizzo (o meno) di meccanismi di **autenticazione dispositivi e utenti**.
- La gestione degli **aggiornamenti firmware/software** nei dispositivi chiave.
- La presenza di **sistemi di logging**, audit e alerting in tempo reale.

Il focus è su **integrità, riservatezza e tracciabilità**, elementi essenziali per evitare manipolazioni e accessi non autorizzati.

4. Fase - Test e simulazioni controllate

In questo punto l'obiettivo è verificare **in condizioni simulate o controllate** la reazione del sistema a eventi imprevisti, scenari di errore o attacchi informatici.

Questa fase, che può variare in complessità, include:

- Test di penetrazione selettivi (penetration test) in ambiente sandbox o con strumenti automatici.
- Simulazione di disservizi (disconnessione di dispositivi critici, crash di hub, failover).
- Analisi dei log e dei sistemi di notifica per rilevare anomalie.
- Verifica della capacità di **recupero automatico** o manuale (disaster recovery).

Questa attività misura il **livello di resilienza operativa e sicurezza dinamica** del sistema BEMS.

5. Fase - Classificazione del rischio e raccomandazioni

In questo punto l'obiettivo è sintetizzare i risultati ottenuti in un **profilo di rischio coerente e interpretabile**, da cui derivare interventi di miglioramento tecnico e organizzativo.

L'attività conclusiva prevede:

- Assegnazione di punteggi ai vari domini di sicurezza (rete, protocolli, autenticazione...).
- Elaborazione di un **report tecnico con raccomandazioni operative**, classificate per priorità.
- Supporto alla pianificazione di un piano d'azione, anche su più fasi (es. transizione graduale verso BACnet/SC).

Questa fase rappresenta l'output tangibile dell'intero processo e fornisce le basi per un **ciclo virtuoso di revisione e miglioramento continuo**.

7.3 Griglia di validazione e punteggio

Nel tentativo di definire un metodo abbiamo puntato come obiettivo quello di fornire un **modello di riferimento pratico e misurabile** per classificare in modo oggettivo il livello di sicurezza raggiunto da un sistema BEMS, facilitando la comparabilità tra sistemi diversi o nel tempo. Con la volontà di creare uno strumento utile, immaginiamo una griglia di validazione accompagnata da un sistema di valutazione a punteggio.

La griglia proposta si basa su un sistema di punteggio per ciascun dominio critico, come:

- la segmentazione di rete,
- la sicurezza del protocollo di comunicazione,
- l'autenticazione,
- la gestione degli aggiornamenti,
- il logging e il controllo degli accessi remoti.

Per ogni **criterio** viene assegnato un punteggio tra **0 e 2**, dove:

- **0** indica assenza o condizione critica,
- **1** una condizione parziale o sub-ottimale,
- **2** una conformità piena o buona pratica consolidata.

Questa classificazione semplifica il confronto e la definizione delle priorità di intervento, specialmente in contesti multi-sito o con infrastrutture complesse.

La tabella 7.1 rappresenta un esempio di checklist tecnica con scoring associato per la valutazione:

| Dominio | Verifica | Stato | Punteggio (0-2) |
|-----------------------------|--|----------|-----------------|
| Segmentazione della rete | VLAN o firewall tra IT/OT | Si | 2 |
| Protocollo sicuro | Uso di BACnet/SC o TLS attivo | No | 0 |
| Autenticazione utenti | Autenticazione a due fattori | Si | 2 |
| Logging eventi critici | Registrazione centralizzata di accessi e allarmi | Parziale | 1 |
| Patch and firmware | Policy definita e tracciata | No | 0 |
| Supervisione accessi remoti | VPN con MFA, ACL e scadenza certificati | Si | 2 |

Tabella 7.1. Tabella di valutazione con score per validazione

Totale ottenuto: 7/12 → Livello sicurezza: **Intermedio**, azioni migliorative raccomandate.

- Una raccomandazione possibile: procedere all'attivazione di protocolli sicuri e rafforzare il controllo degli aggiornamenti.

7.4 Integrazione con audit e compliance

Qui l'obiettivo è quello di illustrare come la metodologia proposta possa essere **armonizzata all'interno dei processi organizzativi esistenti**, in particolare nelle aziende e negli enti pubblici che già adottano sistemi di gestione per la sicurezza e la qualità.

La validazione può essere integrata nei seguenti ambiti:

- **Audit di sicurezza periodici:** la checklist tecnica può essere usata come base per le verifiche ricorrenti sull'infrastruttura BEMS.
- **Commissioning e collaudi funzionali:** durante la messa in servizio, la metodologia aiuta a formalizzare il controllo della componente informatica oltre a quella funzionale.
- **Compliance normativa** (es. GDPR, ISO 27001): molti standard richiedono dimostrazione di misure di sicurezza in fase documentale. La metodologia proposta si presta a essere tracciabile, con evidenze tecniche e verbali allegabili ai fascicoli impiantistici.
- **Business continuity e risk management:** i dati raccolti nella validazione possono essere inseriti nei piani aziendali di gestione dei rischi, migliorando la capacità di reazione a eventi cyber.

In sintesi, la metodologia può essere **istituzionalizzata** nei processi interni, elevando il profilo professionale della manutenzione e della gestione tecnica dei sistemi BEMS.

7.5 Esempio applicativo semplificato

In questo esempio l'obiettivo è fornire un **caso concreto di applicazione della metodologia**, dimostrando come essa possa essere usata nella pratica per identificare criticità e indirizzare azioni correttive in modo misurabile.

Scenario: Un impianto HVAC con supervisione centralizzata BACnet/IP è installato in un edificio scolastico con accesso remoto per i tecnici esterni.

Risultati della validazione:

- Rete OT senza VLAN: **0 punti**
- Supervisore accessibile da IP pubblico, senza VPN: **0 punti**
- Nessun meccanismo di autenticazione utenti o dispositivi: **0 punti**
- Nessun logging o tracciabilità degli eventi: **0 punti**
- Protocollo in chiaro (BACnet/IP non cifrato): **0 punti**

Totale: 0/12 – Livello di sicurezza critico

Raccomandazioni:

- Implementare una **VLAN dedicata per la rete OT** con firewall tra IT e BEMS.
- Adottare una **VPN con autenticazione a due fattori** per gli accessi remoti.
- Migrare progressivamente a **BACnet/SC**.
- Attivare logging centralizzato e meccanismi di auditing.
- Definire una **politica di aggiornamento firmware** con tracciabilità.

Questo esempio dimostra come, anche in contesti reali con risorse limitate, la metodologia consenta di avviare un processo strutturato di **miglioramento progressivo**, permettendo così agli attori coinvolti ciascuno con il proprio ruolo e responsabilità di pianificare interventi mirati e monitorare l'efficacia nel tempo

La validazione della sicurezza nei BEMS non può essere improvvisata né affidata a controlli isolati. Serve una metodologia strutturata, tecnica e integrabile nei processi di governance aziendale. Il modello proposto in questo capitolo fornisce una base pratica per audit, collaudi e adeguamenti di impianti esistenti o in fase di progettazione, orientando la transizione verso architetture cifrate, certificate, segmentate e monitorate, in linea con le best practice IT/OT.

7.6 Casi Studio Reali

In questo capitolo vengono presentati e analizzati **diversi casi reali** di implementazione di sistemi BEMS con focus su **interoperabilità, sicurezza e architettura di rete**. Ogni scenario è stato selezionato per evidenziare scelte progettuali significative, punti critici ricorrenti e strategie adottate per garantire efficienza, comfort e protezione informatica nell'ambito dell'interoperabilità.

7.6.1 Caso Studio A – Edificio Direzionale con rete segregata e BACnet/IP

Contesto:

- Edificio Alto di recente costruzione, destinato ad uffici aziendali, Multi Tenant, infrastruttura ad alta densità energetica
- BEMS su server Locale composto da controllori DDC, supervisione locale senza integrazione con rete aziendale ma con postazione dedicata per la gestione del Facility da un PC collegato sulla rete dei Server
- Livello di affollamento quotidiano da 2500-4000 persone al giorno

Architettura:

- Rete OT con diverse VLAN ma comunque tutto completamente e fisicamente separata dalla rete IT aziendale del Cliente.
- Dispositivi circa +700 controllori BACnet:
 - DDC BACnet/IP, con indirizzamento privato statico e distribuzione su diverse VLAN interne.
 - * Device Multivendor a Livello DDC (B-BC, B-ASC, B-A)
 - DDC BACnet/IP che fungono da Gateway da **altri protocolli standard** a BACnet per prodotti (Attuatori, Sensori, PdC, Chiller, VAV, Schermature, Gestione Ambienti, Gestione Carichi, Gestione Illuminazione, Automazioni dei comandi elettrici, o controllori) che supportano comunicazioni su protocolli standard come:
 - * MODBUS RTU
 - * MODBUS TCP
 - * MBUS 485
 - * DALI
 - * KNX
 - DDC BACnet/IP che fungono da Gateway (B-BC/B-GW) da protocolli proprietari a BACnet per sistemi come
 - * Rivelazione Incendi
 - * Gestione Ascensori
 - * Gestione UPS e GE
 - * Sistemi di Spegnimento
 - * Sistemi gestione delle emergenze di Public Addressing
- Entità delle informazioni gestite, +40.000 data-point fisici, + 500.000 oggetti BACnet (data-point virtuali), tutto in realtime.
- Supervisioni Locali in specifico ambiente Locale Telecontrollo interno per Manutenzione e/o in postazioni Dedicate all'interno dell'edificio collegate direttamente alla rete OT anche per il cliente Finale su una VLAN in grado di vedere solamente i Server e non i controllori con regole firewall a doppio livello.
- Un totale attuale di 7 BBMD per raggruppamento piani sulle diverse VLAN
- Avviato processo di analisi per implementazione VPN per accesso segregato al server di supervisione su VM per portale BACnet Corporate dalla rete per accesso

Sicurezza:

- Nessun accesso diretto dall'esterno, con in progress Accesso da remoto via VPN su VLAN dedicata.

- Logging centralizzato e doppio firewall interno con archiviazione locale dei dati registrati che fanno parte del BEMS
- Nessuna cifratura dei dati → BACnet “classico” **in chiaro su diverse porte UDP** verso i diversi BBMD.

Note:

- Architettura BACnet Multivendor robusta e ben isolata (isolata), ma **non cifrata**.
- Limitata scalabilità verso architetture distribuite o Cloud.
- In progress improvement per accesso via VPN da Remoto su server Server di supervisione di un ulteriore Vendor

7.6.2 Caso Studio A-Bis – Edificio Direzionale con rete segregata e BACnet/IP+SC

Contesto:

- Edificio Alto di recente costruzione, destinato ad uffici aziendali, Single Tenant, infrastruttura ad alta densità energetica
- BEMS su Server Locale composto da controllori DDC, supervisione locale senza integrazione con rete aziendale ma con postazione dedicata per la gestione del Facility da un PC collegato sulla rete dei Server
- Livello di affollamento/occupazione quotidiano da 800-3000 persone al giorno

Architettura:

- Rete OT con diverse VLAN ma comune tutto completamente e fisicamente separata dalla rete IT aziendale del Cliente
- Introduzione segregazione per collegamento sistema BEMS edificio a portale BEMS BACnet Nativo mondiale all’interno di un Corporate Data Center T1 via BACnet/SC, con collaborazione con IT cliente nello specifico dei team Networking e Security
- Dispositivi circa +2300 controllori BACnet:
 - DDC BACnet/IP, con indirizzamento privato statico e distribuzione su diverse VLAN interne.
 - * Device Multivendor a Livello DDC (B-BC, B-ASC, B-A)
 - DDC BACnet/IP che fungono da Gateway da **altri protocolli standard** a BACnet per prodotti (Attuatori, Sensori, PdC, Chiller, VAV, Schermature, Gestione Ambienti, Gestione Carichi, Gestione Illuminazione, Automazioni dei comandi elettrici, o controllori) che supportano comunicazioni su protocolli standard come

- * MODBUS RTU
- * MODBUS TCP
- * MBUS 485
- * DALI
- * KNX
- DDC BACnet/IP che fungono da Gateway (B-BC/B-GW) da **protocolli proprietari** a BACnet per sistemi come
 - * Gestione Locali Tecnici IT e Centro Stella Tecnologico
 - * Rivelazione Incendi
 - * Gestione UPS e GE
 - * Sistemi di Spegnimento
 - * Sistemi gestione delle emergenze di Public Addressing
- Entità delle informazioni gestite, +24.000 data-point fisici, + 200.000 oggetti BACnet (data-point Virtuali), tutto in realtime
- Supervisioni Locali in Locale Telecontrollo interno per Manutenzione e/o in postazioni Dedicate all'interno dell'edificio collegate direttamente sulla rete OT anche per il cliente Finale su una VLAN in grado di vedere solamente i Server e non i controllori con regole firewall a doppio livello
- Supervisione BEMS BACnet in Cloud con portale Pubblico ma in Datacenter Mondiale segregato all'applicazione WEB BEMS BACnet Nativa
- Bridge BACnet Locale BBD e livello Enterprise Corporate via BACnet SC Un device per la connessione BACnet S/C per il centro-stella presso il Datacenter Corporate

Sicurezza:

- Nessun accesso diretto dall'esterno, con in progress Accesso da remoto via VPN su VLAN dedicata.
- Logging centralizzato e doppio firewall interno con archiviazione locale dei dati registrati che fanno parte del BEMS
- Nessuna cifratura dei dati → BACnet “classico” **in chiaro su diverse porte UDP**.

Note:

- Architettura BACnet Multivendor robusta e ben isolata, ma **non cifrata**.
- Limitata scalabilità verso architetture distribuite o Cloud.
- In progress improvement per accesso via VPN da Remoto su server Server di supervisione di un ulteriore Vendor
- BACnet/SC nel bridge di segregazione con Routing + Crittografia verso Datacenter Centrale

7.6.3 Caso Studio B – Super Condomini: BEMS distribuito e accesso remoto via VPN

Contesto:

- Infrastruttura Multi-Site articolata composta da **diversi siti** (+3) con **diversi edifici** (+4 che contengono diverse unità abitative per un totale di +1300 UI con strutture di servizi generali a parte.
- Supervisione centralizzata in Cloud Pubblico, per accesso remoto alle diverse figure coinvolte nella gestione delle diverse strutture (Facility management, Asset management, Energy Manager, Property, Administrative Management e Billing), servizi esterni offerti da terzi mediante l'uso dei dati grezzi.
- Doppio Cloud BEMS connesso ai siti uno del cliente e uno per servizi middleware intermedi per terzi utilizzatori dei dati e per servizi di manutenzione
- Livello di affollamento/occupazione 1300 famiglie e oltre 30 attività commerciali

Architettura:

- Reti Locali OT completamente e fisicamente separate dalla rete IT aziendale del Cliente.
- Segregazione OT/IT con implementazione di Firewall e segregazione unità di Routing + BACnet/SC sulla rete OT e verso la rete del cliente in un datacenter corporate privato esterno con Server Virtuali di centralizzazione Applicazione BEMS su portale WEB
- Dispositivi circa +1500 controllori BACnet:
 - DDC BACnet/IP, con indirizzamento privato statico e distribuzione su diverse VLAN interne.
 - * Device Multivendor a Livello DDC (B-BC, B-AAC, B-ASC, B-S, B-A)
 - DDC BACnet/IP che fungono da Gateway da **altri protocolli standard** a BACnet per prodotti (Attuatori, Sensori, PdC, Chiller, VAV, Schermature, Gestione Ambienti, Gestione Carichi, Gestione Illuminazione, Automazioni dei comandi elettrici, o controllori) che supportano comunicazioni su protocolli standard come
 - * MODBUS RTU
 - * MODBUS TCP
 - * MBUS 485
 - DDC BACnet/IP che fungono da Gateway (B-BC/B-GW/B-OD) da **protocolli proprietari** a BACnet per sistemi come
 - * Rivelazione Incendi

* Allarmi Safety

- Entità delle informazioni gestite, +20.000 data-point fisici, + 300.000 oggetti BACnet (data-point Virtuali), tutto in realtime
- Reti locali MS/TP e RS485 (altri protocolli standard) nei singoli edifici, collegate via gateway BACnet/IP con Router BACnet e BACnet Gateway
- Un BBMD per ogni sito
- Supervisore BACnet/IP con accesso doppia VPN su rete Privata

Sicurezza:

- VPN IPSec P2P tra single Site e Cloud
- Doppio Cloud BEMS uno del cliente e uno di backup del fornitore
- Policy di aggiornamento firmware a necessità (minimo garantito almeno semestrale su segnalazione).
- Logging eventi su server serverlog centrale,
- Nessuna cifratura dei pacchetti BACnet in rete OT → vulnerabilità intermedia.

Note:

- Buon compromesso tra accessibilità e segregazione.
- Assenza di BACnet/SC rende vulnerabili le trasmissioni esterne.

7.6.4 Caso Studio C – Insediamento Industriale Multivendor: su Private-Cloud Cliente e accesso remoto via VPN con MFA

Contesto:

- Infrastruttura Single Site articolata composta da diversi un unico insediamento industriale con diversi edifici (+5) e reparti Produttivi e/o di stoccaggio (+15) e svariate Centrali di produzione (+20) con una moltitudine di impianti sia di processo che di Controllo
- Supervisione centralizzata in Cloud Privato dentro un datacenter locale con, per accesso via web-browser dalla rete di stabilimento interna alle diverse figure coinvolte nella gestione delle diverse strutture (Manutentore con presidio in un locale di controllo all'interno dell'edificio Centrale, Responsabili di Stabilimento delle Facilities e del Processo, HMI di accesso locale al sistema da ogni singolo reparto.) Facility management, Asset management, Energy Manager, Property, Administrative Management e Billing, servizi esterni offerti da terzi mediante l'uso dei dati grezzi.

Architettura:

- Reti locali MS/TP nei singoli edifici, collegate via gateway BACnet/IP.
- Reti Locali OT integrate nella Rete IT Tecnica di Stabilimento con una VLAN dedicata al solo BMS gestita da una serie di Firewall con IT Cliente per renderla completamente e fisicamente separata dalla rete IT aziendale del Cliente
- Dispositivi circa +800 controllori BACnet:
 - DDC BACnet/IP, con indirizzamento privato statico sulla VLAN.
 - * Device Single-Vendor a Livello DDC (B-BC, B-AAC, B-ASC, B-S, B-A)
 - DDC BACnet/IP che fungono da Gateway da **altri protocolli standard** a BACnet per prodotti (Attuatori, Sensori, PdC, Chiller, VAV, Schermature, Gestione Ambienti, Gestione Carichi, Gestione Illuminazione, Automazioni dei comandi elettrici, o controllori) che supportano comunicazioni su protocolli standard come
 - * MODBUS RTU
 - * MODBUS TCP
 - DDC BACnet/IP che fungono da Gateway (B-BC/B-GW/B-OD) da **protocolli proprietari** a BACnet per sistemi come
 - * Contabilizzazioni di tutti i vettori Energetici: Elettrici, Termici, Fluidi, Gas di Processo, Analisi Fumi, Trattamento Acque
 - * Gestione Cabine di Trasformazione AT/BT con interrompibilità
 - * Connettori di interfaccia BACnet a sottosistemi proprietari
 - * PLC MultiVendor da sistema di processo e funzionamento Sottostazioni
 - * Sistemi di trasferimenti dati a terzi via BACnet webservice
- Entità delle informazioni gestite, +12000 data-point fisici, + 75.000 oggetti BACnet (datapoint Virtuali), tutto in realtime
- Supervisione BEMS in Cloud con portale Privato segregato all'applicazione WEB BEMS BACnet Nativa
- Reti locali MS/TP e RS485 (altri protocolli standard/proprietary) nei singoli edifici, collegate via gateway BACnet/IP con Router BACnet e BACnet Gateway
- Suddivisione stabilimento in due Macro aree con 2 BBMD uno di Backup all'altro
- Data lake population di oltre 2500 oggetti verso sistemi di livello enterprise del cliente con API BACnet
- Supervisore BACnet/IP con accesso VPN su rete pubblica con MFA

Sicurezza:

- VPN con autenticazione a due fattori MS.
- Policy di aggiornamento firmware semestrale o secondo necessità.
- Logging eventi su serverlog centrale.
- Gestione di certificati HTTPS per
- Doppio Server on-premise in datacenter cliente per l'applicazione BEMS BACnet e uno per l'archiviazione BACnet
- Nessuna cifratura dei pacchetti BACnet → vulnerabilità limitata.

Note:

- Buon compromesso tra accessibilità e segregazione.
- Gestione sinergica delle Reti OT con quelli IT con i Teams di Networking più quello di Security del Cliente
- Assenza di BACnet/SC rende vulnerabili le trasmissioni esterne.

7.6.5 Caso Studio D – Connessione di edificio Residenziale e Ufficio con architettura full BACnet/SC

Contesto:

- Infrastruttura di studio con un appartamento ed un ufficio di un edificio residenziale.
- Sistemi HVAC e integrazione sicurezza con supervisione BEMS in cloud esterno pubblico.

Architettura:

- Tutti i dispositivi parlano BACnet/SC.
- Hub centrale certificato installato in DMZ tra IT e OT.
- Utilizzo di certificati X.509 e TLS 1.3.

Sicurezza:

- Tutte le comunicazioni cifrate.
- Isolamento fisico OT.
- Integrazione con SIEM aziendale.

Note:

- Architettura conforme a best practice IT/OT.
- Investimento elevato per la tipologia di intervento, ma garantisce sicurezza by design.

7.7 Riepilogo - Lezioni apprese e buone pratiche

Dai casi reali, riassunti in una matrice funzionale comparativa, tabella 7.2 emergono alcune buone pratiche trasversali:

| Elemento | Caso A | Caso ABis | Caso B | Caso C | Caso D |
|--------------------------------|--------------|-----------------------|--------------------------------|--------------------------|----------------------------|
| Architettura | VLAN isolata | VLAN isolata | Reti MS/TP + IP + VPN | Reti MS/TP + IP + VPN | Full BACnet/SC |
| Accesso remoto | Interno | Interno/Esterno | VPN esterna + Accesso pubblico | VPN esterna + | Nessun accesso diretto |
| Protocollo | BACnet/IP | BACnet/IP – BACnet/SC | MS/TP + RS485 BACnet/IP | MS/TP + RS485 BACnet/IP | BACnet/SC |
| Sicurezza applicativa | Assente | Parziale | Parziale | Parziale + Audit Interni | Totale (TLS + certificati) |
| Logging e tracciabilità | Interna | Centralizzata | Centralizzata | Integrazione con SIEM | Integrazione con SIEM |
| Scalabilità | Limitata | Buona | Buona | Buona | Ottima |

Tabella 7.2. Riepilogo comparativo casi di studio

- Segregare sempre la rete OT: VLAN, firewall o DMZ.
- Adottare il principio “zero-trust”: autenticazione per ogni attore.
- Cifratura end-to-end dove possibile: BACnet/SC o VPN + TLS.
- Supervisione centralizzata e logging continuo.
- Policy di aggiornamento e gestione certificati.

Queste strategie risultano efficaci nel ridurre la superficie d’attacco, migliorare la tracciabilità e supportare l’evoluzione verso infrastrutture “*Smart*” e “*sicure*”.

L’analisi dei casi studio mostra come la progettazione dell’architettura di rete, la scelta dei protocolli e l’adozione di misure di sicurezza coerenti possano determinare il livello effettivo di resilienza e affidabilità di un sistema BEMS.

L’evoluzione tecnologica verso BACnet/SC e la convergenza IT/OT richiedono oggi competenze trasversali che integrino **Automazione**, **Networking** e **Cyber-security**.

Capitolo 8

Linee Guida e Raccomandazioni Operative

La messa in sicurezza dei sistemi BEMS non può basarsi su soluzioni improvvisate, ma deve fondarsi su principi progettuali, strumenti professionali e metodologie coerenti. L'adozione di un **approccio sistemico** alla sicurezza nei BEMS non può prescindere da una solida impostazione metodologica, che parta dalla fase di progettazione per arrivare fino alla gestione operativa e alla risposta agli incidenti. In questo capitolo vengono definite una serie di linee guida tecniche e operative, frutto dell'analisi critica svolta nei capitoli precedenti, e orientate a garantire la resilienza, integrità, disponibilità e sicurezza dei sistemi di automazione negli edifici intelligenti.

8.1 Principi per l'integrazione sicura di sistemi BEMS

Un sistema BEMS sicuro non è solo il risultato di tecnologie avanzate, ma di **principi progettuali corretti e coerenti**. Tra i principali:

(a) Security by Design

La sicurezza non deve essere un'aggiunta postuma, ma integrata sin dall'inizio nella progettazione. Ciò implica:

- *Specificazione dei requisiti di sicurezza in fase di capitolato*
- *Adozione di standard aggiornati (BACnet/SC, ISO 27001, ISO 16484)*
- *Considerazione delle superfici di attacco nella fase di disegno architettonico*

(b) Least Privilege e Zero Trust

Ogni componente (controllore, supervisore, gateway) deve disporre solo delle autorizzazioni strettamente necessarie al suo ruolo. Nessun dispositivo o utente deve essere considerato "di fiducia" per default.

(c) **Separazione dei domini funzionali**

La rete di automazione deve essere logicamente e fisicamente separata da quella IT e da altri sottosistemi (illuminazione, sicurezza, videosorveglianza), tramite VLAN o firewall interni.

(d) **Documentazione tecnica dettagliata**

Ogni modifica infrastrutturale o logica deve essere tracciata e documentata. Devono essere prodotti e aggiornati regolarmente:

- *Schemi architetturali di Rete*
- *Mappe degli oggetti BACnet*
- *Policy di accesso e gestione*

8.2 Strumenti di progettazione e configurazione dei dispositivi

L'uso di strumenti professionali è cruciale per progettare, implementare e mantenere sistemi BEMS interoperabili e sicuri. I principali ambiti di utilizzo sono:

(a) **Progettazione assistita e modellazione**

Software specifici di schematizzazione (liberi o commerciali) o tool di configurazione dei controllori (importante precisare che per la programmazione ogni Vendor/Produttore continua ad utilizzare il proprio) permettono:

- *Modellazione degli impianti e delle reti*
- *Associazione tra dispositivi fisici e oggetti logici*
- *Simulazione funzionale del comportamento*
- *Implementazione delle logiche di processo, controllo*

(b) **Strumenti di commissioning BACnet**

Strumenti come **YABE (Yet Another BACnet Explorer)**, **BACeye**, **Wireshark con dissector BACnet** permettono:

- *Scansione e discovery dei dispositivi*
- *Analisi del traffico in tempo reale*
- *Validazione della conformità ai BIBBs*

(c) **Template e standardizzazione**

L'utilizzo di modelli standardizzati per configurazioni, nomi punto, logiche di rollback e gestione allarmi riduce errori e agevola la scalabilità del sistema.

(d) **Hardening dei dispositivi**

- *Disattivare servizi inutili (es. FTP, HTTP se non cifrato)*

- *Aggiornare firmware*
- *Disabilitare accessi telnet o seriali in ambienti produttivi*
- *Eliminare il superfluo o quanto non strettamente necessario per i processi da implementare*

8.3 Gestione sicura degli aggiornamenti, dei certificati e degli accessi

La gestione del ciclo di vita dei dispositivi e della comunicazione sicura rappresenta una delle sfide più complesse nei moderni sistemi BEMS. Possiamo tristemente confermare che fino ad oggi molto poco viene messo in campo come azione proattiva per questo tipo di attività. Tuttavia le condizioni appena descritte sono destinate a cambiare anche per una volontà intrinseca legata all'evoluzione dei sistemi e degli standard e le necessità sempre più stringenti dettate dalle mutevoli esigenze degli utilizzatori di questi sistemi (utilizzatori più attenti ed esigenti).

(a) Gestione aggiornamenti

- *Stabilire una finestra temporale periodica per aggiornamenti firmware*
- *Test preliminari in ambienti staging*
- *Deploy in ambienti di produzione*
- *Procedure di rollback documentate*

(b) Gestione dei certificati digitali (per BACnet/SC)

- *Impiego di PKI (Public Key Infrastructure) interna o affidata a ente certificatore esterno*
- *Scadenza dei certificati con notifica automatica*
- *Revoca tempestiva in caso di compromissione*

(c) Accessi remoti e locali

- *Utilizzo di autenticazione multifattoriale (MFA) per l'accesso al supervisore*
- *Log degli accessi amministrativi*
- *Limitazione degli accessi locali non tracciati (USB, console seriale)*

(d) Provisioning e decommissioning sicuro

- *Automazione del processo di onboarding di nuovi dispositivi*
- *Rimozione sicura e tracciata di dispositivi obsoleti*

8.4 Logging, auditing, monitoraggio e reazione agli incidenti

L'assenza di logging è una delle cause principali del fallimento nella gestione di incidenti OT. Una buona prassi prevede:

(a) Centralizzazione dei log

- *Integrazione dei log BACnet con sistemi di Security Information and Event Management (SIEM) (es. Splunk, Graylog, ELK)*
- *Uso di syslog standard o protocollo MQTT per l'invio sicuro dei log*

(b) Auditing regolare

- *Analisi periodica degli accessi e delle modifiche alla configurazione*
- *Audit trail degli allarmi e comandi manuali*

(c) Monitoraggio in tempo reale

- *Dashboard di supervisione con notifiche proattive*
- *Analisi comportamentale dei dati per individuare deviazioni*

(d) Incident Response

- *Procedure di **contenimento e isolamento dei nodi compromessi***
- *Lista predefinita dei contatti e escalation*
- *Verifica dell'integrità del sistema dopo un attacco*

Fino a qui le raccomandazioni delineate rappresentano un riferimento concreto per la progettazione, gestione e audit di sistemi BEMS sicuri. Esse pongono le basi per un nuovo paradigma: quello di un edificio intelligente, interconnesso, ma soprattutto affidabile e resiliente.

Capitolo 9

Conclusioni e Sviluppi Futuri

Concludendo questa prima tappa nel mondo dei sistemi BEMS e delle sfide imposte dalla Cybersecurity, appare evidente come i dati non siano più soltanto numeri, ma si trasformino in informazioni tecniche diventando un vero valore economico e strategico. In un contesto in cui IT e OT si intrecciano sempre più, si aprono nuove domande e scenari da esplorare.

Questa tesi vuole offrire una base da cui partire per sviluppare ulteriori ricerche e casi applicativi, mettendo a fattor comune le potenzialità delle tecnologie emergenti e dei nuovi modi di progettare e gestire edifici sempre più intelligenti e sicuri.

9.1 Sintesi dei risultati

La messa in sicurezza dei sistemi BEMS non può basarsi su soluzioni improvvisate, ma deve fondarsi su **principi progettuali**, strumenti professionali e metodologie coerenti. Questo lavoro fornisce indicazioni pratiche e raccomandazioni per l'integrazione sicura di sistemi BACnet, con focus su configurazione, aggiornamenti, accessi e risposta agli incidenti.

Questa tesi ha analizzato in modo esteso e tecnico il tema **dell'interoperabilità e della sicurezza informatica** nei Building Energy Management Systems (BEMS), con particolare attenzione all'evoluzione dei protocolli BACnet e all'introduzione di BACnet Secure Connect (SC).

I principali risultati e contributi emersi sono:

- Una panoramica solida dello **stato dell'arte** nei sistemi BEMS, nelle architetture IT/OT e nei protocolli di comunicazione industriale.
- Un confronto tecnico tra **BACnet classico** e **BACnet/SC**, mettendo in evidenza vantaggi, limiti e implicazioni sulla sicurezza.
- L'analisi approfondita delle **vulnerabilità tipiche** nei sistemi BEMS e delle principali contromisure (segregazione, VPN, autenticazione, cifratura).
- L'identificazione di **casi studio reali** e l'estrapolazione di buone pratiche applicabili in contesti professionali.

- La proposta di una **metodologia di validazione** strutturata, pensata per supportare audit tecnici e transizioni verso modelli più sicuri.

Questi contenuti hanno permesso di **collegare concettualmente e operativamente** le esigenze di comfort, efficienza e sostenibilità con le necessarie garanzie di integrità, disponibilità e protezione del dato, oggi imprescindibili in qualunque infrastruttura “smart”.

Le ipotesi formulate nel Capitolo 1 sono confermate:

- La crescente apertura delle reti BEMS richiede un nuovo paradigma di protezione.
- L’interoperabilità può essere mantenuta solo con standard aperti e una semantica condivisa.
- La sicurezza deve essere integrata a livello di protocollo, non solo perimetrale.

9.2 Riflessioni conclusive

L’integrazione sempre più spinta tra reti IT e ambienti OT ha trasformato profondamente la natura dei BEMS, che oggi non possono più essere considerati meri strumenti di supervisione tecnica, ma veri e propri **nodi digitali attivi** nella rete informativa dell’edificio.

BACnet/SC rappresenta un passo decisivo verso un modello di **sicurezza applicativa integrata**, con un approccio “zero-trust” più vicino alle logiche dei moderni sistemi informativi aziendali. Tuttavia, la sola adozione di nuove tecnologie non basta: è fondamentale **governare la complessità** con processi di analisi, validazione e aggiornamento continui.

In questo contesto, **l’ingegnere dell’automazione e il professionista IT devono convergere e collaborare** adottando linguaggi e strumenti comuni, per assicurare il corretto equilibrio tra operatività e protezione.

9.3 Limiti del lavoro

Come in ogni attività di ricerca e analisi tecnica, alcuni limiti sono da evidenziare:

- L’approccio proposto si basa su un’analisi qualitativa e semi-quantitativa; una **validazione estesa su larga scala** richiederebbe accesso a dataset più ampi e a reti operative complesse.
- Le **simulazioni di test** e attacchi controllati sono descritte a livello metodologico, ma non condotte su impianti reali, per motivi di sicurezza e riservatezza.
- Alcuni aspetti emergenti, come l’integrazione di **intelligenza artificiale** nei BEMS o l’adozione di **architetture cloud-native**, sono stati volutamente esclusi per mantenere il focus sui temi centrali.

9.4 Sviluppi futuri

Il lavoro svolto apre a numerose possibilità di **approfondimento accademico e applicativo**, tra cui:

- **Sviluppo di strumenti software** per automatizzare la validazione della sicurezza nei BEMS (es. tool di analisi di rete, generatori di report, motori di scoring).
- **Applicazione sul campo** della metodologia in contesti reali, anche in ambienti critici (ospedali, data center, infrastrutture pubbliche).
- **Estensione della metodologia alla componente cloud** dei BEMS moderni, con focus su API, edge computing e architetture ibride.
- **Integrazione di sistemi SIEM o SOC/NOC (Security Operation Center)** per la supervisione in tempo reale dei BEMS da parte di team IT centrali.
- **Valutazione dell'impatto normativo** di nuove direttive europee sulla sicurezza informatica (es. NIS2) sui sistemi di automazione edilizia.

Questi sviluppi potrebbero alimentare progetti di tesi successive, attività di R&D in ambito Aziendale o Industriale, o percorsi di innovazione all'interno di enti pubblici o privati che gestiscono edifici o aggregati di questi più o meno complessi distribuiti sul territorio.

La crescente digitalizzazione dell'ambiente costruito richiede un cambio di paradigma nella progettazione, gestione e validazione dei sistemi BEMS. Questa tesi ha cercato di offrire strumenti concettuali e pratici per affrontare tale sfida con competenza tecnica e visione interdisciplinare, unendo le esigenze di efficienza energetica, interoperabilità dei sistemi e cybersecurity.

Tutto lo studio ed il lavoro svolto confermano che non si può prescindere da un parallelo adeguamento culturale di tutte le figure coinvolte nei processi. Questo risultato può essere raggiunto solo se accompagnato da un importante e continuo processo di formazione e sensibilizzazione globale nella filiera.

Bibliografia

- [1] ASHRAE, “Ansi/ashrae standard 135-2020 – bacnet: A data communication protocol for building automation and control networks,” 2020.
- [2] ISO, “Iso 16484-5:2017, building automation and control systems (bacs) – part 5: Data communication protocol,” 2017.
- [3] ISO/IEC, “Iso/iec 20922:2016, information technology – message queuing telemetry transport (mqtt) v3.1.1,” 2016.
- [4] IEC, “Iec 62541-1 to 62541-13, opc unified architecture (opc ua) – specifications,” 2021.
- [5] K. Association, “Knx secure – technical application note,” KNX.org, Tech. Rep., 2021. [Online]. Available: <https://www.knx.org>
- [6] M. Organization, “Modbus messaging on tcp/ip implementation guide v1.0b,” 2006. [Online]. Available: <https://modbus.org>
- [7] B. International, “Bacnet secure connect – an overview, white paper,” BACnet International, Tech. Rep., 2021. [Online]. Available: <https://www.bacnetinternational.org>
- [8] F. Jammes and H. Smit, “Service-oriented paradigms in industrial automation,” *IEEE Transactions on Industrial Informatics*, vol. 1, no. 1, pp. 62–70, Feb 2005.
- [9] H. Boyes, B. Hallaq, J. Cunningham, and T. Watson, “The industrial internet of things (iiot): An analysis framework,” *Computers in Industry*, vol. 101, pp. 1–12, 2018.
- [10] M. Cheminod, L. Durante, and A. Valenzano, “Review of security issues in industrial networks,” *IEEE Transactions on Industrial Informatics*, vol. 9, no. 1, pp. 277–293, 2013.
- [11] N. I. of Standards and Technology, “Nist sp 800-82 rev. 2, guide to industrial control systems (ics) security,” NIST, Tech. Rep., 2015.
- [12] ENISA, “Good practices for security of smart buildings,” European Union Agency for Cybersecurity (ENISA), Tech. Rep., 2020. [Online]. Available: <https://www.enisa.europa.eu>
- [13] L. Ristori and D. D. Pietro, *Cybersecurity per l’automazione industriale*. Milano: FrancoAngeli, 2022.
- [14] S. Parise and A. Avitabile, *Building Management Systems: Digitalizzazione, interoperabilità e sicurezza*. Roma: EPC Editore, 2021.
- [15] D. Controls, “Delta controls bacnet/sc security guide,” Delta Intelligent Building Technologies Inc., Tech. Rep., 2019–2025.
- [16] —, “Delta controls enteliweb guide,” Delta Intelligent Building Technologies Inc., Tech. Rep., 2019–2025.

- [17] —, “Delta controls red5 family for bacnet/sc,” Delta Intelligent Building Technologies Inc., Tech. Rep., 2019–2025.
- [18] —, “Delta controls cybersecurity bulletin,” Delta Intelligent Building Technologies Inc., Tech. Rep., 2022–2025.
- [19] WG-FM, “Bacnet from global point of view, opc ua information model for bacnet, wg-fm guideline “cyber security in building automation”,” BIG-EU, Tech. Rep., 2020. [Online]. Available: <https://www.big-eu.org>
- [20] A. Catalano, “Sistemi di automazione edificio intelligenti: uno strumento per la riduzione dei fabbisogni,” in *AICARR - 48° Convegno Internazionale – Baveno*, relazione ad invito.
- [21] —, “Il ruolo del sistema di automazione: l’importante legame dato-protocollo-processo,” in *AICARR – 30° Convegno Nazionale Bologna*, relazione ad invito.
- [22] —, “Bacnet: la potenza di un protocollo aperto orientato agli oggetti,” in *AICARR – 20° Convegno Internazionale Milano*, relazione ad invito.
- [23] —, “Interoperabilità & smart building: Bacnet, come risposta alle necessità di ridurre i fabbisogni,” in *OIT & Politecnico di Torino – Convegno sulla Gestione dell’Opera Pubblica*, 2015, relazione ad invito.
- [24] ASHRAE, *Managed BACnet Guidance*. ASHRAE, 2025. [Online]. Available: <https://www.ashrae.org/file%20library/technical%20resources/bookstore/managedbacnet.pdf>