

Sicurezza e Interoperabilità nei BEMS: Valutazione del Rischio e Scenari di Protezione tra VPN, Segregazione e BACnetSC

Security Assessment di architetture reali in ambienti convergenti IT/OT

Candidato: Antonio Catalano

Relatore: Prof. Fulvio Valenza, Prof.ssa Maria Ferrara

1 Introduzione e Motivazioni

Nel contesto della crescente digitalizzazione e degli edifici intelligenti, i sistemi BEMS (Building Energy Management Systems) rappresentano l'infrastruttura strategica per il controllo, il monitoraggio e l'ottimizzazione dei principali sistemi orizzontali/verticali, ad esempio impianti tecnologici: HVAC, illuminazione, energia, sicurezza e accessi. L'interoperabilità tra dispositivi di diversi Vendor (più generalisti o specifici) nelle diverse applicazioni è oggi un requisito essenziale per garantire comfort ambientale, efficienza operativa, safety in tempo reale e sostenibilità energetica.

In questo scenario, BACnet (ISO 16484-5) si è affermato come standard di riferimento per i sistemi BEMS grazie alla sua concezione di Architettura Aperta, orientata agli Oggetti, e alla capacità di integrare dispositivi di produttori diversi su reti Ethernet con o senza protocollo IP e bus di comunicazione in modo naturale; il tutto è stato anche favorito da una convergenza sempre maggiore tra il mondo dei Sistemi per Edifici (Intelligent Building) e quello trainante delle Reti Informatiche (IT/ITC) con la distribuzione delle informazioni anche al livello geografico. Tuttavia, l'apertura dei sistemi BEMS verso reti IT e ambienti connessi se pur distribuiti, ha introdotto nuove aree di attacco, vulnerabilità degli impianti (anche strategici) e ha reso la sicurezza informatica un elemento imprescindibile nella progettazione delle architetture.

Originariamente e storicamente, la protezione, quando presente, veniva attuata solo attraverso soluzioni infrastrutturali come la segregazione delle reti OT tramite VLAN o DMZ, con l'utilizzo di firewall industriali e l'adozione di VPN per le connessioni remote, che rimangono del tutto attuali. L'evoluzione tecnologica e la stringente necessità ravvisata da tutti gli operatori dei Sistemi tecnologici nonché le associazioni che si coordinano con lo sviluppo dello standard AHRAE SSPC-135 ha portato oggi a BACnet Secure Connect (SC), dove la sicurezza è stata portata a livello applicativo attraverso crittografia TLS, mutua autenticazione e gestione dei certificati digitali, abilitando una comunicazione più sicura nativamente ed integrata nel protocollo.

Questa tesi si è proposta di analizzare le opportunità e i rischi dell'interoperabilità nei sistemi BEMS, con parti-

colare attenzione al ruolo di BACnet e alla sua evoluzione verso BACnetSC.

Il lavoro si è svolto seguendo un approccio comparativo e integrato, attraverso l'analisi di diversi casi reali con architetture di rete eterogenee, confrontando soluzioni tradizionali e moderne in termini di sicurezza, scalabilità e resilienza. L'obiettivo è stato quello di:

1. valutare modelli di riferimento per l'implementazione di sistemi BEMS efficienti, interoperabili, sicuri e orientati alla continuità operativa degli edifici intelligenti;
2. creare un processo di validazione delle architetture dei sistemi BEMS di utilità nella fase progettuale o anche in itinere durante il commissioning

uno degli scopi di questa attività di ricerca è avviare un processo di verifica del livello di sicurezza dei sistemi stessi, con focus sulla valutazione del rischio e sul miglioramento progressivo ai fini di una migliore compliance con le politiche interne di Cybersecurity degli utilizzatori di questi sistemi, che funga da apripista per ulteriori sviluppi di metodologie di verifica.

2 Contributi della tesi

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 BACnetSC affrontando temi storici legati allo scambio, gestione e distribuzione di dati con la loro valorizzazione e problematiche attuali della loro trattazione in modo più "sicuro".

L'ambizione della tesi è stata duplice: da un lato, esaminare criticamente le soluzioni tecnologiche esistenti, le loro potenzialità e i loro limiti e dall'altro, proporre un metodo di validazione tecnica, utile a progettisti, integratori e gestori per selezionare e implementare architetture BEMS più robuste e sicure. Nello sviluppo viene adottato un approccio guidato a ipotesi di lavoro e quesiti di ricerca nello sviluppo di soluzioni BEMS più sicure in un contesto globale connesso dove la Cybersecurity sta assumendo un ruolo fondamentale ed imprescindibile nelle azioni di pre-

venzione e contenimento di attacchi informatici derivanti da diversi vettori di minaccia.

2.1 Struttura BACnetSC

Il primo input è l'evoluzione di BACnet verso una maggiore sicurezza e compatibilità IT ha portato allo sviluppo di BACnet Secure Connect (SC). Con la sua introduzione, approvato nel 2019 Annex bj del 135-2016 come estensione ufficiale dello standard, si è colmata la mancanza di sicurezza strutturale nel protocollo; questo consente l'abbandono del broadcast e del protocollo UDP, a favore della cifratura TLS 1.3, rendendolo compatibile con le infrastrutture IT moderne. BACnetSC utilizza una topologia hub-and-spoke, con relay centralizzati che redistribuiscono il traffico BACnet e introduce livelli aggiuntivi utilizzando TLS 1.3 e TCP, permettendo una comunicazione sicura e conforme alle moderne architetture IT, pertanto presenta una topologia incentrata su IP, dove:

- Tutto il BACnet è un "Application", incluso il BACnetSC BACnet Datalink
- HTTP HTTPS 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 supporti IPv4 o IPv6: Ethernet, WLAN, 4G/5G, ... ,

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

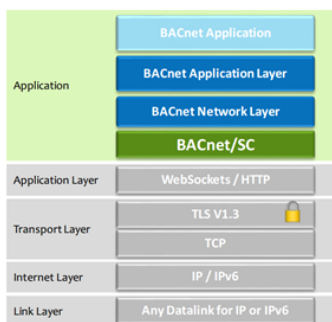


Figure 1: BACnetSC nel modello ISO/OSI

La topologia impiegata da BACnetSC 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 diretto ad un altro Nodo o deve essere invece inoltrato a tutti i Nodi collegati. 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) che si instrada verso un sistema BACnet esistente oppure direttamente 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 BACnetSC supportano un meccanismo di Failover per garantire che il sistema

rimanga operativo in caso di guasto o manutenzione preventiva. Tutti i nodi BACnetSC sono tenuti a supportare la connessione all'Hub di Failover, se l'Hub Primario non è raggiungibile/operativo; inoltre tra le possibilità i Nodi possono anche eseguire delle connessioni dirette ad altri Nodi oltre a quella verso l'Hub.

2.2 Architetture Sicure BACnetSC

Il secondo input sono le molteplici soluzioni di architetture che si possono implementare grazie a BACnetSC, ovvero una infrastruttura di sicurezza di nuova generazione nel contesto dei BEMS



Figure 2: Canale Nodo-HUB

Tra Nodo e Hub vi è una comunicazione criptata mentre nel resto della rete no questo per indicare che il traffico BACnet viaggia all'interno di un canale sicuro per cui è possibile sicurizzare tutta o solo una porzione di rete dei device in base alle necessità e topologie dei diversi sistemi da interconnettere.

Nel lavoro sono richiamate quattro differenti topologie di collegamento BACnetSC e successivamente raffrontate tra di loro rispetto all'affine ma diverso approccio precedente di BACnet (via BBMD) per portarsi successivamente alle diverse valutazioni negli scenari di validazione.

2.3 Valutazione dei rischi e criticità nei sistemi

Una parte consistente del lavoro di tesi si è concentrata sulla definizione del processo di validazione per la definizione di linee guida per l'analisi e il confronto di diversi progetti BACnet, evidenziandone i punti di forza e debolezza rispetto allo standard.

Da queste analisi si sono ipotizzate un insieme di regole di mitigazione dei rischi Cyber per decidere se e come operare nell'implementazione delle diverse architetture BEMS, applicando modelli di architetture BACnet compliant (BACnet Ethernet, BACnet UDP, BACnetSC e miste).

L'attività è stata anche supportata da una serie di analisi legate ai diversi rischi e alle criticità di sistemi reali di BEMS interconnessi; si sono analizzati in modalità teorica i principali vettori di attacco, le debolezze architetture più comuni, le pratiche consolidate per la mitigazione e i criteri professionali per la validazione della sicurezza dei sistemi.

Sono stati definiti criteri tecnici oggettivi più o meno efficaci nelle fasi di validazione, da cui è emersa una sintesi dei principali ambiti da verificare anche nel contesto della validazione.

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 BACnetSC 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

Table 1: Tabella criteri di valutazione rischi e validazione

Questi criteri vengono suggeriti per essere formalizzati in check-list e audit periodici per garantire conformità normativa (es. ISO 27001, IEC 62443) o semplicemente buone pratiche operative anche in fase di validazione.

3 Implementazione e Validazione

L'adozione di standard di comunicazione sicuri come BACnetSC 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 questa tesi è stato ipotizzato anche un possibile processo di validazione tecnico-procedurale, da applicare a sistemi BEMS in esercizio o in fase di progettazione, con focus su interoperabilità, sicurezza e compliance normativa. In aggiunta alla semplice verifica della presenza di tecnologie aggiornate o protocolli sicuri, viene valutato 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 del Sistema in questione con elementi che si riferiscono a: Obiettivo, Struttura Metodologica, Griglia di Validazione con Ranking e Audit Compliance.

4 Conclusioni e Sviluppi Futuri

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. BACnetSC 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.

Il lavoro svolto apre a numerose possibilità di approfondimento accademico e applicativo, di interesse strategico per l'ente IT, il Facility Manager e l'End-User o Property Manager 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 non 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.