

"MONITORAGGIO ENERGETICO ED AMBIENTALE"

STUDIO DI FATTIBILITA' PIATTAFORMA METERING

Infrastruttura fisica e di rete [FIELD LAYER]

Codice rapporto:

C1_Infrastruttura-Fisica-Rete_FIELD-LAYER_COTRAL_0

Prepared by:

Federico Grione

Nella tabella che segue sono indicate le revisioni del documento.

Documento: **C1_Infrastruttura-Fisica-Rete_FIELD-LAYER_COTRAL_0**

Date	Version	Provided	Review	Approved	Main Changes
19/07/2022	01	FG	FG	FG	Prima emissione
29/09/2022	02	FG			Revisione

Indice

Indice	3
Introduzione	5
Strumentazione tipicamente utilizzata nei diversi spazi	5
Tecnologie per la realizzazione dell'infrastruttura fisica e di rete.....	6
Introduzione	6
Cablati	7
Ethernet	7
Power Line Networking.....	8
RS-232, RS-422 RS-485.....	9
KNX Bus System	10
Wireless a corto raggio	13
Zigbee	13
Z-Wave.....	15
Wi-Fi.....	16
Wireless a lungo raggio.....	17
LoRa WAN	17
APPARATI DI UNA INFRASTRUTTURA FISICA	21
Network Hub.....	21
Network switches	21
Network router	21
Network gateway.....	22
Network signal converter.....	22
Network firewall	23
Requisiti ambientali dei sensori	23
IoT Gateway	24
Sintesi dell'infrastruttura di rete AS-IS.....	25
Sede aziendale corporate	25
Sedi secondarie	25
Strutture rilevanti di interconnessione tra le sedi.....	25
Reti Wi-Fi	26
Video Sorveglianza	26
Telefonia VoIP	26

Sicurezza perimetrale	26
Esempi di infrastruttura fisica	27
Sede aziendale corporate	27
Tipologia di spazi	27
Infrastruttura fisica e configurazione	28
Officine	28
Tipologia di spazi	28
Infrastruttura fisica e configurazione	29
Uffici presso impianti e uffici esercizio	30
Tipologia di spazi	30
Infrastruttura fisica e configurazione	30
Depuratori	31
Tipologia di spazi	31
Infrastruttura fisica e configurazione	31
Archi di lavaggio	33
Tipologia di spazi	33
Infrastruttura fisica e configurazione	33
Piazzali di sosta	34
Tipologia di spazi	34
Infrastruttura fisica e configurazione	34
Flowchart per la selezione dell'infrastruttura fisica	35
Protocolli di comunicazione impiegati	36
MQTT	36
AMQP	37
OpcUA	38
Modbus	39
LonWorks	40
BacNET	41
Profibus e ProfiNET	43

Introduzione

Il progetto avrà bisogno di differenti approcci a seconda degli spazi e necessità, in base alla documentazione ricevuta possiamo inquadrare le seguenti categorie di spazi:

1. Uffici Esercizio, spazi che comprendono i seguenti ambienti:
 - a. Uffici
 - b. Sale per autisti
 - c. Sale ricreative
 - d. Servizi igienici
2. Uffici manutenzione
3. Officine
4. Impianto di depurazione acque
5. Sede aziendale

Ogni spazio essendo diverso presenta differenti sfide che necessiteranno la scelta della tecnologia più adatta e appropriata al monitoraggio delle risorse che vengono utilizzate.

Strumentazione tipicamente utilizzata nei diversi spazi

Qui di seguito è riportato un elenco dei principali strumenti e impianti per ogni spazio:

1. Generale:
 - a. Impianto fotovoltaico
 - b. Impianto condizionamento
 - c. Impianto di illuminazione
2. Uffici:
 - a. Laptop/PC
 - b. Stampanti, scanner, plotter
 - c. Armadi rack
3. Officine:
 - a. Ponti sollevatori a colonna da 8500Kg
 - b. Compressore aria rotativo
 - c. Pressa elettro-idraulica
 - d. Vasche di lavaggio a ultrasuoni
 - e. Quadri di distribuzione elettrica
 - f. Archi di lavaggio
4. Impianto di depurazione:
 - a. Depuratori acqua centralizzati
 - b. Depuratori acqua piovana e acqua di piazzale
 - c. Depuratore acque biologiche
 - d. Depuratore acqua archi di lavaggio
 - e. Pozzi estrazione acqua

Tecnologie per la realizzazione dell'infrastruttura fisica e di rete

Introduzione

Le tecnologie necessarie alla realizzazione dell'infrastruttura per la raccolta dati possono essere classificate in due macrocategorie:

- Cablate
- Wireless

A loro volta la categoria Wireless può essere suddivisa in:

- A lungo raggio
- A corto raggio

In base a questa macro-suddivisione possiamo individuare le seguenti tecnologie applicabili, iniziando dalla categoria cablata troviamo:

- Ethernet
- Power Line Networking
- RS-232 e RS485
- KNX Bus System
- M-Bus

Per la categoria wireless a corto raggio troviamo invece:

- Zigbee
- Z-Wave
- Wi-Fi

Infine, per le tecnologie wireless a lungo raggio abbiamo:

- LoRa WAN
- NB-IoT
- Sigfox

Qui di seguito viene riportato una breve descrizione tecnica per ogni tecnologia elencata.

Cablata

Ethernet

La tecnologia Ethernet è una tra le più diffuse ed utilizzate nell'ambito della trasmissione dati. Questa tecnologia è normata IEEE 802.3 ed opera ai primi 2 livelli del modello OSI, ovvero a livello fisico e di data link.

Un tipico impianto che utilizza la trasmissione di dati tramite Ethernet ha bisogno di effettuare diversi cablaggi in quanto la tecnologia utilizza 4 coppie di cavi twisted pair. I cavi utilizzati si dividono in categorie (CAT) con una numerazione che va da 1 fino ad 8 che corrisponde all'ultimo standard attuale.

A ciascuna categoria corrisponde una diversa capacità di trasmissione dati, per applicazioni moderne tipicamente si impiegano cavi di CAT 6, la cui capacità di trasmissione è pari 1 Gbps, la capacità di trasmissione in questo caso dipende dai dispositivi collegati alla rete stessa e alle loro caratteristiche.

Oltre a questa tipologia di cavo, la tecnologia può anche essere utilizzata con altri mezzi di trasmissione quali fibra ottica.

Su tecnologia Ethernet trova poi applicazione una miriade di protocolli di comunicazione e controllo i cui esempi più interessanti per il progetto sono:

- Modbus
- OpcUA
- EtherNET/IP
- BACNet
- LonWorks

Tutti questi protocolli di comunicazione sfruttano infatti la tecnologia ethernet come mezzo di trasmissione dati principale.

La massima distanza di trasmissione per un cavo CAT 6 è 100 m per trasmissione dati a 1Gbps, se invece si utilizza la stessa tipologia di cavo per trasmettere a 10Gbps la distanza massima viene ridotta a 55 m.

La tecnologia ethernet che utilizza cavi "Categoria-N" può beneficiare di ulteriori benefici quali ad esempio la possibilità di alimentare i dispositivi utilizzando la tecnologia Power Over Ethernet (PoE). Questa tecnologia riesce infatti a portare 48V DC ai vari dispositivi permettendo di alimentarli, naturalmente il dispositivo deve essere in grado di supportare tale tecnologia. L'utilizzo del PoE permette di ridurre la quantità di cavi da stendere in quanto elimina la necessità di dover portare cavi di alimentazione vicino ai dispositivi, nel caso inoltre i dispositivi che gestiscono la rete ethernet non siano in grado di fornire alimentazione PoE questa mancanza può essere sopperita da appositi dispositivi che "iniettano" il voltaggio 48V nella linea (PoE Injector) e permettendo l'integrazione di tale tecnologia in reti già esistenti.

Per quanto riguarda la trasmissione con fibra ottica va innanzitutto distinto il tipo di fibra ottica utilizzato, esistono infatti due tipi principali di fibre ottiche: mono-modale e multimodale.

La fibra mono-modale presenta infatti meno attenuazione rispetto alla controparte, permettendo così la trasmissione fino a 5km di distanza senza l'ausilio di ripetitori, la fibra multimodale invece presentando più attenuazione può trasmettere fino a 550m poi necessita di apparati di ripetizione. In termini di costo la fibra ottica multimodale è molto più economica rispetto alla mono-modale.

Riassumendo qui di seguito l'elenco dei vantaggi e svantaggi della tecnologia ethernet:

1. Vantaggi:
 - a. È la tecnologia che presenta la più vasta adozione da parte dei dispositivi
 - b. La velocità di trasmissione dati è la più alta in assoluto ed anche la più affidabile
 - c. Rapidità di messa in opera della rete
 - d. Topologia della rete estremamente flessibile
 - e. Manutenzione molto semplificata della rete
 - f. Tramite la tecnologia PoE riduce il numero di cablaggi e trasmette alimentazione ai dispositivi
 - g. Supporta la maggior parte dei protocolli esistenti
2. Svantaggi:
 - a. Necessità di maggiore forza-lavoro per le operazioni di messa in opera dell'impianto
 - b. Poca flessibilità se si ha necessità di aggiungere/togliere dispositivi in quanto bisogna stendere nuovi cavi (generalmente 1 per ogni dispositivo)
 - c. Richiede apparati di rete specifici (hub, switch, router, gateway, firewall...) per gestire il sistema

Power Line Networking

Il Power Line Networking (PLN) è una soluzione per trasmissione dati che sfrutta la rete elettrica di alimentazione di un edificio per trasmettere dati. Questa soluzione trova applicazione in ambienti dove non è possibile far arrivare altri tipi di tecnologie di comunicazione (come, ad esempio, il WiFi o l'Ethernet). È una tecnologia di “bridging” ed è un aiuto per portare capacità di trasmissione dati dove non si riesce diversamente.

Questa tecnologia trasmette i dati utilizzando i cavi neutro e linea dell'impianto elettrico esistente. La velocità di trasmissione dati è di circa 200Mbps; il segnale trasmesso da tali dispositivi inoltre può subire interferenze dagli altri dispositivi elettronici collegati alle prese di corrente.

Riassumendo la tecnologia PLN:

1. Vantaggi:
 - a. Sfrutta la rete elettrica esistente per trasmettere dati
 - b. Installazione facile
 - c. Ideale per portare trasmissione dati in ambienti dove non è possibile intervenire altrimenti
2. Svantaggi:
 - a. Velocità di trasmissione dati limitata se comparata con ethernet e Wi-Fi le sue tecnologie “sorelle”
 - b. Tecnologia soggetta a interferenze da parte degli altri dispositivi collegati alla rete elettrica
 - c. La trasmissione avviene da punto a punto non permettendo operazioni avanzate quali ad esempio il routing del segnale

RS-232, RS-422 RS-485

Questa famiglia di tecnologie è stata sviluppata con l'intento di favorire lo scambio di informazioni tra due dispositivi in maniera estremamente semplice, fanno parte di standard industriali e di comunicazione consolidatisi nel tempo.

Il tipo di comunicazione avviene in maniera seriale e a seconda dello standard adottato può essere half duplex ovvero è consentita la trasmissione soltanto in una direzione alla volta oppure full duplex cioè la trasmissione dati può avvenire in contemporanea in entrambe le direzioni, in particolare:

RS-232 e RS-422 sono full duplex mentre RS-485 è half duplex.

Questa tecnologia utilizza una semplice logica TTL per trasmettere i dati in cui +3 V equivale al segnale 1, diversamente è 0. I dispositivi in questa tecnologia si differenziano in:

- Dispositivo di trasmissione (Data Transmission Equipment – DTE)
- Dispositivo di comunicazione (Data Communication Equipment – DCE)

Questi standard per poter comunicare utilizzano diversi tipi di cablaggio, in particolare:

1. RS-232 per funzionare ha bisogno di almeno 3 cavi RX, TX, GND (=Ground)
2. RS-422 e RS-485 utilizzano due doppie di cavi per trasmissione e ricezione: RX+, RX-, TX+, TX- e GND

La distanza massima di trasmissione di questa tecnologia è di circa 1Km, tuttavia, bisogna tenere presente che maggiore è la distanza più si dovrà ridurre il baud rate della trasmissione e quindi la quantità di dati che si può trasmettere.

Il principale vantaggio di queste famiglie di tecnologie è la semplicità con cui si può comunicare: tuttavia per poter essere integrati nel nuovo paradigma IoT questi segnali necessitano di gateway che convertano il tipo di segnale in altri formati/protocolli mantenendo le informazioni originali.

Riassumendo RS-232, RS-422, RS-485:

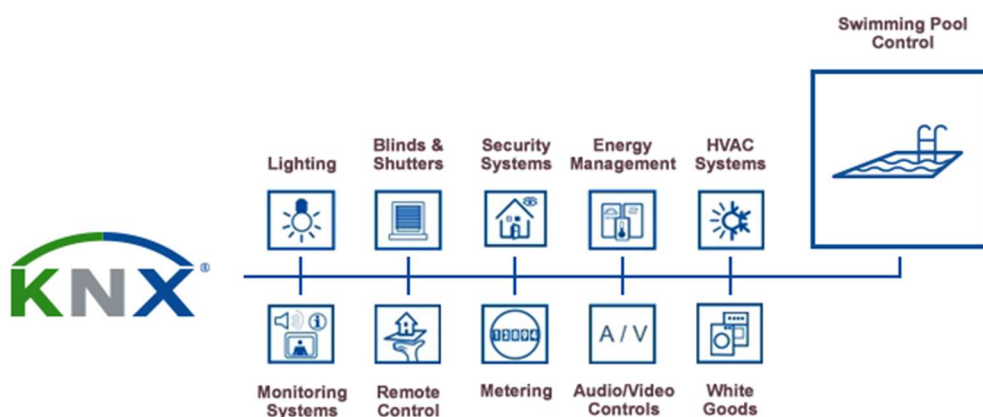
1. Vantaggi:
 - a. Semplicità di comunicazione
 - b. Comunicazione robusta e garantita punto a punto
 - c. Vasto utilizzo in sensori e macchinari industriali
 - d. Comunicazione immune da interferenze esterne
 - e. Costo estremamente basso
 - f. Vasto parco di convertitori e dispositivi per trattare segnali di questa famiglia
2. Svantaggi:
 - a. Comunicazione punto-punto senza possibilità di effettuare operazioni complesse quali il routing
 - b. Data rate basso (massimo 119200 bit/sec)

KNX Bus System

KNX è uno standard open utilizzato in ambito di building automation con svariate capacità di monitoraggio e controllo.

Un Sistema KNX è composto da quattro elementi principali:

1. Un bus KNX
2. Dei sensori: possono essere qualsiasi dispositivo, da pulsanti a termostati, a sensori CO2/temperatura ecc.
3. Degli attuatori: convertono i segnali ricevuti dai sensori in azioni; ad esempio il pulsante della luce viene premuto, l'attuatore aziona un relè per accendere la luce vera e propria
4. Un controller: si occupa della logica e automazione dell'impianto, accessibile via REST API da terze parti



Il bus KNX è il centro nevralgico del sistema, si occupa della distribuzione dei segnali provenienti dai vari sensori e attuatori. Il bus è composto essenzialmente da un cavo a doppino intrecciato (twisted pair cable) che lavora a 24V, i dati sono trasmessi in maniera asincrona bidirezionale half-duplex con una velocità di trasmissione di 9600 bit/sec fino a un massimo di 4066 dispositivi possono essere collegati a un bus.

Alcuni sensori possono utilizzare la radiofrequenza 868.3MHz per comunicare tuttavia questa tecnologia in ambito KNX non è molto utilizzata.

KNX integra inoltre la possibilità di accedere al sistema utilizzando la classica cablatura ethernet e/o Wi-Fi: questa feature consente di poter comunicare e inviare dati dal sistema KNX a qualsiasi altro endpoint o necessità.

The diagram illustrates the KNX IoT System Model, showing the integration of external systems with the KNX IoT infrastructure.

System Components and Interactions:

- 3rd Party Client:** Interacts with the **3rd Party API** via a **JSON REST API**.
- 3rd Party API (Gateway):** Acts as a bridge, receiving data from the 3rd Party Client and interacting with the **KNX IoT Point API** and **KNX Classic** devices.
- Semantic Project Export (File):** Provides **Gateway Configuration (device profile in ETS)** to the **3rd Party API**.
- ETS (Tool):** Provides **Device Configuration** to the **KNX IoT Point API** and the **KNX IoT Point API** device.
- KNX IoT Point API (Device/Broker):** Manages communication between the **3rd Party API**, **KNX Classic** devices, and the **KNX IoT Point API** devices.
- KNX IoT Point API (Device):** Facilitates **Sensor/Actuator Group & Pub/Sub Communication** between the **KNX IoT Point API** and the **KNX IoT Point API** devices.

Legend:

- out-of-scope of KNX IoT

- a. Alta integrazione e flessibilità tra sensori e ambiente, con possibilità di prendere azioni direttamente sul posto per ottenere i risultati desiderati (esempio: il sensore CO2 rileva una quantità elevata di CO2 o oltre una certa soglia il sistema KNX automaticamente apre la finestra o attiva HVAC per ridurre il livello di CO2)
- b. Soluzione “future proof”, una volta che il sistema è in piedi può essere espanso a seconda delle esigenze con sensori/attuatori a seconda delle esigenze
- c. Larga adozione in scala industriale di questo tipo di sistema con i maggiori produttori che hanno molte serie di prodotti a seconda delle esigenze
- d. Possibilità di iniziare a ridurre i costi dell’edificio da subito
- e. Standard di tipo open
- f. Crittografia e sicurezza integrata nel sistema
- g. L’integrazione e l’interoperabilità dei dispositivi è garantita dal protocollo stesso

- a. Il cablaggio da effettuare è molto importante
- b. Integrazione con sistemi esistenti difficile, se non addirittura impossibile a volte a causa del cablaggio
- c. L'integrazione con sistemi non KNX richiede hardware aggiuntivo (esempio: convertitore da modbus a KNX oppure da MQTT a KNX)
- d. Barriera economica di ingresso elevata

M-Bus

La tecnologia M-Bus (Meter Bus) può essere applicata per monitorare e controllare dispositivi fino a 5 km di distanza.

M-Bus utilizza un paradigma Master/Slave, in cui il dispositivo master è responsabile della sincronizzazione del sistema la cui topologia può essere di tipo stella, linea o bus.

M-Bus utilizza normalmente cavo telefonico twisted pair (per la precisione J-Y(ST)Y 2 x 2 x 0.8 mm) per la creazione della rete, il data rate è piuttosto basso, il massimo è infatti 38.400bps, tuttavia, per installazioni che necessitano di lunghe distanze esso deve essere abbassato a 300 bps.

M-Bus supporta fino a 250 dispositivi per network.

Una versione wireless del protocollo M-Bus utilizza la trasmissione in radiofrequenza tramite banda a 169MHz e la trasmissione può essere ricevuta fino a 3.5Km in aree urbane.

Per riassumere la tecnologia M-Bus:

1. Vantaggi:

- a. Standard utilizzato principalmente in ambito sensoristico
- b. Installazione relativamente facile se la costruzione è nuova
- c. Lettura dati in tempo reale
- d. Possibilità di lettura dati e messa in opera in modalità wireless

2. Svantaggi:

- a. Difficile da integrare in costruzioni e/o sistemi già esistenti se si vuole utilizzare il bus
- b. Numero di sensori limitato

Wireless a corto raggio

Zigbee

La tecnologia Zigbee è nata specificatamente per essere applicata in monitoraggio e controllo di edifici, è uno standard open source ed è mantenuto dalla Connectivity Standard Alliance (<https://csa-iot.org/all-solutions/zigbee/>).

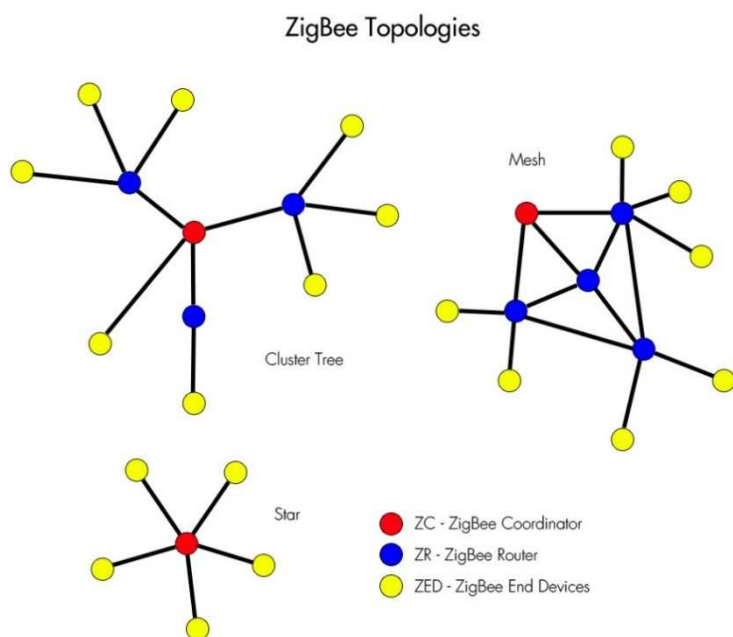
Questa tecnologia può operare utilizzando sia la frequenza di banda 2.4GHz che 868MHz ed i sensori che utilizzano questo tipo di tecnologia possono operare sia con l'ausilio di alimentatori esterni che a batteria. Nel caso dell'utilizzo a batteria la durata di esse è molto elevata; infatti, generalmente questi dispositivi rimangono attivi fino a cinque anni prima di necessitare di un cambio batteria (questa tipologia è la più diffusa).

In questa tecnologia i dispositivi vengono suddivisi in:

1. End device: può essere un sensore, un attuatore, un microcontrollore o tutti questi assieme (dipende dal dispositivo stesso)
2. Router: si occupa di ricevere le informazioni dagli end device, aggiungere end device ad un network Zigbee esistente, effettuare il routing delle informazioni tra i dispositivi e tra network diversi ed effettuare operazioni di buffering
3. Coordinator: il coordinator si occupa di avviare il network di dispositivi e mantenere il network attivo. Solo 1 coordinator per network è ammesso.
4. Gateway: il gateway riceve tutti i dati dai vari network Zigbee e si occupa di inviarli nella rete pubblica (Internet) dove sono richiesti.

La tecnologia Zigbee è utilizzata principalmente in spazi interni quali appunto uffici perché uno dei suoi vantaggi è il non dover effettuare operazioni di cablaggio, in quanto la maggior parte dei dispositivi opera tramite batteria e la trasmissione dei dati avviene in maniera wireless.

Uno dei punti di forza di Zigbee è la tipologia di network che viene creata che è di tipo mesh, una delle più robuste ed affidabili topologie.



Questa topologia è generata in maniera automatica dai dispositivi e aggiornata in maniera automatica: se qualche dispositivo va offline o non ha più alimentazione le informazioni possono essere trasmesse e ritrasmesse da ogni dispositivo a seconda delle esigenze.

Un network Zigbee può avere fino a 64000 dispositivi, il raggio di trasmissione varia dai 10 ai 100 metri a seconda degli ostacoli che sono presenti tra trasmettitore e ricevitore, grazie alla topologia di tipo mesh; tuttavia, va considerato che in molti casi il segnale può essere ritrasmesso da un dispositivo per cui la ricezione del dato è garantita.

In alcuni dispositivi può essere anche installata una antenna con un link budget di 20dBm il che estende la massima distanza di trasmissione fino a 1km con visuale libera.

Per concludere qui di seguito c'è un riassunto dei vantaggi e svantaggi di questa tecnologia:

1. Vantaggi:

- a. Network robusto grazie alla topologia mesh
- b. Cablaggi limitati
- c. Basso consumo
- d. Standard Open Source
- e. Numero molto elevato di dispositivi sul mercato
- f. Costo per dispositivo relativamente basso
- g. Ritrasmissione tra dispositivi senza limiti
- h. Crittografia implementata nativamente

2. Svantaggi:

- a. Necessità di pianificazione per decidere dove installare i dispositivi
- b. Necessita di quantità di hardware maggiore se confrontato con tecnologie della stessa categoria
- c. Utilizza la banda 2.4GHz, una delle più affollate e soggette a interferenza
- d. Dato che lo standard è open source bisogna verificare la compatibilità tra dispositivi se presi da diversi produttori

Z-Wave

La tecnologia Z-Wave è una tecnologia proprietaria e i dispositivi hanno bisogno di una licenza per essere costruiti; la manutenzione del codice è della Z-Wave Alliance (<https://z-wavealliance.org/>).

Questa tecnologia è nata per monitoraggio e controllo di edifici, utilizza la banda libera 900MHz per la trasmissione dei dati, anche in questo caso la maggior parte dei dispositivi Z-Wave è alimentato a batteria limitando il bisogno di effettuare cablaggi elettrici.

I dispositivi sono catalogati in:

1. **Nodo:** può essere un sensore, un attuatore, un microcontrollore o tutti questi assieme (dipende dal dispositivo stesso),
2. **Controller:** raccoglie i dati dai vari nodi per effettuare operazioni di monitoraggio e controllo, solo un controller per rete è ammesso,
3. **Gateway:** trasmette i dati dal controller alla rete pubblica (Internet) o dove richiesti.

Anche in questo caso il campo di applicazione di questa tecnologia sono gli ambienti chiusi come uffici, il raggio di trasmissione di circa 150m, la topologia di network di tipo mesh, tuttavia ci sono le seguenti limitazioni:

- Un network può avere al massimo 232 dispositivi,
- Il numero massimo di ritrasmissioni tra un dispositivo e l'altro è 4.

Un vantaggio della tecnologia Z-Wave è che la compatibilità tra dispositivi è garantita dal sistema di licenze, inoltre un database con tutti i dispositivi Z-Wave è disponibile e al momento ci sono circa 4000 dispositivi certificati sul mercato un numero in crescita costante.

Per riassumere la tecnologia Z-Wave:

1. **Vantaggi:**
 - a. Network robusto grazie alla topologia mesh
 - b. Cablaggi limitati
 - c. Basso consumo
 - d. Compatibilità tra dispositivi garantita dal sistema di licenze
 - e. Utilizzo della frequenza di banda 900MHz libera da interferenze
 - f. Raggio di trasmissione più elevato rispetto a Zigbee
 - g. Richiede meno hardware rispetto a Zigbee
 - h. Crittografia implementata nativamente
 - i. Database pubblico con prodotti certificati
2. **Svantaggi**
 - a. Necessità di pianificazione per decidere dove installare i dispositivi
 - b. Ritrasmissione limitata a 4 tentativi
 - c. Massimo numero di dispositivi per network limitata a 232

Wi-Fi

La tecnologia Wi-Fi è forse la più conosciuta ed utilizzata.

Questa tecnologia utilizza la frequenza di banda 2.4GHz per la trasmissione dati ed è nata per trasmettere una elevata quantità di dati motivo per cui è particolarmente energivora rispetto alle tecnologie descritte in precedenza: per tale motivo quasi tutti i sensori che utilizzano questa tecnologia hanno bisogno di alimentazione esterna: esistono sensori in commercio che utilizzano batterie ma queste hanno una durata molto limitata e devono essere sostituite solitamente una o più volte l'anno.

Il raggio di trasmissione è di circa 50m: questo aumenta il numero di access point necessari a coprire la stessa superficie rispetto alle tecnologie descritte precedentemente (Zigbee e Z-Wave).

Con l'aumento di access point aumenta anche la necessità di effettuare cablaggi; tuttavia, se è già presente nell'edificio un impianto di accesso WiFi esso può essere sfruttato tranquillamente per integrare i sensori.

Per quanto riguarda la topologia di network essa può essere di qualsiasi tipo utilizzando la tecnologia WiFi; sarà necessario prevedere l'installazione di un gateway ad-hoc che riceva i dati dai vari sensori, uniformi il dato e lo trasmetta.

Anche in questo caso i protocolli più interessanti per il progetto sono:

- Modbus
- OpcUA
- EtherNET/IP
- BacNET
- LonWorks

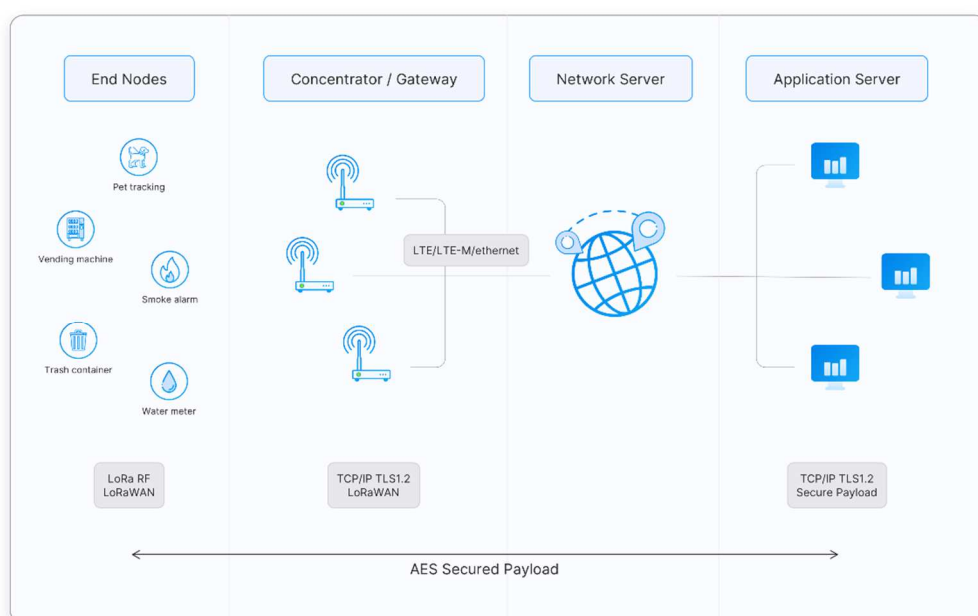
Wireless a lungo raggio

LoRa WAN

La tecnologia LoRa WAN fa parte di una famiglia di tecnologie chiamate LPWAN (Low Power Wide Area Network), il cui scopo principale è rendere possibile la trasmissione di dati a lunga distanza nell'ordine dei chilometri utilizzando bassa potenza.

Un network LoRa WAN ha sempre la topologia a stella ed è formato dai seguenti elementi:

1. End device: dispositivo che invia/riceve i dati,
2. Gateway: riceve i messaggi dagli end device e li invia al Network Server, questi gateway vengono in genere presi in affitto da terze parti, in particolare da compagnie telefoniche in quanto queste hanno antenne con la migliore visibilità e ricezione per questo tipo di tecnologia,
3. Network server: software che si occupa di gestire l'intero network e i dati del sistema ad un Application Server.



I dati sono trasmessi utilizzando crittografia di tipo AES.

Nell'Unione Europea questa tecnologia opera utilizzando la banda 863-870MHz con un duty cycle massimo pari all'1%. Questo significa che per legge un dispositivo LoRa WAN può trasmettere e ricevere al massimo 864 secondi al giorno ovvero circa 15 minuti; tuttavia, bisogna controllare il tipo di contratto che si va ad effettuare con la compagnia che ha il gateway in quanto ulteriori restrizioni potrebbero essere in atto.

Il fatto che questa tecnologia sia di tipo LPWAN fa sì inoltre che i data rate siano bassi, motivo per cui si arriva fino a un massimo di circa 5kbps; va considerato che il data rate è determinato dal cosiddetto spreading factor (SF), va quindi trovato il giusto equilibrio tra questo fattore e la durata della batteria dei dispositivi che trasmettono i dati: maggiore è lo SF più il dispositivo dovrà rimanere attivo per trasmettere e quindi ridurrà la vita della batteria più velocemente.

Tutte queste considerazioni fanno sì che questa tecnologia trovi impiego nei seguenti scenari:

1. Trasmissione di dati a lunga distanza, svariati km (tipicamente 5km in ambito urbano e 15km in ambito rurale),
2. Trasmissione di dati non in tempo reale,
3. Trasmissione da località remote come appunto dei pozzi per estrazione acqua o dei depuratori.

Per riassumere la tecnologia LoRa WAN:

1. Vantaggi:
 - a. Possibilità di trasmettere dati da località remote su lunga distanza
 - b. Consumo batteria del dispositivo molto bassa, se il dispositivo è equipaggiato con pannello solare e batteria tampone la durata dipende solo dalla vita della batteria stessa
 - c. Gateway distribuiti sul territorio grazie alle antenne delle varie Telco, in alternativa progetti community driven sono disponibile (The Thing Network per esempio)
 - d. Facile da rendere operativo grazie ad una architettura semplice
 - e. Trasmissione praticamente esente da interferenze
 - f. Costo basso (circa 20 euro per modulo LoRa WAN)
 - g. Se non c'è copertura da parte delle varie Telco si può costruire un gateway in maniera semplice e fare un deploy custom di esso con costi bassi
2. Svantaggi:
 - a. Bassa capacità di trasmissione dati
 - b. Dimensione del pacchetto dati molto limitata
 - c. Tempo di trasmissione limitato per legge
 - d. Non adatta ad applicazioni e monitoraggio in tempo reale
 - e. Vista la limitata dimensione del pacchetto e il poco tempo di trasmissione a disposizione una architettura che preveda conferma non è consigliata, il tipo "fire and forget" è il più indicato

NB-IoT

Narrow Band IoT è la tecnologia più recente disponibile sul mercato. A differenza di LoRa WAN e Sigfox utilizza la frequenza di banda sotto licenza LTE, permettendo di sfruttare la rete cellulare esistente per la trasmissione e ricezione dati e offrendo la più grande copertura finora vista.

La larghezza di banda è di massimo 200kHz e sono previste 3 modalità di trasmissione possibili:

1. Standalone: utilizza parte della banda GSM per trasmettere
2. In-Band: utilizza una porzione della frequenza LTE
3. Guard Band: utilizza una frequenza tra due carrier LTE per trasmettere i dati

Il data rate massimo teorico è di 100 kbps il più alto tra le tecnologie analizzate finora tuttavia anche il consumo energetico risulta essere più elevato.

Anche in questo caso questa tecnologia non è adatta per applicazioni in tempo reale in quanto la latenza complessiva può arrivare anche a 1.5-2 secondi. Il link budget complessivo è pari a 164dBm che permette ai dispositivi di avere una alta penetrazione anche in ambienti indoor o chiusi.

NB-IoT non necessita della presenza di un gateway: in questo caso, infatti, dato che si sfrutta la rete cellulare esistente i dispositivi possono comunicare direttamente con la destinazione senza aver bisogno di un gateway intermedio.

Per riassumere la tecnologia NB-IoT:

1. Vantaggi:
 - a. Utilizza la rete cellulare già esistente, quindi la copertura è la più ampia disponibile
 - b. Grazie al link elevato ha copertura anche indoor
 - c. Data rate più elevato rispetto ai competitor (fino a 100kbps)
 - d. Nessuna limitazione alla trasmissione/ricezione dati
2. Svantaggi:
 - a. No roaming dati disponibile (finora)
 - b. Necessita di SIM o sottoscrizione per poter essere utilizzato

Sigfox

Anche Sigfox fa parte della famiglia di tecnologie LPWAN. Utilizza la frequenza di banda 868MHz il raggio d'azione va da 5Km in aree urbano a 35km in aree rurali. La tecnologia di trasmissione impiegata è diversa rispetto a LoRa WAN: in questo caso, infatti, la trasmissione avviene tramite tecnologia Ultra Narrow Band (UNB) il che aumenta la probabilità di ricevere i messaggi a spese però della quantità di dati che si possono inviare.

La tecnologia Sigfox permette infatti di inviare al massimo 140 messaggi al giorno con un payload di 12byte e una velocità massima di trasmissione pari a 100 byte/sec. Le stesse limitazioni per quanto riguarda la banda a 868MHz sono presenti anche in Sigfox (duty cycle pari all'1%, possibilità di trasmettere al massimo circa 15 min al giorno).

Il network Sigfox si compone come segue:

1. Objects: sono i dispositivi finali che possono inviare/ricevere messaggi,
2. Stazioni di ricezione Sigfox: sono le antenne di ricezione proprietarie della rete Sigfox,
3. Sigfox Cloud: raccoglie tutti i messaggi provenienti dalle antenne di ricezione, viene interpellato dagli end device tramite API.

Sigfox operando tramite antenne proprietarie e Cloud proprietario è molto più simile ad un classico operatore telefonico che vende servizi, per cui ci sono costi aggiuntivi per utilizzare questa tecnologia; un'altra cosa che bisogna tenere in considerazione è anche la copertura che va verificata prima di effettuare la messa in opera dei vari sensori e dispositivi.

Per riassumere la tecnologia Sigfox:

1. Vantaggi:
 - a. Possibilità di trasmettere dati da località remote su lunga distanza
 - b. Consumo batteria del dispositivo molto bassa, se il dispositivo è equipaggiato con pannello solare e batteria tampone la durata dipende solo dalla vita della batteria stessa
 - c. Comunicazione robusta e raggio di trasmissione molto elevato
 - d. Dispositivi molto economici e con i consumi più bassi sul mercato
 - e. Backend e architettura di rete gestita
2. Svantaggi:
 - a. Low data rate, solo 100 byte/sec
 - b. Messaggi limitati a 12 byte nel caso uplink (trasmissione) e 8 byte per il downlink (ricezione)
 - c. Necessità di sottoscrivere un abbonamento
 - d. Nel caso non ci sia copertura non si può creare la propria infrastruttura
 - e. Non adatta ad applicazioni e monitoraggio in tempo reale

APPARATI DI UNA INFRASTRUTTURA FISICA

Network Hub

Un Hub è un dispositivo di rete che riceve un segnale e lo ritrasmette a tutti gli altri dispositivi collegati alla rete. Gli hub di rete operano utilizzando sempre la modalità half-duplex il che significa che permettono la trasmissione del segnale in invio o in ricezione in una sola direzione quindi l'invio e ricezione di dati in contemporanea non è possibile.

Gli hub si possono categorizzare in attivi e passivi; gli hub attivi quando ricevono il segnale provvedono anche ad amplificarlo agendo da "ripetitori", gli hub passivi si limitano a ripetere il segnale senza amplificarlo.

Questa tipologia di dispositivi di rete è di tipo legacy ed è stata soppiantata in favore dei network switches.

Network switches

Uno switch di rete è un dispositivo che mette in comunicazione più dispositivi nella stessa rete. Lo switch opera al livello due del modello ISO/OSI. La principale differenza tra l'hub e lo switch è che lo switch invia il segnale solo alla porta e al dispositivo a cui è destinata la trasmissione del segnale.

Esistono switch a numero fisso di porte e switch modulari che possono essere configurati a seconda delle esigenze.

Gli switch si possono inoltre differenziare in unmanaged and managed.

Gli switch unmanaged sono il tipo più basilare e offrono una configurazione fissa che non può essere modificata.

Gli switch managed offrono invece la possibilità di effettuare configurazioni personalizzate quali ad esempio la creazione di reti virtuali (VLAN), il settaggio delle porte e la qualità e priorità del traffico.

Alcuni switch possono avere la possibilità di utilizzare la tecnologia Power Over Ethernet (PoE) integrata al loro interno, questa tecnologia consente l'alimentazione dei dispositivi collegati tramite la trasmissione di tensione a 48V DC.

Network router

Il router è un dispositivo che serve a connettere due o più reti diverse tra loro.

A differenza di switch e hub il router utilizza pacchetti di dati, la sua funzione principale, infatti, è quella di gestire una tabella chiamata routing table dove vengono memorizzate alcune informazioni provenienti dai pacchetti, in particolare:

- Indirizzo IP e subnet mask della rete
- Indirizzo IP dei router delle reti verso cui deve essere instradato il traffico
- Informazioni riguardanti le interfacce dei dispositivi che sono collegati alla rete

Esistono due tipi di tabelle di routing: statiche e dinamiche.

Le tabelle statiche sono create manualmente da chi programma il dispositivo, non vengono aggiornate in maniera automatica.

Le tabelle dinamiche invece vengono generate automaticamente dal dispositivo utilizzando dei protocolli di routing per "scoprire" i router vicini e determinare i possibili instradamenti del segnale fino a destinazione.

Esistono diversi tipi di router, i principali sono:

- Wired router: mette in comunicazione reti cablate tra di loro
- Wireless router: utilizzati per mettere in comunicazione reti Wi-Fi con altre reti quali ad esempio la rete pubblica (Internet)
- Core router: utilizzati in grandi reti per trasmettere grandi quantità di dati all'interno di una rete ma non tra reti diverse, questo tipo di router viene impiegato dagli ISP (Internet Service Provider) per creare l'infrastruttura della rete di tipo WAN (Wide Area Network)
- Edge router: utilizzati per mettere in comunicazione core router con reti esterne
- Virtual router: applicazione software che implementa le funzionalità di un dispositivo router

Network gateway

Il network gateway è un dispositivo il cui compito è tradurre pacchetti dati tra diversi protocolli. Permettono il collegamento di reti che utilizzano protocolli di comunicazione diversi tra loro.

I gateway si possono distinguere in: monodirezionali e bidirezionali.

Un gateway monodirezionale permette l'instradamento di dati in una sola direzione (in ingresso o in uscita), mentre il gateway bidirezionale permette l'instradamento in entrambe le direzioni.

I principali tipi di gateway sono:

- Network gateway: è il tipo più comune di gateway e permette la comunicazione tra reti con protocolli diversi
- Cloud storage gateway: questo tipo di gateway si occupa di tradurre i pacchetti dati in ingresso come ad esempio richieste API, SOAP o REST in richieste storage verso risorse cloud.
- Internet To Orbit (I2O) gateway: questo tipo di gateway mette in comunicazione risorse Internet con i vari satelliti presenti in orbita
- IoT gateway: questo tipo di gateway traduce dati provenienti da sensori e dispositivi IoT come ad esempio Modbus, Zigbee, RS232... in pacchetti dati comprensibili per endpoint cloud
- VoIP Trunk Gateway: questo tipo di gateway mette in comunicazione linee telefoniche analogiche (POTS) con linee telefoniche digitali (VoIP)

Network signal converter

I network signal converter sono dispositivi che convertono i segnali da un tipo di tecnologia di trasmissione ad un altro tipo.

I principali tipi di operazioni che si possono eseguire sono:

- Conversione da un segnale analogico a digitale, esempio: lettura di un valore di corrente in ingresso, conversione del valore in digitale, confezionamento del dato in un pacchetto di trasmissione, e invio del pacchetto tramite rete Ethernet,
- Conversione di pacchetti dati da un protocollo ad un altro protocollo, esempio: lettura dati da Modbus, conversione dati letti in formato MQTT e invio tramite rete Ethernet,
- Trasmissione di un dato e/o segnale da un punto ad un altro, esempio: invio di segnale HDMI tramite rete Ethernet a distanze elevate.

Durante la progettazione di qualsiasi tipo di impianto che preveda l'utilizzo di tecnologie digitali e/o di trasmissione dati l'impiego di questo tipo di dispositivo semplifica l'integrazione di diversi dispositivi o il raggiungimento di distanze elevate.

Network firewall

Sono dispositivi di rete che si occupano della sicurezza della rete.

Un firewall si occupa di analizzare il traffico della rete in ingresso ed in uscita, ed in base a delle regole definite decide se consentire o negare il permesso ai pacchetti dati di passare.

Lo scopo principale di un firewall è quello di creare una barriera tra il traffico interno ed esterno alla rete.

Esistono due principali forme di firewall: firewall software e firewall hardware.

Il firewall software è una applicazione installata in un PC oppure a livello di sistema operativo di un dispositivo, che si occupa della protezione “base” del dispositivo.

Il firewall hardware è invece un dispositivo che integra componenti specifici per svolgere il lavoro di firewall: esso è un appliance hardware autonomo nel quale gira lo strato software (sistema operativo + servizi di analisi del traffico di rete). Una rete moderna utilizza questo tipo di dispositivo come protezione primaria.

I principali tipi di firewall sono:

- Packet Filtering firewall: questa è la versione più semplice di firewall. Questo firewall analizza i pacchetti in arrivo e in uscita e determina se possono passare oppure no,
- Stateful Packet Inspection firewall: evoluzione del Packet Filtering che gestisce le sessioni mantenendo una tabella dello stato delle connessioni,
- Proxy firewall: utilizzato assieme ad un dispositivo gateway questo firewall crea una sessione intermedia tra il gateway e l'esterno rendendo così più difficile ad eventuali malintenzionati l'intrusione all'interno della rete. Questo tipo di firewall analizza solo traffico di tipo Internet,
- Deep Packet Inspection firewall: riunisce al suo interno le caratteristiche dello Stateful Packet Inspection e del Proxy, aggiungendo la funzionalità di ispezione granulare dei dati (payload) presenti nei pacchetti al fine di bloccare minacce note o data exfiltration,
- NAT firewall: questo firewall permette a dispositivi di diverse reti di collegarsi alla rete pubblica utilizzando un unico indirizzo IP, questo tipo di firewall permette di mantenere anonimi gli indirizzi IP dei dispositivi della rete,
- Internal Segmentation firewall: questo tipo di firewall gestisce l'accesso nei segmenti interni e di accesso della rete per controllare ed ispezionare in particolar modo il traffico in uscita.

Requisiti ambientali dei sensori

Tutti i sensori devono fornire una adeguata protezione per eventuali intrusioni di agenti esterni; per questo a seconda del tipo di ambiente ciascun sensore e dispositivo dovrà avere un adeguato livello di “Ingress Protection” (IP)

Lo standard IP è uno standard internazionale che garantisce diversi livelli di protezione da agenti esterni, questo standard prende in considerazione solidi e liquidi e classifica il livello di protezione utilizzando due numeri.

Il primo numero può variare da 0 a 6 e rappresenta la protezione dall'ingresso di particelle solide, 0 significa nessuna protezione mentre 6 significa che il dispositivo è completamente sigillato e a prova di polvere. In maniera analoga il secondo numero rappresenta la protezione contro l'intrusione di acqua; in questo caso il numero vanno da 0 a 9 dove 0 non presenta nessuna protezione mentre 9 è la protezione massima e offre resistenza a getti ad alta pressione e alta temperatura a distanza ravvicinata. La categoria 9 si divide inoltre in altre sotto categorie speciali a seconda del tipo di liquido.

Per gli ambienti esterni si raccomanda un livello minimo IP 44 che offre protezione da polveri e oggetti esterni più grandi di 1mm e protezione dall'acqua proveniente da qualsiasi direzione.

IoT Gateway

Un gateway IoT è un dispositivo collegato che ha il ruolo di:

1. Rendere possibile la comunicazione tra dispositivi con tecnologie di comunicazione diverse
2. Mette in comunicazione i dispositivi del cosiddetto "field layer" ovvero tutti i sensori, attuatori e dispositivi che compongono la rete di dispositivi IoT
3. Effettua il pre-processamento dei dati, ovvero si occupa di raccogliere, aggregare tutti i dati provenienti dal "field layer" tradurli in un protocollo di comunicazione comprensibile al backend, impacchettare i dati ed inviarli al livello tecnologico successivo.
I protocolli che possono subire più facilmente il processo di "ingestion" nel cloud sono: HTTP(S), AMQP(S), MQTT(S).
4. Provvede una sicurezza aggiuntiva ai dispositivi del "field layer" in quanto essi non vengono esposti direttamente alla rete pubblica ma vengono mascherati dal gateway IoT. Da notare comunque che per garantire un livello di sicurezza ottimale il gateway IoT viene usato in congiunzione ad uno o più network firewall.
5. Il gateway IoT può funzionare come "intelligent edge" cioè eseguire operazioni di controllo dei dispositivi del "field layer" andando così a prendere in carico azioni in base ai dati in ingresso.
6. Il gateway IoT può anche provvedere storage locale per effettuare operazioni di caching e/o storage dei dati provenienti dal field layer.

Esistono normalmente due tipi di IoT gateway in commercio:

1. Dispositivi con usi specifici come, ad esempio, convertire dati provenienti da protocollo Modbus a MQTT: generalmente questo tipo di dispositivi hanno hardware embedded dedicato ed ottimizzato per il compito. Questo tipo di dispositivo non richiede inoltre programmazioni di tipo custom ma solo di essere configurati,
2. Dispositivi generici, ad esempio si può adibire un industrial PC a gateway IoT. In questo caso il PC avrà bisogno di programmazione custom o applicazioni di terze parti per poter accedere a tutti i dati provenienti dal field layer.

Sintesi dell'infrastruttura di rete AS-IS

Sede aziendale corporate

La sede principale di Cotral è ubicata in Via B. Alimena, 105 – 00173 Roma

La sede è adibita ad uso uffici: operativi e direzionali. L'edificio è di tipo direzionale.

Ha il ruolo di centro stella per le telecomunicazioni. Ospita le sale server per le apparecchiature fisiche.

Sedi secondarie

Destinazione d'uso

- Officine: spazi in cui si svolgono attività di manutenzione (con risorse interne o esterne) sulla flotta autobus al fine di consentire il corretto espletamento del servizio di TPL nel rispetto delle condizioni previste di sicurezza, regolarità e affidabilità.
- Uffici Esercizio: Locali adibiti a personale in cui vengono svolte attività propedeutiche all'erogazione del servizio del trasporto pubblico (uffici – sale per autisti - sale ricreative - servizi igienici).
- Uffici Manutenzione: Locali adibiti a personale nei quali vengono svolte attività per gestione operativa ed amministrativa della flotta autobus.
- Magazzini: locali adibiti allo stoccaggio di materiale necessario alla manutenzione dei mezzi.
- Capolinea: aree adibite allo stazionamento dei bus in partenza, spesso provviste di infrastrutture come biglietterie, sale di aspetto con monitor informativi ed uffici per il personale Cotral.

Il cablaggio orizzontale può essere in rame o in fibra ottica, a seconda delle distanze tra gli apparati.

Ogni destinazione d'uso richiede diverse tipologie di apparati ed una sede potrebbe accorparne più di una. Gli apparati IT locali sono di supporto alle funzioni specifiche della sede. In generale, sono presenti uno o più rack che contengono:

1. switch per collegare pc, stampanti, lettori di badge, bigliettatrici, Access Point, monitor informativi
2. server per funzioni locali (DHCP, printer, raccolta dati da autobus) e per la trasmissione al Data Center nella sede principale

Strutture rilevanti di interconnessione tra le sedi

Cotral conta un totale di 50 siti remoti consolidati e 3 nuovi in allestimento, legati all'incorporazione delle ferrovie concesse del Lazio. Al momento i collegamenti verso la sede costituiscono un MPLS. Le attuali connessioni dalle sedi sono così suddivise:

- 16 fibra ottica FTTH con backup in fibra o in xDSL
- 6 xDSL di categoria business (>8 Mbps) con backup in xDSL con banda pari al 50% della primaria
- 33 xDSL (<8 Mbps) con backup in xDSL con banda pari al 50% della primaria
- 1 sede con connettività solo 4G
- Non ci sono WLAN di categoria business

Le linee di backup sono, dove possibile, su POP differenti ma usano lo stesso provider (Fastweb)

Considerata la maggiore affidabilità delle fibre ottiche, è in atto un progetto con Fastweb per utilizzare questa tecnologia in tutte le sedi: il provider informa Cotral circa le estensioni della propria rete nel Lazio al fine di valutare congiuntamente e tempestivamente la possibilità di raggiungere un deposito Cotral.

Siti non connessi da infrastrutture IT:

- Amatrice
- Filettino
- Leonessa

- Tolfa – in fase di valutazione da parte di Fastweb la copertura 4G

La piattaforma di Metering / Energy Monitoring, laddove tecnicamente possibile o conveniente darà preferenza alle connessioni cablate

Reti Wi-Fi

Al momento COTRAL copre piazzali e officine mediante opportuna ubicazione di Access Point. Per le finalità di futuro utilizzo di sensoristica sul campo, sarà possibile fare uno (o più) SSID dedicati al Metering / Energy Monitoring con autenticazione ad hoc

Video Sorveglianza

È completamente separata dalla rete IT, anche per quanto riguarda la trasmissione immagini verso la/le Centrale/i esterne.

Nei locali tecnici presso i depositi ci sono rack e cablaggio separati per la videosorveglianza. Anche nella sede centrale è tutto autonomo.

Non se ne prevede l'uso per la piattaforma di Metering / Energy Monitoring

Telefonia VoIP

Cotral è dotata di una centrale telefonica Avaya Aura, installata presso la sede di via Alimena. In questa sede tutti i derivati sono VoIP o FoIP.

Circa nel 50% dei depositi sono stati installati telefoni VoIP, che fanno riferimento alla Aura citata.

La telefonia tradizionale è in uso ove non sia stato possibile portare VoIP.

Non se ne prevede l'uso per la piattaforma di Metering / Energy Monitoring

Sicurezza perimetrale

La sicurezza perimetrale è gestita da due cluster di firewall e da un proxy con anti-malware, SSL Inspection e content filtering.

Il traffico in ingresso (da client Internet verso server pubblici di Cotral) è protetto da un cluster di firewall, mentre quello in uscita (da client interni verso server su Internet) è protetto dall'altro cluster e dal proxy.

Il traffico dalle sedi periferiche verso il Data Center può essere filtrato ma, attualmente, non ci sono protocolli o porte bloccate.

Nell'ottica di un progetto di metering, considerato che spesso i sensori o i gateway locali usano comunicazioni non proxabili, ampi intervalli di porte TCP/UDP, protocolli non RFC-compliant, certificati auto emessi e non trustabili, si ritiene ideale l'architettura descritta di seguito:

1. I sensori trasmettono dati verso gateway locali attraverso interfacce di tipo qualsiasi. Cotral non imporrebbe alcun vincolo su queste comunicazioni

2. I gateway locali trasmettono via TCP/IP i dati ad un message broker interno a Cotral. Sarebbe ideale che i gateway fossero appliance rugged perché l'alimentazione elettrica non è stabile in molte sedi periferiche
3. Il message broker trasmette i dati raw/elaborati ad un server esterno. Cotral è in grado di fornire l'infrastruttura per un message broker "intelligente", che effettui molte elaborazioni prima della trasmissione. Inoltre, avere un singolo punto di uscita permetterebbe di gestire al meglio la sicurezza della comunicazione

Esempi di infrastruttura fisica

Per concludere questo capitolo riguardante l'infrastruttura fisica riportiamo alcuni esempi di infrastrutture tipiche divise per tipo di spazio. Gli esempi non sono vincolanti per future scelte implementative ma rappresentano alcuni scenari coerenti con il presente studio di fattibilità, soprattutto per dare concretezza alle diverse teorie esposte.

Sede aziendale corporate

Tipologia di spazi

Si tratta di locali destinati prevalentemente ad un uso tipico da ufficio; le attività che vengono svolte all'interno di tali locali sono tipicamente:

- Lavoro a PC
- Riunioni
- Attività intellettuali

Gli ambienti tipici interni sono:

- Locali tecnici:
 - o cabina ricezione energia elettrica (POD)
 - o cabina di trasformazione MT/BT (se applicabile)
 - o cabina ricezione gas (PDR)
- Uffici singoli o multi-postazione
- Corridoi
- Sale riunioni
- Servizi
- Sale server
- Magazzini e archivi
- Reception

Gli ambienti tipici esterni sono:

- Piazzali di manovra
- Parcheggi auto
- Tettoie / terrazzi

Gli impianti tipicamente presenti sono:

- Computer
- Stampanti e plotter
- Armadi Rack per cablaggio strutturato
- Climatizzazione invernale
 - o Impianto centralizzato a Gas Metano o Gasolio
 - o Impianto centralizzato a pompa di calore
- Climatizzazione estiva
 - o Impianto centralizzato Gruppo Frigo (idronico o espansione diretta)
 - o Illuminazione interna ed esterna
 - o Solare fotovoltaico (autoproduzione)
 - o Rete idrica (acqua potabile e/o acqua di pozzo)

Infrastruttura fisica e configurazione

La sede aziendale può puntare ad essere il "fiore all'occhiello" di tutto il progetto.

Per questo l'esempio seguente propone una soluzione di intelligent building.

Per realizzare tale soluzione si vanno a integrare sistemi di analisi dei dati e building automation (o building management system), lo scopo di tale integrazione è quello di andare a monitorare e a prendere azioni in tempo reale al fine di ottimizzare consumi e ridurre gli sprechi, il risultato finale sarà quello di avere un edificio "vivo" in quanto l'automazione presente in loco prenderà decisioni in autonomia e gli attuatori andranno ad agire in maniera autonoma.

Tale sistema si andrà a occupare di:

- Monitoraggio e controllo HVAC
- Monitoraggio e gestione luci e livello luce
- Gestione aperture finestre e tapparelle
- Monitoraggio e ottimizzazione uso acqua
- Monitoraggio occupazione locali

Per realizzare questo si procede in 3 fasi distinte:

1. Realizzazione infrastruttura distribuita di controllo, attuazione e monitoraggio con tecnologia KNX
2. Integrazione di sistemi già esistenti all'interno del nuovo sistema
3. Ottimizzazione del sistema tramite analisi dei dati e ottimizzazione della programmazione del sistema di controllo, attuazione e monitoraggio

Si andrà a realizzare una rete di sensori e attuatori utilizzando sia l'infrastruttura già presente in loco che l'installazione di nuovi dispositivi.

Si possono evidenziare in particolare l'uso in loco di:

- Infrastruttura Ethernet + Wi-Fi
- Infrastruttura Modbus per controllo HVAC

L'infrastruttura in loco andrà affiancata da una nuova infrastruttura a bus KNX; tale infrastruttura sarà distribuita al fine di ridurre i costi di stesura di nuovi cavi specializzando ciascuna sezione dell'infrastruttura in una o più mansioni contemporaneamente.

La nuova infrastruttura invierà i dati monitorati al backend, utilizzando un gateway, per effettuare l'analisi degli stessi e studiare metodi di ottimizzazione, il quale potrà essere riprogrammato in base alle soluzioni scelte andando così a ottimizzare i consumi dell'edificio e individuare gli sprechi al fine poi di andarli a ridurre.

Un'altra soluzione più economica potrebbe essere l'utilizzo dell'infrastruttura già esistente, utilizzando sensori con protocollo di comunicazione Modbus trasmesso tramite l'infrastruttura WiFi presente in loco, utilizzando poi un gateway MQTT per l'invio dei dati dall'edificio verso il backend.

Officine

Tipologia di spazi

Si tratta di locali destinati prevalentemente alla manutenzione sulla flotta di autobus; le attività che vengono svolte all'interno di tali locali sono tipicamente:

Infrastruttura fisica e di rete [FIELD LAYER]

- Lavori meccanici
- Lavori elettrici

Gli ambienti tipici interni sono:

- Locali tecnici:
- cabina ricezione energia elettrica (POD)
- cabina di trasformazione MT/BT (se applicabile)
 - o cabina ricezione gas (PDR)
 - o Officina
 - o Servizi
 - o Magazzini ricambi

Gli ambienti tipici esterni sono:

- Piazzali di manovra
- Parcheggi auto

Gli impianti tipicamente presenti sono:

- Ponti sollevatori da 8500 Kg a colonna
- Compressore aria rotativo
- Pressa elettro-idraulica da 100 ton
- Vasche di lavaggio ad ultrasuoni
- Quadri di distribuzione per attrezzature varie
- Illuminazione locali per attività manutentive industriali
- Solare fotovoltaico (autoproduzione)
- Rete idrica (acqua potabile e/o acqua di pozzo)

Infrastruttura fisica e configurazione

I vari reparti officine presentano diverse tipologie di ambienti e ampi spazi.

A seconda dello spazio e della dimensione di quest'ultimo si andranno quindi a adottare diverse tipologie di infrastruttura.

Se il magazzino possiede già una infrastruttura Ethernet e/o Wi-Fi, questa sarà estesa al fine di integrare i nuovi sensori di misurazione. Il reparto officina può presentare un sistema di gestione integrato e quindi una infrastruttura Ethernet; nel caso questo non sia presente si provvederà a creare la nuova infrastruttura che sfrutterà eventuali equipaggiamenti già presenti in loco, quali ad esempio cavidotti, per ridurre i costi della stesura dell'infrastruttura. Il sistema poi si farà uso di network converters per convertire eventuali segnali industriali monitorati quali ad esempio RS-232 e RS-485 provenienti dai dispositivi di officina, oltre a questo i nuovi sensori potranno essere integrati usando la stessa metodologia se necessario.

I locali tecnici generalmente ospitano già dispositivi e apparati di rete quindi integrarli all'interno del sistema di monitoraggio dovrebbe risultare abbastanza semplice.

I servizi invece si possono integrare sfruttando sensori che utilizzano la tecnologia WiFi andando a piazzare opportunamente degli access point vicino ad essi. Qualora non sia possibile si potranno utilizzare sensori Zigbee o Z-Wave per aggiungere tali dispositivi alla rete di monitoraggio evitando così di dover effettuare stesure cavi.

Il monitoraggio di un eventuale sistema fotovoltaico può essere affidato a dei sensori che utilizzano NB-IoT oppure LoRa WAN a seconda del numero delle letture e della copertura di tali tecnologie.

Nel caso il sistema di monitoraggio si trovi in un locale tecnico si possono utilizzare eventuali infrastrutture presenti nel medesimo locale.

Per quanto riguarda il monitoraggio dei piazzali di manovra e dei parcheggi, qualora non ci sia adeguata copertura Wireless, si aprono 2 possibili vie:

- Utilizzare una tecnologia di comunicazione wireless a lungo raggio, ovvero: NB-IoT, LoRa WAN e Sigfox se c'è copertura per l'impiego di tali tecnologie

- Nel caso non fosse presente copertura per usare direttamente una tecnologia wireless a lungo raggio si dovrà procedere a cablare il piazzale con l'ausilio di fibre ottiche oppure creare una rete di comunicazione punto-punto utilizzando il protocollo LoRa (non a lungo raggio)

Eventuali impianti HVAC possono essere integrati andando a leggere e convertire i dati in Modbus RTU o TCP utilizzando dei network converters e inviando poi il dato.

I dati raccolti utilizzando queste infrastrutture avranno gateway di tipo diverso a seconda della tecnologia impiegata e i sensori impiegati e saranno inviati al backend per essere analizzati e determinare quali strategie introdurre per ridurre i costi di esercizio dell'edificio, ottimizzarne i consumi e ridurre gli sprechi.

Uffici presso impianti e uffici esercizio

Tipologia di spazi

Si tratta di locali destinati prevalentemente alla gestione operativa ed amministrativa della flotta di autobus; le attività che vengono svolte all'interno di tali locali sono tipicamente:

- Attività al PC e d'ufficio in generale
- Riunioni
- Programmazione

Gli ambienti tipici interni sono:

- Locali tecnici:
 - o cabina ricezione energia elettrica (POD)
 - o cabina di trasformazione MT/BT (se applicabile)
 - o cabina ricezione gas (PDR)
- Uffici
- Sale riunioni
- Sale server
- Servizi
- Magazzini e archivi
- Sale autisti
- Sale ricreative
- Servizi

Gli ambienti tipici esterni sono:

- Parcheggi auto

Gli impianti tipicamente presenti sono:

- Computer
- Stampanti e plotter
- Armadi Rack per cablaggio strutturato
- Climatizzazione invernale
 - o Impianto centralizzato a Gas Metano o Gasolio
 - o Impianto centralizzato a pompa di calore
- Climatizzazione estiva
 - o Impianto centralizzato Gruppo Frigo (idronico o espansione diretta)
- Illuminazione interna ed esterna
- Solare fotovoltaico (autoproduzione)
- Rete idrica (acqua potabile e/o acqua di pozzo)

Infrastruttura fisica e configurazione

Questo tipo di locale presenta già una infrastruttura IT la cui composizione è fatta da punti di accesso Ethernet e Wi-Fi.

In questo caso si può pensare di integrare i sensori all'interno dell'infrastruttura già esistente andando a sfruttare principalmente la tecnologia Wi-Fi. Nel caso questo non sia possibile si può pensare di utilizzare i sensori in congiunzione con network converters e creare una rete mesh ad-hoc usando la tecnologia Zigbee o Z-Wave, questa rete necessita poi di un gateway per inviare i dati al backend.

L'impianto HVAC degli uffici può essere integrato utilizzando sia Modbus TCP o RTU oppure se presente l'interfaccia ethernet.

Il monitoraggio di un eventuale sistema fotovoltaico può essere affidato a dei sensori che utilizzano NB-IoT oppure LoRa WAN a seconda del numero delle letture e della copertura di tali tecnologie.

Nel caso il sistema di monitoraggio si trovi in un locale tecnico si possono utilizzare eventuali infrastrutture presenti nel locale oppure effettuare la messa in opera di cablaggio atto a integrare l'impianto nell'infrastruttura IT esistente.

I sensori nei parcheggi auto possono in questo caso utilizzare comunicazione wireless a lungo raggio come NB-IoT, LoRa WAN o Sigfox o se disponibile anche nel parcheggio effettuare una integrazione tramite Wi-Fi.

I dati raccolti dai vari sensori utilizzeranno gateway di vario tipo per inviare i dati al backend per monitoraggio e analisi.

Soluzioni di smart building sono integrabili in queste aree senza particolari difficoltà.

Depuratori

Tipologia di spazi

Si tratta di siti destinati al trattamento delle acque di prima pioggia e acque reflue; le attività che vengono svolte all'interno di tali locali sono tipicamente:

- Trattamento acque

Gli ambienti tipici interni sono:

- Locali tecnici:
 - o cabina ricezione energia elettrica (POD)
 - o cabina di trasformazione MT/BT (se applicabile)
 - o cabina ricezione gas (PDR)

Gli impianti tipicamente presenti sono:

- Impianti destinati al trattamento delle acque reflue e prima pioggia
 - o Depuratori Centralizzati
 - o Depuratori Acque prima pioggia o acque di piazzale
 - o Depuratori Acque biologiche
- Prelievo dell'acqua con elettropompe
- Illuminazione interna ed esterna
- Rete idrica (acqua di pozzo)

Infrastruttura fisica e configurazione

Questo tipo di impianto non necessita di un monitoraggio costante e in tempo reale in quanto il ciclo di trattamento delle acque può impiegare anche più di 24 ore per essere completato.

Un aspetto da tenere in considerazione per questa tipologia di impianto è il fatto di proteggere gli equipaggiamenti ed i sensori installati assicurandosi che abbiano un grado di protezione contro la presenza di acqua e liquidi idonea con un rating IP minimo pari a 23 ovvero protezione da penetrazione di oggetti di dimensioni più grandi di 12.5mm (classe di protezione 2) e protezione da spruzzi di acqua con un angolo fino a 60° (classe di protezione 3), eventuali cablaggi dovranno usare cavi di tipo outdoor/waterproof se posati in prossimità di acqua.

Gli impianti di depurazione non hanno infrastrutture IT disponibili in loco quindi l'installazione di sensori dovrà prevedere l'uso di uno o più gateway con tecnologie di trasmissione a lungo raggio.

I dispositivi presenti in loco presentano tecnologie di comunicazione di tipo industriale quindi RS232 o RS485 con protocolli vari, tra cui i più diffusi sono Modbus e sensori a tensione analogici.

Per tali interfacce si provvederà a mettere in opera network converters e dispositivi gateway che sfruttino le tecnologie di comunicazione a lungo raggio quali NB-IoT, LoRa WAN e Sigfox.

Archi di lavaggio

Tipologia di spazi

Si tratta di sistemi di lavaggio a portale con doppia spazzola per la pulizia delle superfici esterne degli autobus; le attività che vengono svolte all'interno di tali locali sono tipicamente:

- Lavaggio autobus
- Trattamento acque

Gli ambienti tipici interni sono:

- Locali tecnici:
 - o cabina ricezione energia elettrica (POD)
 - o cabina di trasformazione MT/BT (se applicabile)
 - o cabina ricezione gas (PDR)

Gli impianti tipicamente presenti sono:

- Portale lavaggio
- Pompe di rilancio
- Depuratore arco di lavaggio
- Prelievo dell'acqua con elettropompe
- Illuminazione interna ed esterna
- Rete idrica (acqua di pozzo)

Infrastruttura fisica e configurazione

L'infrastruttura da realizzare presso queste installazioni presenta sfide ulteriori rispetto alle altre, in quanto sono presenti fattori di rischio ambientale per la vita dei sensori e le apparecchiature elettroniche in generale in quanto sono presenti getti di acqua ad alta pressione e altri fattori di rischio quali polveri dovute al lavaggio dei bus stessi.

Viste queste premesse quindi l'infrastruttura realizzata dovrà essere "waterproof" e offrire un adeguato livello di protezione IP, il cui livello consigliato se vengono posizionati sensori o dispositivi vicino agli archi stessi è di grado 69.

Eventuali cablaggi ed i relativi connettori dovranno essere di tipo outdoor/waterproof per ridurre eventuali rischi di elettrocuzione dovuti alla presenza appunto di acqua.

I locali tecnici di ricezione energia elettrica, cabina di trasformazione e ricezione del gas saranno molto probabilmente lontano dagli equipaggiamenti, questo per garantire appunto la sicurezza del posto di lavoro per cui probabilmente non saranno raggiunti da infrastrutture di rete preesistenti: sarà quindi opportuno pensare a soluzioni di tipo wireless a lungo raggio per consentire l'invio di dati provenienti da tali locali; stessa cosa si può applicare alle pompe e all'acqua di pozzo estratta e il sistema di illuminazione esterno.

Per quanto riguarda invece l'impianto di distribuzione dell'acqua questo molto probabilmente avrà un sistema di controllo integrato che utilizza la tecnologia M-Bus. Se questo è il caso allora la soluzione più semplice sarà utilizzare un network converter in congiunzione con un gateway per convertire i dati che arrivano dal sistema M-Bus in dati leggibili per il backend.

Per il monitoraggio degli archi di lavaggio si dovrà invece procedere ad integrare eventuali sistemi di monitoraggio industriale della macchina utilizzando network converters e gateway, in alternativa se la macchina prevede già la possibilità di monitoraggio tramite Ethernet sarà opportuno creare una rete locale per accedere e monitorare tutti i dispositivi utilizzando un unico punto di accesso. La connessione in questo caso può essere fatta utilizzando un gateway con accesso alla rete cellulare integrato oppure un gateway wireless a lungo raggio. La scelta di una tipologia di accesso rispetto all'altra deve essere fatta in funzione della quantità di dati che devono essere monitorati e se è necessario o meno il monitoraggio in tempo reale della macchina.

Come evidenziato, questo tipo di ambiente necessita di più tecnologie al fine di creare la rete di monitoraggio dati richiesta.

Piazzali di sosta

Tipologia di spazi

Si tratta di sistemi di area parcheggio e movimentazione bus; le attività che vengono svolte all'interno di tali locali sono tipicamente:

- Parcheggio autobus

Gli ambienti tipici interni sono:

- Locali tecnici:
 - o cabina ricezione energia elettrica (POD)

Gli impianti tipicamente presenti sono:

- Illuminazione interna ed esterna
- Solare fotovoltaico (autoproduzione)

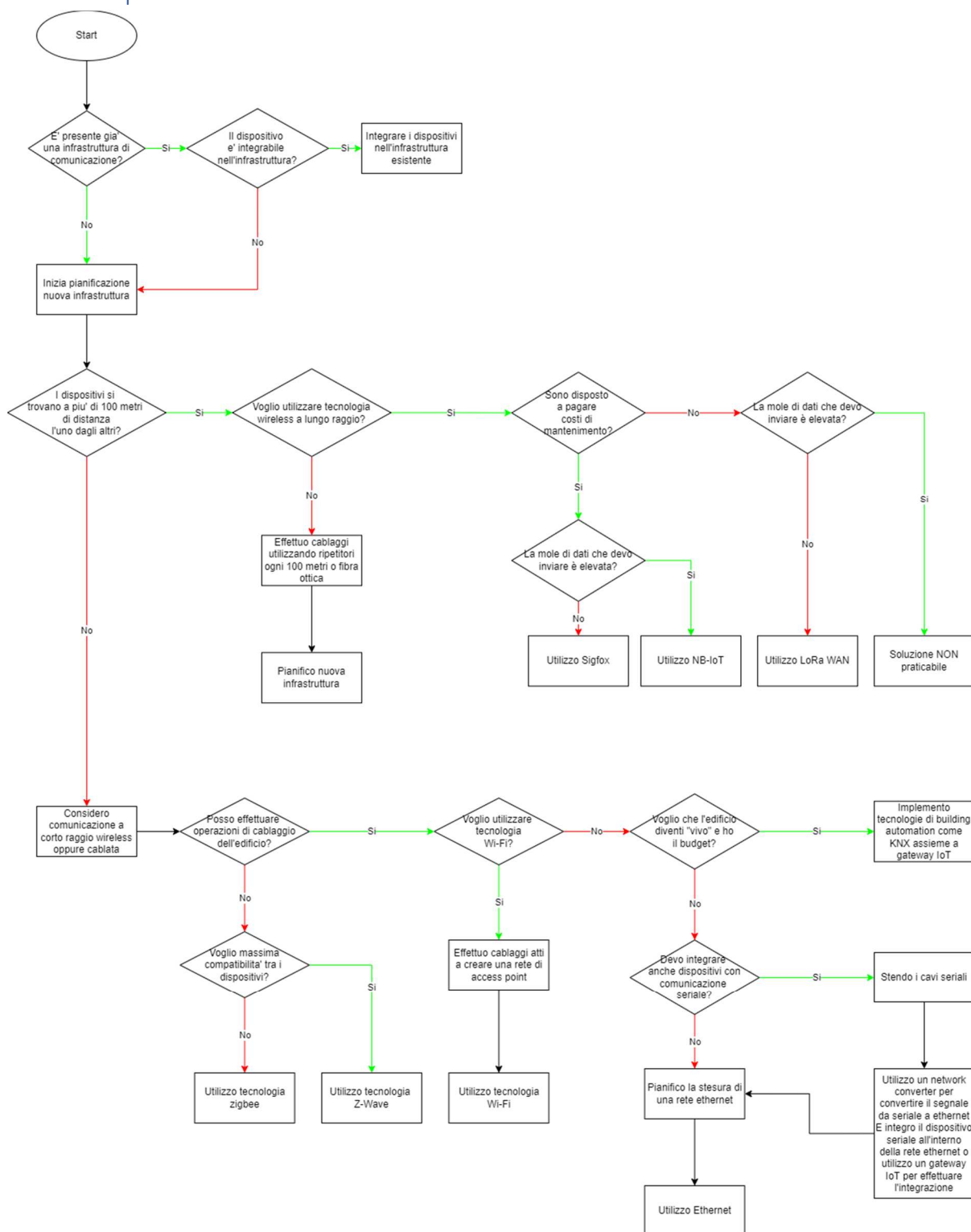
Infrastruttura fisica e configurazione

Questo tipo di spazio è caratterizzato dal fatto di avere una ampia superficie da monitorare, essere outdoor e non avere infrastrutture IT presenti.

Secondo quanto citato prima, la soluzione ottimale per creare l'infrastruttura fisica in questa zona è l'impiego di tecnologie wireless a lungo raggio (NB-IoT, LoRa WAN, Sigfox e rete cellulare) per effettuare l'invio dei dati.

I dispositivi e sensori dovranno essere almeno IP44 al fine di prolungare la vita dei medesimi.

Flowchart per la selezione dell'infrastruttura fisica



Protocolli di comunicazione impiegati

Finora abbiamo visto l'infrastruttura dal punto di vista fisico ovvero la realizzazione materiale dell'infrastruttura. I protocolli di comunicazione sono un insieme di regole che permettono a due sistemi di comunicare e scambiare informazioni.

Questi protocolli sono indipendenti dalla realizzazione dell'infrastruttura fisica in quanto essi sono trasportati da questa infrastruttura, può essere quindi che troviamo mezzi di trasmissione diversi quali ad esempio la rete cablata e il wi-fi che però sono in grado di supportare e trasmettere dati utilizzando gli stessi protocolli di comunicazione.

I protocolli di comunicazione sono una parte fondamentale dell'infrastruttura IoT in quanto determinano come le informazioni e quindi i dati sono trasmessi e codificati.

A scopo di chiarimento qui di seguito sono spiegati brevemente i principali protocolli di comunicazione che verranno utilizzati nell'infrastruttura.

MQTT

Il protocollo MQTT (Message Queue Telemetry Transport) è lo standard di comunicazione dati dal field layer verso il Cloud; quasi tutti i provider Cloud supportano questo protocollo di comunicazione.

Compito principale dei gateway IoT sarà tradurre infatti i dati in arrivo dal field layer a questo protocollo di comunicazione e inviare poi i dati in Cloud.

Questo protocollo è progettato per essere leggero e utilizza poca banda di trasmissione.

La caratteristica principale di MQTT è di funzionare con un paradigma publish/subscribe, i dati infatti sono scritti in un argomento (o topic). Il client si iscrive all'argomento e quando un nuovo dato arriva una notifica viene inviata al client che a quel punto va a leggere i nuovi dati in arrivo.

Il protocollo ha inoltre dei meccanismi di sicurezza integrati quali la trasmissione crittografata utilizzando TLS e dei sistemi di autenticazione che limitano l'accesso ai dati ai dispositivi autorizzati.

La comunicazione con questo tipo di protocollo può essere bidirezionale permettendo così non solo la lettura ma anche la scrittura di dati, consentendo anche la comunicazione tra dispositivi tramite un broker intermedio.

MQTT incorpora inoltre un sistema di qualità del servizio (QoS) che rende il sistema di trasmissione robusto, garantendo la consegna dei messaggi e correzione degli errori.

Riassumendo i principali vantaggi di MQTT come protocollo di comunicazione sono:

- Può trasportare qualsiasi tipo di dato, come ad esempio dati di tipo binario o ASCII
- La dimensione dei pacchetti è contenuta il che fa sì che la banda occupata sia molto limitata
- Si può utilizzare in dispositivi con risorse molto limitate quali ad esempio dispositivi a batteria o con poca potenza di calcolo
- La QoS garantisce la trasmissione del messaggio
- È scalabile in quanto si utilizza una architettura publish/subscribe
- In caso di connessione non affidabile visto che i pacchetti sono di dimensioni contenute la trasmissione è facilitata
- Il protocollo è asincrono il che fa sì che i dati siano generati solo in casi specifici come ad esempio un evento
- Sicurezza integrata nativamente

Le controindicazioni sono invece:

- Latenza in quanto utilizza TCP come trasporto
- Non è possibile inviare proprietà nel messaggio utilizzando ad esempio un header
- La scalabilità del sistema è limitata dalle capacità del broker, il quale è anche il punto critico del sistema, se infatti il broker non funziona, smette di funzionare anche tutto il resto (single point of failure)
- L'implementazione di sistemi che utilizzano MQTT risulta elaborata in quanto la gestione del dato e del protocollo devono essere sviluppati ad-hoc per il sistema
- Mancanza di un meccanismo di discovery tra i dispositivi
- Nonostante possa trasportare qualsiasi tipo di payload, la dimensione massima di esso è limitata

AMQP

Un altro protocollo ampiamente accettato nel cloud è AMPQ (Advanced Message Queuing Protocol). Questo protocollo necessita per forza di un broker che agirà anche da middleware a cui arrivano i messaggi: questi sono salvati in una coda.

I messaggi sono pubblicati da un dispositivo (publisher), aggiunti alla coda a cui si sottoscrive il destinatario. Il messaggio si compone di più campi i cui principali sono:

- Broker destinatario
- Routing key
- Argomento (topic)
- Messaggio (Payload)

Il broker ha il compito di assicurare la ricezione del messaggio.

Questo protocollo presenta più sistemi di distribuzione in particolare:

1. Publish/subscribe: uno o più client si collegano al broker e sottoscrivono un argomento, il routing è fatto utilizzando un campo chiamato “Binding Key” che deve corrispondere alla “Routing Key” del messaggio, il messaggio viene copiato e inviato a tutti i client che hanno una sottoscrizione valida
2. Lavoro distribuito: simile al modello publish/subscribe si differenzia nel fatto che i sottoscrittori non ricevono una copia del messaggio ma utilizzano il messaggio originale potendolo così modificare

AMQP implementa un sistema di notifica della lettura e consegna dei messaggi.

La sicurezza della comunicazione è garantita a livello di trasporto mediante TLS per crittografia dei dati e presenta inoltre un layer di autenticazione di tipo SASL (Simple Authentication Security Layer).

Rispetto a MQTT questo protocollo utilizza più banda, determinando un maggior uso di risorse rispetto a MQTT e quindi più costi.

AMQP inoltre ha meno dispositivi che lo supportano nativamente rispetto a MQTT per cui si rendono necessari hardware e software aggiuntivi.

I principali vantaggi di questo protocollo sono:

- Utilizzo del QoS che garantisce la consegna del messaggio
- Interoperabilità del protocollo in quanto i dati sono inviati come stream di byte
- Sicurezza integrata nativamente su più livelli, TLS e autenticazione in particolare
- Implementazione facilitata rispetto a MQTT
- Supporto di più architetture di distribuzione

- Il protocollo è orientato verso i servizi

Di contro abbiamo però:

- Utilizzo di banda maggiore rispetto a MQTT dovuto a dimensione dei pacchetti più grande
- Mancanza di retrocompatibilità tra versioni
- Mancanza di un meccanismo di discovery dei dispositivi
- Necessita di più risorse di calcolo per poter funzionare rispetto a MQTT

OpcUA

OpcUA è uno standard di comunicazione industriale con architettura unificata open source e cross platform il cui scopo è mettere in comunicazione macchinari tra di loro.

La caratteristica principale di OpcUA è quella di avere un sistema integrato di modellazione delle informazioni standardizzato; ciascuna informazione è contenuta all'interno di un nodo.

Ciascun nodo ha un ID che lo caratterizza e che deve essere univoco.

OpcUA ha una architettura server-client che incorpora le seguenti funzionalità:

- DA Server: questo server effettua una validazione del dato nativamente determinando tempo, valori e qualità del dato stesso,
- Alarm Exchange Server: questo tipo di server definisce degli allarmi e i messaggi di allarme che poi vengono inviati tramite un sistema di notifica. Le variabili che attivano l'allarme possono essere associate a stati ed eventi,
- HDA (Historic Data) server: questo server viene utilizzato per effettuare analisi del macchinario in quanto effettua il salvataggio tramite dei dati al fine di analizzarli a posteriori.

Il server OpcUA raccoglie i dati provenienti dai sensori, attuatori e tutti i componenti di una macchina (o di un sistema) o anche un OpcClient e li rende disponibili ad altri dispositivi Opc utilizzando il protocollo di comunicazione OpcUA.

Questo protocollo è molto scalabile e può essere utilizzato sia nella rete locale che tramite Internet.

A livello di sicurezza implementa crittografia TLS, un sistema di autenticazione e di permessi di accesso ai dati e si possono inoltre utilizzare certificati custom per garantire l'accesso al sistema.

I principali vantaggi di OpcUA sono pertanto:

- È uno standard industriale de facto, supportato da tutti i big player del settore
- Decentralizzazione dell'infrastruttura di scambio dati
- Elevata scalabilità di architettura e di trasmissione
- Meccanismo di discovery dei dispositivi integrato
- Sicurezza integrata a più livelli
- Elevata interoperabilità del protocollo
- Possibilità di effettuare modellazione di oggetti avanzati
- Il protocollo è indipendente dal mezzo di trasporto

Gli svantaggi sono invece:

- Alcuni dispositivi possono non seguire la struttura open del protocollo implementando la propria specifica
- La trasmissione dei dati verso il cloud presenta maggiori difficoltà
- Il protocollo è molto complicato in quanto ha molti feature
- La messa in opera di dispositivi con OpcUA è complicata

Modbus

Questo protocollo di comunicazione è uno dei più usati in ambito industriale in quanto facile da implementare, senza costi di licenza; è uno standard consolidato e robusto che può vantare il fatto di poter essere trasmesso utilizzando più infrastrutture fisiche.

Modbus può comunicare utilizzando diverse infrastrutture fisiche quali cavi seriali, in particolare RS232 e RS485, cavi Ethernet e anche tecnologia Wi-Fi.

Il paradigma di comunicazione di questo protocollo è master/slave nel caso di trasmissione seriale oppure server/client nel caso di trasmissione tramite Ethernet o Wi-Fi.

Il protocollo presenta solo quattro tipi di oggetto chiamati registri:

- Bobina (Coil): usato per attivare/disattivare relè, questo tipo di oggetto può essere letto e scritto,
- Input discreto: oggetto in sola lettura il cui valore può essere solo 0 o 1,
- Input registro: oggetto in sola lettura il cui valore può essere rappresentato usando 16 bit, generalmente utilizzato per leggere dati da sensori,
- Registro holding: oggetto con capacità di lettura e scrittura a 16 bit.

Ciascun tipo oggetto ha un indirizzo unico e uno spazio indirizzi riservato. Il protocollo prevede diversi sistemi di verifica di integrità del dato quale ad esempio CRC (Cyclic Redundant Check).

Il protocollo può essere categorizzato in base al mezzo di trasmissione in:

- Modbus RTU (Remote Terminal Unit): questa è la versione più comune di questo protocollo, utilizza la comunicazione seriale i cui dati sono rappresentati in maniera binaria; il dato è validato utilizzando la verifica CRC. I dati sono trasmessi di continuo sulla linea seriale e separati da periodi di silenzio (IDLE) determinati dal baud rate,
- Modbus ASCII: simile alla versione precedente solo che i dati vengono rappresentati utilizzando caratteri ASCII; la verifica è leggermente diversa ed utilizza il sistema LRC (Longitudinal Redundancy Check) per validare i dati. Anche in questo caso i dati sono inviati in maniera continua sulla linea seriale; i messaggi iniziano con il simbolo “:” e terminano con i caratteri speciali “CR+LF”,
- Modbus TCP/IP: detto anche Modbus RTU/IP, questa versione utilizza come mezzo di trasporto cavi Ethernet o il Wi-Fi,
- Modbus UDP: utilizza UDP al posto di TCP come pacchetto di trasporto, così facendo utilizza meno banda in quanto l’handshaking e tutti i controlli e meccanismi aggiuntivi di TCP non sono presenti.

Questo protocollo presenta utilizzo di banda molto basso e grazie al fatto che i dati sono trasmessi di continuo è un protocollo perfetto per il controllo di dispositivi in tempo reale.

Modbus non presenta meccanismi di sicurezza integrati all’interno del protocollo per cui per motivi di sicurezza questo protocollo viene utilizzato solo in locale ed è bene non esporlo pubblicamente ma utilizzare un gateway dedicato per inviare i dati Modbus nel Cloud.

I principali vantaggi di modbus sono quindi:

- indipendenza del mezzo di trasporto
- estremamente facile da implementare e mantenere
- standard industriale de-facto utilizzato da tutti i big player del settore
- integrazione di dispositivi immediata
- comunicazione stabile e garantita
- interoperabilità elevata
- elevato numero di convertitori di segnali disponibili sul mercato

Gli svantaggi sono invece:

- La specifica è molto vecchia e non è stata aggiornata per scenari moderni
- La scalabilità è limitata a causa del tipo di architettura master/slave
- I dati vengono classificati in registri e bobine (coil)
- Numero massimo di dispositivi monitorati limitato a 247
- Sicurezza non presente nel protocollo a nessun livello

LonWorks

Il protocollo è utilizzato principalmente in ambito di building e home automation, industrial automation, ambito trasporti, controllo luminarie, controllo HVAC e utility control network.

La particolarità di questo protocollo è che per funzionare necessita di hardware dedicato, in particolare di un processore chiamato neuron realizzato dalla Echelon corporation la quale è stata acquisita del gruppo Renesas per cui le proprietà intellettuali ora fanno parte di questo gruppo.

LonWorks utilizza un paradigma di comunicazione peer to peer, i dati possono quindi essere scambiati tra tutti i dispositivi della rete ed essere anche ritrasmessi da un dispositivo all'altro.

La comunicazione avviene attraverso canali; i pacchetti sono di grandezza variabile e contengono informazioni per il layer applicativo del dispositivo e l'indirizzo del dispositivo.

Quando il dispositivo riceve un messaggio effettua un controllo e, se l'indirizzo corrisponde con il proprio, il dato viene utilizzato dall'applicazione del dispositivo altrimenti il messaggio viene scartato.

Il processo con cui si collegano i dispositivi utilizzando LonWorks è chiamato “Binding”; in questo processo vengono informati i dispositivi sulla destinazione verso cui devono trasmettere e quale tipo di dato trasmettere.

Il protocollo supporta due tipi di oggetti:

- Variabili di rete (Network Variables): rappresentate da 200 tipi di dati, ciascun tipo di dato viene utilizzato per un uso standardizzato (esempio: lettura valore di temperatura, lettura valore di tensione, valore di pressione ecc...), questo per assicurare la compatibilità tra diversi dispositivi di diversi produttori per cui un valore di tensione sarà uguale in qualsiasi dispositivo indipendentemente dal produttore,
- Messaggi espliciti: questo tipo di oggetto contiene fino a 229 byte creati in maniera custom dal programmatore del sistema.

LonWorks espande in maniera sostanziale le capacità di comunicazione di dati rispetto a Modbus in quanto i tipi di dato sono espansi e ottimizzati per ciascun tipo di grandezza; Modbus può essere infatti

nativamente incorporato all'interno di LonWorks e i suoi 4 tipi di oggetto non sono altro che 4 tipi di dato all'interno di una rete LonWorks.

I messaggi all'interno di LonWorks sono tipicamente cambi di stato variabili di rete al fine di informare i dispositivi che compongono il sistema del cambio di stato ed effettuare le appropriate azioni.

A livello di sicurezza questo protocollo non implementa nessuna crittografia dei dati, ma solo una autenticazione a 48 bit tramite security key, che lo rende inadatto alla trasmissione nella rete pubblica: un gateway IoT si rende necessario per effettuare la raccolta dati e l'invio di essi in Cloud.

I principali vantaggi di questo protocollo sono:

- Topologia molto flessibile
- Messa in opera dei dispositivi semplice, quasi a livello di "plug & play"
- Il sistema di controllo si presenta come una soluzione unificata
- Semplificazione a livello hardware dei dispositivi

Gli svantaggi sono invece:

- Utilizzo di hardware proprietario in particolare il chip neuron
- Il protocollo non è completamente aperto al pubblico

BacNET

Il protocollo BacNET viene utilizzato in ambito Building Automation e Control NETWORK.

Lo scopo principale è permettere l'interoperabilità di dispositivi di controllo e monitoraggio di edifici e di comunicare e scambiare informazioni al fine di avere un controllo integrato di tutti i sistemi tramite un sistema di controllo centralizzato.

La specifica si compone di tre parti principali:

1. Oggetti: rappresentano in maniera standardizzata gli equipaggiamenti dell'edificio e i dispositivi di campo,
2. Servizi: contengono dei metodi per creare messaggi standardizzati che vengono poi inviati nella rete per monitorare e controllare i vari dispositivi e creare così l'automazione (i tipi di servizi sono 32 in totale),
3. LAN e Inter-Networking: definisce il mezzo fisico di trasmissione e i parametri fisici e di trasmissione di essi.

Gli oggetti sono l'unità di collezione delle informazioni: ciascun oggetto è identificato in maniera univoca e l'accesso ad essi è consentito tramite la rete BACNet in maniera standardizzata. Esempi di standardizzazione sono: input fisici, output fisici e processi software quali loop, allarmi, calcoli. In totale BACNet ha 60 tipi di oggetti standardizzati ciascuno con proprietà e metodi di accesso definiti (3 proprietà sono sempre necessarie e sono: identificativo dell'oggetto, nome dell'oggetto e tipo dell'oggetto).

Gli oggetti comunicano tra di loro tramite una serie di servizi che inviano richieste ad un oggetto, il quale risponde con pacchetti dati.

I servizi BacNet si occupano della creazione e risposta alle varie richieste ed il processamento di esse in totale ci sono 32 servizi che possono essere suddivisi in 5 tipi:

- Servizi di accesso agli oggetti,
- Servizi di allarme ed eventi,
- Servizi di accesso ai file,

- Servizi di accesso remote,
- Servizio di terminale virtuale.

I servizi possono inoltre avere oppure no un servizio di conferma; a livello di architettura sono presenti, inoltre, servizi quali:

- "Who-Is" e "I-am" per effettuare la scoperta dei vari dispositivi della rete,
- "Who-Has" e "I-Have" per identificare i servizi presenti su ciascun dispositivo.

BacNET può essere trasmesso e utilizzato con i seguenti mezzi di trasmissione:

- Ethernet e/o WiFi
- ArcNET
- RS-485 e RS232
- LonWorks

Il mezzo di trasmissione che offre le caratteristiche migliori è l'Ethernet ed è anche il più utilizzato.

L'opzione RS-485 è invece quella che offre la maggior lunghezza di trasmissione, si può arrivare fino a circa 1.2km.

Come evidenziato il protocollo BacNET è integrato anche su reti LonWorks tramite il chip neuron.

La sicurezza in BacNET viene implementata utilizzando VLAN, Firewall e VPN.

Recentemente (gennaio 2022) è stata introdotta una nuova funzionalità del protocollo che implementa la crittografia dei dati nativamente sia nella comunicazione tra dispositivi che verso l'esterno: questa nuova feature si chiama BacNET/SC dove SC sta per Secure Connection, nuovi dispositivi con questa feature saranno disponibili a breve nel mercato.

È stato inoltre annunciato che funzionalità aggiuntive quali l'autenticazione saranno a breve incorporate all'interno del protocollo nativamente.

I principali vantaggi di BacNet sono:

- Indipendenza dal mezzo di trasporto
- Elevata scalabilità
- Standard open
- Internetworking robusto
- Protocollo nato e sviluppato specificatamente per building automation

Gli svantaggi sono invece:

- Sicurezza non implementata a livello di protocollo (anche se una soluzione è in arrivo)
- Richiede più risorse di storage e memoria rispetto gli altri protocolli
- Individuare i problemi all'interno di una rete BacNET è leggermente più complicato rispetto gli altri protocolli

Profibus e ProfiNET

Sono protocolli di comunicazione industriali utilizzati in reti controllo.

Profibus utilizza un bus di comunicazione per la trasmissione dei dati: questo bus è tipicamente realizzato usando cavi RS232 o RS485 in daisy chain. Ciascun dispositivo ha un indirizzo unico da 1 fino a 127 il che significa che una rete Profibus può avere fino a 127 dispositivi.

ProfiNET utilizza invece Ethernet come mezzo di trasmissione: in questo caso il dispositivo è caratterizzato da indirizzo IP, indirizzo MAC e nome del dispositivo.

Tra i due protocolli quello che sta avendo maggior adozione è profiNET in quanto l'utilizzo dell'ethernet permette di effettuare operazioni avanzate quali il routing dei segnali/messaggi.

Lo scopo principale di questo protocollo è garantire una comunicazione e conferma di ricezione dei messaggi con latenze molto basse; infatti, a seconda dell'operazione che si va ad eseguire le latenze possono essere anche inferiori ad 1ms.

Per effettuare la configurazione dei dispositivi questo protocollo utilizza gli standard TCP/IP e UDP/IP; tuttavia, per le azioni in cui il tempo è un fattore critico si utilizza un'altra tecnica chiamata real time framing. Questa tecnica fa sì che alcuni passaggi del modello ISO/OSI vengano saltati andando a comunicare direttamente con il destinatario a livello applicativo rendendo così la trasmissione in tempo reale, ottenendo latenze di circa 250 microsecondi; non è richiesto nessun hardware speciale per ottenere questo tipo di performance.

Ulteriori protocolli speciali sono disponibili, tutti creati con lo scopo di avere una latenza molto bassa ed avere così una comunicazione quanto più vicina al tempo reale.

Una tipica configurazione include: un controller, dei dispositivi e l'infrastruttura di trasmissione del segnale.

A livello di sicurezza il protocollo implementa delle classi di sicurezza a seconda del tipo di ambiente e dispositivo:

- Classe 1: separa i dispositivi di campo limitando la comunicazione tra dispositivi
- Classe 2: più sistemi e dispositivi implementano un sistema di autenticazione e verifica dell'integrità dei messaggi
- Classe 3: lo scambio di informazioni viene criptato e l'accesso consentito solo tramite certificati e chiavi specifiche, i dati sui controller vengono a loro volta crittografati.

Vista la particolarità di questo protocollo l'integrazione con il Cloud non è consigliata né possibile in maniera semplice, per questo un gateway IoT si rende necessario.

I principali vantaggi sono:

- Big player supportano il protocollo
- Scalabilità e facilità d'uso elevati
- Elevate performance e basso consumo di energia
- Sicurezza implementata nativamente e a più strati

Gli svantaggi sono:

- Difficoltà di portare i dati nel cloud
- Portare i dati nel cloud fa sì che i vantaggi di velocità di trasmissione vengano persi
- Il protocollo è in parte open ed è mantenuto in maniera closed-source