



[Domotica filare e wireless: da sistemi antagonisti ad ibridi]

Sistema
Domotico su
piattaforma
Arduino



AUTORE: ANDREA LANDO

REVISIONE 1.0.0

DATA ULTIMA REVISIONE: 09.05.2026

Sommario

Prefazione	5
Domotica filare vs wireless	6
Principi generali: Filare vs Wireless	6
Comparazione per tipologia di dispositivo	6
Rischi specifici del wireless (riassunto).....	8
Rischi specifici del filare (riassunto).....	9
Conclusione sintetica.....	9
Matrice unificata (wireless / filare), Rischio–Impatto	10
Matrice per tipologia, Rischio–Impatto	12
📶 Wireless.....	12
🔌 Filare.....	12
Raccomandazioni per la progettazione di un impianto ibrido	13
Telecamere – Preferibile Filare (PoE)	13
Serrature Smart – Filare con Backup BLE	14
Sensori di Allarme Critici (Gas, Fumo, Allagamento) – Filare	14
Sensori Ambientali Non Critici – Wireless (Zigbee/Thread)	14
Illuminazione – Filare.....	14
Prese e Attuatori Principali – Filare	14
Termostati e HVAC – Filare.....	14
Citofoni e Videocitofoni – Filare PoE con protocolli H.264/H.265	15
Motivazioni tecniche principali.....	15
Perché evitare soluzioni wireless.....	15
Assistenti Vocali – Wireless o Ethernet	16
Elettrodomestici Smart – Wireless	16
Gateway Domotici – Ethernet	16
Impianto Ibrido: la Soluzione Ottimale.....	16
Linee guida spicciole	16
Conclusione	17
Prontuario del progettista e dell’installatore	18
Premessa e Avvertenze	18
Introduzione alla Domotica Moderna	18
Filosofie Progettuali: Filare vs Wireless.....	18
Domotica Filare.....	18
Domotica Wireless.....	18
Principi Generali di Progettazione	19
Architettura a Livelli.....	19

Scelta dei Mezzi di Comunicazione.....	19
Preferenza per i Bus di Campo Filari (Modbus)	20
Normative Tecniche di Riferimento.....	20
Progettazione della Rete IP	20
Sicurezza Informatica Applicata alla Domotica	21
Continuità Operativa e UPS	21
Manutenzione Programmata	21
Scenari Applicativi Reali.....	22
Criteri di Scelta dei Protocolli	22
Criteri di Scelta dei Cavi	22
Raccomandazioni per Tipologia di Dispositivo	23
Conclusioni.....	23
Disclaimer Legale – Limitazione di Responsabilità	24

Prefazione

La domotica moderna si trova oggi al centro di una trasformazione profonda, in cui convivono due filosofie progettuali molto diverse: la **domotica filare**, erede diretta dell'automazione industriale, e la **domotica wireless**, nata per rispondere alle esigenze di flessibilità, rapidità di installazione e accessibilità del mercato consumer. Entrambe le soluzioni hanno raggiunto un livello di maturità significativo, ma presentano caratteristiche, vantaggi e limiti profondamente differenti. Comprendere queste differenze è essenziale per progettare impianti affidabili, sicuri e sostenibili nel tempo.

La comparazione tra filare e wireless non è un esercizio teorico: è un passaggio fondamentale per chiunque debba progettare o valutare un impianto domotico, sia esso destinato a un'abitazione privata, a un edificio complesso, a una struttura ricettiva o a un ambiente di lavoro. Le scelte fatte in fase progettuale influenzano direttamente la continuità di servizio, la qualità dell'esperienza utente, la manutenzione futura, la sicurezza operativa e persino il benessere delle persone che vivono o lavorano negli ambienti controllati dal sistema.

La **domotica filare** si basa su protocolli cablati come Modbus, KNX, RS485 e altre tecnologie industriali. Questi sistemi sono progettati per garantire stabilità, determinismo e continuità operativa anche in condizioni avverse. La loro affidabilità deriva da un'architettura semplice, priva di interferenze radio, con comunicazioni robuste e prevedibili. Non è un caso che la filare sia la scelta preferita negli impianti professionali, dove la continuità del servizio non è un optional ma un requisito imprescindibile. Tuttavia, la filare richiede una progettazione accurata, cablaggi dedicati, terminazioni corrette e competenze tecniche elevate, elementi che possono aumentare la complessità e i costi iniziali.

La **domotica wireless**, al contrario, si è affermata grazie alla sua flessibilità, alla facilità di installazione e alla capacità di integrare rapidamente un'ampia gamma di dispositivi. Protocolli come Zigbee, Thread, Z-Wave, Wi-Fi e BLE hanno reso possibile la creazione di reti mesh dinamiche, adattabili e ricche di funzionalità. Questa filosofia ha permesso alla domotica di entrare nelle case di milioni di persone, democratizzando l'accesso a tecnologie avanzate. Tuttavia, la natura stessa delle comunicazioni radio introduce variabili difficili da controllare: interferenze, saturazione dello spettro, distanze, ostacoli fisici, qualità dei gateway e dipendenza dall'alimentazione dei nodi. Questi fattori possono influire sulla stabilità dell'impianto, soprattutto in contesti complessi o ad alta densità di dispositivi.

La comparazione tra filare e wireless non deve essere interpretata come una contrapposizione assoluta, ma come un'analisi delle caratteristiche intrinseche di ciascun approccio. In molti casi, la soluzione migliore è un'architettura ibrida, in cui la filare gestisce le logiche critiche (HVAC, sicurezza, automazioni primarie) mentre il wireless viene utilizzato per sensori non critici, dispositivi mobili o funzioni di comfort. La scelta dipende dal contesto, dal livello di affidabilità richiesto, dal budget, dalla complessità dell'edificio e dalle competenze disponibili.

Un ulteriore elemento che rende questa comparazione particolarmente attuale riguarda il tema della **salute e del benessere negli ambienti interni**. Sebbene gli studi sugli effetti a lungo termine delle emissioni RF siano ancora in corso e non esistano conclusioni definitive, è ragionevole adottare un approccio prudentiale, soprattutto negli ambienti in cui si trascorre la maggior parte del tempo. La domotica filare, priva di emissioni radio, offre un vantaggio intrinseco in questo senso, mentre la domotica wireless richiede una progettazione attenta per evitare sovrapposizioni di segnali, gateway ridondanti o reti mesh eccessivamente dense.

Questa introduzione prepara il lettore a una comparazione dettagliata che analizzerà in modo oggettivo i punti di forza e i limiti di entrambe le tecnologie, considerando aspetti come affidabilità, continuità di servizio, scalabilità, manutenzione, costi, impatto RF, sicurezza, complessità di installazione e ruolo ideale all'interno dell'impianto. L'obiettivo non è decretare un vincitore assoluto, ma fornire gli strumenti necessari per scegliere consapevolmente la soluzione più adatta alle esigenze specifiche del progetto.

Domotica filare vs wireless

suddivisa per tipologia di dispositivo, con **i rischi specifici** per ciascuna tecnologia. L'obiettivo è darti una vista **pratica e ingegneristica**, non ideologica: cosa cambia davvero tra filare e wireless in termini di **affidabilità, sicurezza, privacy, salute e continuità operativa**.

Principi generali: Filare vs Wireless

Domotica filare

- Comunicazione tramite cavo (Ethernet, BUS proprietari, KNX, Modbus, RS485, ecc.)
- Alimentazione e dati spesso sullo stesso cavo
- Richiede infrastruttura fisica

Punti di forza: stabilità, sicurezza, immunità ai disturbi, nessuna emissione RF, privacy elevata **Rischi:** guasti fisici ai cavi, costi di installazione, scarsa flessibilità post-installazione

Domotica wireless

- Comunicazione tramite radiofrequenza (Wi-Fi, Zigbee, Z-Wave, BLE, Thread, 433/868 MHz)
- Installazione semplice, dispositivi economici

Punti di forza: flessibilità, retrofit, costi bassi **Rischi:** interferenze, attacchi RF, privacy, dipendenza dal cloud, esposizione RF (bassa ma presente)

Comparazione per tipologia di dispositivo



A. Sensori (temperatura, movimento, porte/finestre, qualità aria)

Tecnologia	Rischi principali
Wireless (Zigbee, Z-Wave, BLE, Wi-Fi)	- Interferenze RF → perdita pacchetti - Batteria → rischio mancata rilevazione - Possibili attacchi RF (replay, jamming) - Privacy: dati ambientali inviati al cloud - Esposizione RF minima ma presente
Filare (BUS, RS485, KNX)	- Guasto fisico al cavo - Installazione complessa - Nessun rischio RF - Sicurezza elevata (linea chiusa) - Privacy molto alta

Vantaggio netto: Filare, soprattutto per sensori critici (allarmi, allagamento, gas).



B. Serrature smart

Tecnologia	Rischi principali
Wireless (BLE, Wi-Fi, Zigbee)	- Attacchi MITM, replay, spoofing - Jamming RF → impossibilità di aprire - Dipendenza da cloud/app

Tecnologia	Rischi principali
	- Batteria → rischio blocco - Privacy: log accessi inviati online
Filare (BUS, PoE)	- Richiede cablaggio dedicato - Rischio guasto cavo - Sicurezza molto più alta - Nessuna esposizione RF - Nessuna dipendenza dal cloud

Vantaggio netto: Filare, per motivi di sicurezza fisica.

C. Telecamere

Tecnologia	Rischi principali
Wireless (Wi-Fi)	- Attacchi Wi-Fi - Interferenze → perdita video - Privacy: flussi video nel cloud - Esposizione RF moderata (trasmissione continua)
Filare (Ethernet/PoE)	- Richiede cablaggio - Sicurezza molto più elevata - Nessuna interferenza - Nessuna emissione RF - Privacy: flussi locali, non cloud

Vantaggio netto: Filare, senza discussione.

D. Assistenti vocali / Smart speaker

Tecnologia	Rischi principali
Wireless (Wi-Fi + BLE)	- Registrazioni involontarie - Dipendenza totale dal cloud - Profilazione dati - Esposizione RF bassa-media
Filare (Ethernet)	- Riduce attacchi Wi-Fi - Riduce interferenze - Privacy comunque limitata (microfoni sempre attivi)

Vantaggio netto: Filare, ma il rischio principale non è RF: è **la privacy**.

E. Illuminazione smart

Tecnologia	Rischi principali
Wireless (Zigbee, BLE, Wi-Fi)	- Interferenze → ritardi o mancata accensione - Attacchi RF (limitati ma possibili) - Esposizione RF molto bassa

Tecnologia	Rischi principali
Filare (BUS, DALI, KNX)	- Installazione complessa - Affidabilità totale - Nessuna emissione RF

Vantaggio netto: Filare, soprattutto in impianti professionali.

F. Prese smart e attuatori

Tecnologia Rischi principali

	- Interferenze
Wireless	- Possibili attacchi (accensione/spegnimento remoto) - Privacy: dati consumi inviati al cloud
Filare	- Richiede cablaggio - Sicurezza e affidabilità molto superiori

Vantaggio netto: Filare.

G. Termostati e climatizzazione

Tecnologia Rischi principali

	- Interferenze → mancata regolazione
Wireless	- Privacy: dati presenza/abitudini - Attacchi → manipolazione temperatura
Filare	- Richiede cavo - Affidabilità molto maggiore - Nessun rischio RF

Vantaggio netto: Filare, soprattutto in case con impianti complessi.

Rischi specifici del wireless (riassunto)

A. Sicurezza informatica

- Attacchi RF (jamming, replay, spoofing)
- Attacchi Wi-Fi
- Dipendenza da cloud e app

B. Affidabilità

- Interferenze (2.4 GHz molto affollato)
- Perdita pacchetti
- Batteria nei sensori

C. Privacy

- Molti dispositivi inviano dati ai server del produttore
- Telemetria continua

D. Salute

- Emissioni RF **basse**, ma presenti
- Nessuna evidenza di danni certi sotto i limiti, ma alcuni studi suggeriscono possibili effetti non termici → prudenza sensata

Rischi specifici del filare (riassunto)

A. Guasti fisici

- Rottura cavi
- Connettori difettosi

B. Costi e complessità

- Installazione più onerosa
- Richiede progettazione

C. Flessibilità

- Meno adattabile dopo la posa

Conclusione sintetica

Per sicurezza, privacy e affidabilità: vince il FILARE.

Per flessibilità, retrofit e costi: vince il WIRELESS.

La scelta migliore spesso è **ibrida**:

- **filare** per ciò che è critico (allarmi, serrature, telecamere, attuatori principali)
- **wireless** per ciò che è accessorio (sensori non critici, automazioni leggere)

Matrice unificata (wireless / filare), Rischio–Impatto

La tabella seguente confronta in modo sintetico ma tecnico i principali **rischi**, **impatti operativi** e le **motivazioni ingegneristiche** che distinguono le soluzioni **wireless** da quelle **filari** nei sistemi domotici e di automazione. Ogni riga analizza una categoria critica — dalla sicurezza alla continuità di servizio — evidenziando come le due tecnologie si comportano in scenari reali, quali vulnerabilità presentano e quali conseguenze possono generare in caso di guasto o compromissione. L'obiettivo è offrire una valutazione immediata, utile sia per la progettazione sia per la scelta dell'infrastruttura più adatta al contesto.

Categoria	Rischio – Wireless	Rischio – Filare	Impatto – Wireless	Impatto – Filare	Spiegazione tecnica (per riga)
Interferenze / Stabilità	Alto	Molto basso	Medio–Alto	Alto	Wireless: congestione 2.4 GHz, muri, disturbi RF → perdita pacchetti. Filare: quasi immune alle interferenze; se il cavo si danneggia l'impatto è alto perché il dispositivo diventa irraggiungibile.
Sicurezza informatica	Alto	Basso	Alto	Alto	Wireless: attacchi Wi-Fi, spoofing, replay, jamming. Filare: linea chiusa molto più difficile da attaccare; se compromessa, l'impatto è comunque elevato perché coinvolge l'intero bus.
Privacy	Alto	Molto basso	Alto	Alto	Wireless: molti dispositivi inviano dati al cloud; rischio di tracciamento e leak. Filare: dati locali, privacy intrinseca; se violata, l'impatto resta alto perché riguarda dati sensibili.
Affidabilità operativa	Medio	Molto basso	Alto	Alto	Wireless: batterie, interferenze, latenza → rischio di mancata attuazione. Filare: protocolli deterministici (KNX, Modbus) → affidabilità quasi totale; se fallisce, impatto elevato.
Continuità di servizio	Medio	Molto basso	Alto	Alto	Wireless: dipende da Wi-Fi, router, gateway, cloud. Filare: funziona anche senza rete o internet; se un bus cade, impatto elevato.
Manutenzione	Medio	Basso	Medio	Medio	Wireless: batterie da sostituire, aggiornamenti firmware frequenti. Filare: manutenzione minima, ma eventuali interventi su cavi sono più invasivi.
Salute (RF)	Basso	Nessuno	Basso	Nessuno	Wireless: emissioni RF basse ma presenti; nessuna evidenza di danni certi sotto i limiti. Filare: zero emissioni.

Costo installazione	Basso	Alto	Medio	Medio	Wireless: installazione semplice, retrofit immediato. Filare: richiede canaline, cavi, manodopera specializzata.
Flessibilità / Scalabilità	Alto	Basso	Medio	Medio	Wireless: aggiunta dispositivi immediata. Filare: modifiche post-posa complesse e costose.

- **Wireless** → più rischi, impatti elevati, ma flessibile ed economico.
- **Filare** → rischi minimi, impatti elevati solo in caso di guasto fisico (raro).
- **Conclusione tecnica:**
 - **Filare per tutto ciò che è critico** (sicurezza, accessi, video, attuatori).
 - **Wireless per ciò che è accessorio** (sensori leggeri, retrofit, automazioni non vitali).

Matrice per tipologia, Rischio–Impatto

La matrice è costruita su criteri tecnici: sicurezza, affidabilità, privacy, continuità operativa, manutenzione, salute.

Legenda

- **Rischio:** probabilità che si verifichi un problema
- **Impatto:** gravità del problema se si verifica
- Valori: **Basso / Medio / Alto / Molto alto**

Wireless

Categoria	Rischio	Impatto	Note tecniche
Interferenze RF	Alto	Medio	2.4 GHz molto affollato; Zigbee e Wi-Fi competono
Sicurezza informatica	Alto	Alto	Attacchi Wi-Fi, replay, jamming, cloud compromesso
Privacy	Alto	Alto	Telemetria costante, dipendenza da cloud
Affidabilità	Medio	Alto	Sensori a batteria, perdita pacchetti, latenza
Continuità operativa	Medio	Alto	Se cade il Wi-Fi o il cloud → automazioni ferme
Salute (RF)	Basso	Basso	Emissioni basse; rischio percepito più che reale
Manutenzione	Medio	Medio	Batterie, aggiornamenti firmware

Filare

Categoria	Rischio	Impatto	Note tecniche
Guasti fisici (cavi)	Basso	Medio	Rari, ma richiedono intervento fisico
Sicurezza informatica	Basso	Alto	Linea chiusa → molto più sicura
Privacy	Molto basso	Alto	Nessun cloud obbligatorio
Affidabilità	Molto basso	Alto	KNX, Modbus, RS485 → deterministici
Continuità operativa	Molto basso	Alto	Funzionano anche senza rete o cloud
Salute (RF)	Nessuno	Nessuno	Zero emissioni
Manutenzione	Basso	Medio	Quasi nulla, se progettato bene

Raccomandazioni per la progettazione di un impianto ibrido

La progettazione di un impianto domotico ibrido richiede un approccio metodico che combini la robustezza delle tecnologie filari con la flessibilità delle soluzioni wireless. L'obiettivo non è scegliere una tecnologia "migliore" in senso assoluto, ma **assegnare a ciascuna categoria di dispositivo il mezzo di comunicazione più coerente con il suo livello di criticità, il profilo di rischio e le esigenze di manutenzione e scalabilità**. Le raccomandazioni riportate di seguito derivano da criteri tecnici consolidati: affidabilità del canale, continuità operativa, resilienza agli attacchi, consumo energetico, latenza, privacy e possibilità di retrofit.

Questa tabella è pensata per un progettista o system integrator.

Tipologia dispositivo	Raccomandazione	Motivazione tecnica
Telecamere	Filare (PoE)	Sicurezza, banda stabile, privacy
Serrature smart	Filare + backup BLE	Sicurezza fisica, evitare jamming
Sensori allarme (gas, fumo, allagamento)	Filare	Criticità elevata
Sensori ambientali non critici	Wireless (Zigbee/Thread)	Flessibilità, basso traffico
Illuminazione	Filare (DALI/KNX)	Stabilità e sincronizzazione
Prese e attuatori principali	Filare	Evita attacchi e interferenze
Termostati e HVAC	Filare	Affidabilità e continuità
Assistenti vocali	Wireless o Ethernet	Rischio privacy indipendente dal mezzo
Elettrodomestici smart	Wireless	Non critici, retrofit semplice
Gateway domotici	Ethernet	Stabilità e sicurezza

Regola d'oro per un impianto ibrido

Tutto ciò che è critico → filare.

Tutto ciò che è accessorio → wireless.

Telecamere – Preferibile Filare (PoE)

Le telecamere IP rappresentano uno dei dispositivi più sensibili dell'intero ecosistema domotico. La trasmissione video richiede **banda stabile**, latenze ridotte e soprattutto **assenza di interferenze**.

L'alimentazione tramite PoE semplifica l'installazione, elimina alimentatori locali e garantisce continuità anche in caso di blackout se integrata con UPS. Dal punto di vista della sicurezza, il canale filare riduce drasticamente il rischio di intercettazioni RF, spoofing o jamming. Inoltre, la gestione centralizzata dello switch PoE permette un controllo granulare dell'alimentazione e un monitoraggio costante dello stato dei dispositivi.

Serrature Smart – Filare con Backup BLE

Le serrature elettroniche sono dispositivi ad **altissima criticità fisica**: un malfunzionamento o un attacco può compromettere la sicurezza dell'abitazione. La soluzione ideale prevede un collegamento filare per i comandi principali (apertura/chiusura, stato porta, sensori integrati), affiancato da un **backup BLE** per l'accesso locale in caso di guasto del bus o mancanza di rete. Il wireless non deve essere il mezzo primario: è vulnerabile a jamming, replay attack e interferenze. Il BLE, usato come fallback, garantisce comunque un accesso d'emergenza senza esporre la serratura a rischi inutili.

Sensori di Allarme Critici (Gas, Fumo, Allagamento) – Filare

Questi sensori devono funzionare **sempre**, senza eccezioni. La loro affidabilità è direttamente collegata alla sicurezza delle persone. Il collegamento filare elimina problemi di batteria, interferenze e congestione del canale radio. Inoltre, permette l'uso di protocolli fail-safe (NC/NO, supervisione, tamper) e garantisce tempi di risposta immediati. In un impianto professionale, la scelta wireless per questi dispositivi è accettabile solo in contesti dove il cablaggio è impossibile, e comunque con protocolli certificati EN50131.

Sensori Ambientali Non Critici – Wireless (Zigbee/Thread)

Temperatura, umidità, qualità dell'aria, luminosità e altri sensori non critici possono essere gestiti in modalità wireless. Zigbee e Thread offrono **basso consumo**, reti mesh affidabili e ottima scalabilità. La perdita temporanea di un pacchetto non compromette la sicurezza dell'impianto e il retrofit è semplice e poco invasivo. Questi sensori beneficiano della flessibilità del wireless, soprattutto in ambienti già arredati o in ristrutturazioni leggere.

Illuminazione – Filare

L'illuminazione richiede **sincronizzazione perfetta**, tempi di risposta immediati e un controllo preciso dell'intensità e delle scene. DALI, KNX e Modbus sono standard consolidati, progettati per garantire stabilità e prevedibilità. Il wireless può introdurre ritardi, perdita di pacchetti o comportamenti incoerenti, soprattutto in ambienti con molte sorgenti RF. In un impianto professionale, la luce deve essere sempre filare: è un elemento funzionale, non opzionale.

Prese e Attuatori Principali – Filare

Gli attuatori che comandano carichi importanti (prese, elettrovalvole, pompe, motori) devono essere collegati via filo. Motivazioni principali:

- evitare attacchi RF che potrebbero attivare/disattivare carichi critici
- garantire continuità operativa
- ridurre il rischio di interferenze
- assicurare un feedback affidabile sullo stato del carico Il wireless può essere usato per prese smart aggiuntive o funzioni non critiche, ma non per la dorsale principale.

Termostati e HVAC – Filare

Il controllo climatico richiede **continuità**, precisione e integrazione con sensori e attuatori distribuiti. Un termostato wireless può perdere connessione o subire interferenze, causando errori di regolazione o

consumi anomali. Il bus filare (Modbus, KNX, 0–10V, contatti puliti) garantisce stabilità e permette una gestione centralizzata dell'impianto HVAC, fondamentale in edifici complessi o multi-zona.

Citofoni e Videocitofoni – Filare PoE con protocolli H.264/H.265

I videocitofoni moderni non sono più semplici terminali audio: sono veri e propri **nodi video** dell'infrastruttura di sicurezza domestica. Per questo motivo, la scelta del mezzo di comunicazione e dei protocolli supportati è determinante.

La soluzione consigliata è un sistema **filare PoE**, integrato con protocolli video standard come **H.264/H.265**, così da poter essere gestito come una normale telecamera IP all'interno del sistema di videosorveglianza.

Motivazioni tecniche principali

- **Integrazione nativa con NVR/VMS** Utilizzando protocolli video standard, il videocitofono può essere registrato, monitorato e gestito come una telecamera IP. Questo permette:
 - registrazione continua o su evento
 - gestione centralizzata degli stream
 - sincronizzazione con gli altri dispositivi di sicurezza
- **Stabilità e continuità del canale** Il PoE garantisce alimentazione e rete su un unico cavo, riducendo i punti di guasto e permettendo l'uso di UPS centralizzati. La trasmissione filare elimina problemi di interferenze, congestione RF e jamming.
- **Qualità video costante** I protocolli **H.264** e **H.265** assicurano compressione efficiente e qualità elevata anche in condizioni di banda limitata. Questo è fondamentale per riconoscimento facciale, lettura targhe o verifica degli accessi.
- **Sicurezza superiore** Il canale filare riduce drasticamente i rischi di:
 - intercettazione
 - spoofing
 - attacchi man-in-the-middle
 - denial-of-service via radio
- **Compatibilità con sistemi professionali** I citofoni PoE con stream RTSP/H.264 sono compatibili con:
 - NVR professionali
 - sistemi KNX/IP
 - piattaforme di automazione
 - server SIP per chiamate interne

Perché evitare soluzioni wireless

I videocitofoni wireless soffrono di:

- latenza variabile
- perdita di pacchetti

- interferenze ambientali
- dipendenza dal Wi-Fi domestico
- maggiore vulnerabilità agli attacchi RF

In un impianto professionale, queste criticità sono inaccettabili.

Assistenti Vocali – Wireless o Ethernet

Gli assistenti vocali non sono dispositivi critici e la loro affidabilità non dipende dal mezzo di trasmissione. Il vero rischio è **la privacy**, che non cambia tra Wi-Fi o Ethernet: dipende dal cloud del produttore. Ethernet è preferibile quando possibile, per stabilità e latenza; il wireless resta accettabile per la maggior parte degli scenari domestici.

Elettrodomestici Smart – Wireless

Gli elettrodomestici connessi (forni, lavatrici, frigoriferi) utilizzano protocolli proprietari e si integrano tramite Wi-Fi o Zigbee. Non sono dispositivi critici e il loro funzionamento non richiede un canale deterministico. Il wireless permette un retrofit semplice e non richiede cablaggi aggiuntivi.

Gateway Domotici – Ethernet

Il gateway è il cuore logico dell'impianto: deve essere sempre raggiungibile, stabile e protetto. La connessione Ethernet garantisce:

- latenza minima
- assenza di interferenze
- maggiore sicurezza
- possibilità di alimentazione PoE Un gateway wireless rappresenta un singolo punto di vulnerabilità e non è consigliabile in impianti professionali.

Impianto Ibrido: la Soluzione Ottimale

Un impianto ibrido permette di:

- garantire **sicurezza e continuità** dove serve,
- mantenere **flessibilità e scalabilità**,
- ridurre costi e complessità,
- ottimizzare la manutenzione.

Linee guida spicciole

1. **Filare per tutto ciò che è critico** (sicurezza, energia, accessi, video).
2. **Wireless per ciò che è accessorio** (sensori leggeri, automazioni non vitali).
3. **Ethernet per i gateway** per evitare colli di bottiglia e vulnerabilità Wi-Fi.
4. **Segmentazione di rete** per isolare i dispositivi IoT.
5. **Riduzione della dipendenza dal cloud** quando possibile.

Conclusione

La progettazione moderna richiede un approccio ibrido, capace di coniugare **robustezza** e **innovazione**.
Un impianto ben progettato garantisce:

- sicurezza fisica e informatica,
- privacy degli utenti,
- affidabilità nel lungo periodo,
- scalabilità futura.

Prontuario del progettista e dell'installatore

Spunti di lettura da completare con l'affiancamento di professionisti certificati del settore

Premessa e Avvertenze

Le informazioni contenute in questo manuale rappresentano **linee guida tecniche e concettuali** utili per comprendere come progettare un impianto domotico ibrido moderno. Non sostituiscono la progettazione professionale: **impianti elettrici, sistemi di sicurezza, reti IP e bus di campo devono essere realizzati da tecnici abilitati e progettisti certificati**, nel rispetto delle normative vigenti.

Introduzione alla Domotica Moderna

La domotica contemporanea nasce dall'incontro tra due mondi:

- **domotica filare**, erede dell'automazione industriale
- **domotica wireless**, nata per flessibilità e retrofit

Entrambe hanno raggiunto maturità, ma con caratteristiche molto diverse. La scelta tra filare e wireless non è ideologica: è **ingegneristica**.

Filosofie Progettuali: Filare vs Wireless

Domotica Filare

Basata su:

- Modbus
- KNX
- RS485
- Ethernet/PoE

Punti di forza: stabilità, sicurezza, determinismo, nessuna interferenza RF.

Limiti: richiede cablaggio, progettazione accurata, costi iniziali maggiori.

Domotica Wireless

Basata su:

- Zigbee
- Thread
- Wi-Fi
- BLE
- Z-Wave

Punti di forza: retrofit, flessibilità, costi ridotti.

Limiti: interferenze, jamming, dipendenza da cloud, batterie.

Principi Generali di Progettazione

1. Filare per ciò che è critico
2. Wireless per ciò che è accessorio
3. IP per video, citofonia, supervisione
4. Modbus come bus di campo preferenziale
5. Segmentazione di rete
6. Riduzione dipendenza dal cloud
7. Logiche locali anche senza internet

Architettura a Livelli

Livello Campo (Field Layer)

Sensori, attuatori, HVAC, allarmi. → **Modbus RTU** consigliato.

Livello Automazione (Control Layer)

PLC, gateway, logiche locali. → **Modbus TCP / KNX / IP**.

Livello Supervisione (Supervision Layer)

Server domotico, HMI, app. → **IP cablato**.

Livello Rete (Network Layer)

Switch, router, firewall, VLAN. → **Ethernet + PoE**.

Scelta dei Mezzi di Comunicazione

Filare

Per:

- sicurezza
- accessi
- HVAC
- illuminazione primaria
- attuatori
- videosorveglianza
- citofonia

Wireless

Per:

- sensori comfort
- automazioni leggere
- retrofit

Preferenza per i Bus di Campo Filari (Modbus)

Modbus è il bus di campo preferenziale per:

- HVAC
- quadri elettrici
- sensori tecnici
- attuatori
- contatori
- pompe, irrigazione, motori

Motivi:

- protocollo aperto
- robusto
- economico
- diffusissimo
- diagnostica chiara
- integrazione immediata con PLC

Normative Tecniche di Riferimento

- **CEI 64-8** – impianti elettrici
- **CEI 205-18** – sistemi HBES/BACS
- **EN 50131** – allarmi intrusione
- **EN 54** – rivelazione incendi
- **GDPR** – privacy
- **Linee guida AGID** – sicurezza informatica

Progettazione della Rete IP

Segmentazione

- VLAN videosorveglianza
- VLAN domotica
- VLAN utenti
- VLAN guest

Switch PoE

- budget PoE adeguato
- UPS dedicato
- porte gigabit

Wi-Fi

- SSID separati
- potenza contenuta
- evitare mesh consumer

Sicurezza Informatica Applicata alla Domotica

- disabilitare UPnP
- password robuste
- VPN per accessi remoti
- log centralizzati
- firmware aggiornati
- evitare cloud non necessari

Continuità Operativa e UPS

Cosa deve restare acceso

- switch PoE
- gateway
- PLC
- NVR
- router/firewall

Autonomia consigliata

- residenziale: 30–60 min
- strutture critiche: > 2 h

Manutenzione Programmata

Filare

- diagnostica bus
- verifica terminazioni
- controllo UPS

Wireless

- sostituzione batterie
- verifica RSSI

Test annuali

- allarmi gas/fumo
- serrature

- scenari emergenza

Scenari Applicativi Reali

Appartamento

- Modbus per HVAC
- KNX per luci
- wireless per comfort

Villa

- Modbus per quadri, pompe, irrigazione
- PoE per telecamere e citofoni

Uffici / B&B

- dorsale Modbus + KNX
- rete IP segmentata

Criteri di Scelta dei Protocolli

Modbus (preferito)

- HVAC
- quadri
- attuatori
- sensori tecnici

KNX

- illuminazione
- pulsanti

IP

- video
- citofonia
- supervisione

Wireless

- comfort
- retrofit

Criteri di Scelta dei Cavi

Modbus / RS485

- twistato schermato
- topologia lineare

- terminazioni corrette

Ethernet

- CAT6A schermato
- max 90–100 m

Separazione

- potenza e segnale separati

Raccomandazioni per Tipologia di Dispositivo

- Telecamere → **PoE**
- Citofoni → **PoE + H.264/H.265**
- Serrature → **filare + BLE backup**
- Sensori allarme → **filare**
- Sensori comfort → **Zigbee/Thread**
- Illuminazione → **DALI/KNX**
- Attuatori → **filare**
- HVAC → **Modbus**
- Gateway → **Ethernet**

Conclusioni

Un impianto domotico moderno deve essere:

- **ibrido**
- **robusto**
- **scalabile**
- **sicuro**
- **manutenibile**

E deve basarsi su una dorsale **filare**, con **Modbus come bus di campo preferenziale**, affiancato da IP per video e supervisione, e wireless solo dove ha senso.

Disclaimer Legale – Limitazione di Responsabilità

Il software **DomoManager**, la relativa documentazione tecnica e tutti i moduli associati (inclusi ma non limitati a: *DM.hpp*, *DMFrontend.hpp*, *DMSetup.hpp*, *DMDiagnostic.hpp*, automazioni, configurazioni e profili hardware) sono forniti **“così come sono”**, senza alcuna garanzia espressa o implicita.

L'autore e i collaboratori **non assumono alcuna responsabilità** per:

- danni diretti o indiretti
- malfunzionamenti
- perdita di dati
- interruzioni di servizio
- danni a cose, impianti o persone
- utilizzo improprio o non conforme del software
- modifiche non autorizzate al codice o alla configurazione
- integrazioni con dispositivi di terze parti non certificati

L'utente accetta che:

L'installazione, la configurazione e l'uso del software avvengono sotto la propria esclusiva responsabilità.

Il sistema è progettato per applicazioni domotiche e di automazione non critiche. Non deve essere utilizzato in contesti dove un malfunzionamento potrebbe causare:

- rischi per la sicurezza personale
- danni strutturali
- interruzioni di servizi essenziali
- condizioni pericolose per persone o animali

L'utente è tenuto a:

- verificare la correttezza delle configurazioni
- testare ogni automazione prima dell'uso reale
- assicurarsi che i dispositivi collegati siano conformi alle normative vigenti
- implementare adeguate misure di sicurezza elettrica e informatica

L'autore declina ogni responsabilità derivante da:

- modifiche al codice sorgente
- utilizzo in ambienti industriali o critici
- integrazioni con hardware non supportato
- errori di cablaggio o installazione
- uso improprio delle automazioni o delle scene

L'uso del software implica l'accettazione integrale del presente disclaimer.

DOMO Manager è ciò che davvero conta:

*la continuità, la sicurezza, la sostenibilità e la qualità dell'ambiente in cui viviamo ogni
giorno...*
