ED
Eugenio Damaso
ESG · FINANCE · SECURITY · AI

GUIDA PRATICA · SICUREZZA DEGLI IMPIANTI

Separare gli ambienti per ridurre l'*esposizione* in rete

Zone, regole di traffico, accesso dei fornitori e roadmap a 90 giorni. Con i consigli di un CISO.



eugeniodamaso.it
Novembre 2026

Indice

01	A chi serve e come usarla	3
02	Il principio: ciò che non serve su Internet non ci deve stare	3
03	Le zone: dove sta cosa	4
04	Le regole di traffico tra le zone	5
05	L'accesso remoto dei fornitori	6
06	Scoprire l'esposizione	6
07	Credenziali, patch e dispositivi a fine vita	7
08	Monitoraggio e continuità	8
09	Roadmap a 90 giorni	9
10	Otto errori da evitare	9
11	Checklist finale	10
12	Fonti e riferimenti	11

SE HAI POCO TEMPO

- Leggi le sezioni 02, 03, 04 e 05: principio, zone, regole di traffico, fornitori.
- Applica la roadmap a 90 giorni (sezione 09).
- Usa la checklist finale (sezione 11) con chi gestisce i tuoi impianti.

01 A chi serve e come usarla

Questa guida serve a chi gestisce impianti collegati in rete (refrigerazione, climatizzazione, produzione, magazzini) e vuole ridurre ciò che è raggiungibile da Internet.

Nasce da un caso reale. Tra ottobre e inizio novembre 2026 alcuni attaccanti hanno cambiato da remoto i parametri dei controllori di refrigerazione di centinaia di supermercati europei. Il CERT-FR ha confermato numerose compromissioni dei Danfoss AK-SM e AK-SC e dei supervisori Copeland e Dixell xweb, e Danfoss ha spiegato che le unità colpite erano per lo più a fine vita. Gli esempi vengono da quel caso, ma le regole valgono per qualsiasi apparato di impianto: caldaie, compressori, linee di confezionamento, controllo accessi.

Leggi per prime le sezioni sul principio, sulle zone, sulle regole di traffico e sull'accesso dei fornitori. Poi applica la roadmap a 90 giorni e usa la checklist finale con chi gestisce i tuoi impianti.

La guida non sostituisce le istruzioni del produttore né il bollettino dell'ACN «Misure urgenti di verifica e mitigazione per operatori della distribuzione alimentare e della filiera del freddo»: controlla sempre la versione aggiornata. Stato delle informazioni: 3 novembre 2026.

02 Il principio: ciò che non serve su Internet non ci deve stare

Un impianto non ha bisogno di Internet. Ha bisogno che qualcuno, ogni tanto, possa raggiungerlo in modo controllato.

Sono due cose diverse, e quasi tutti gli incidenti nascono dall'averle confuse. Un controllore con l'interfaccia web su un indirizzo pubblico è comodo per il tecnico e comodo per chiunque faccia una scansione. Nella ricerca di Claroty, una sola scansione Censys trovava 2.765 interfacce di gestione dell'AK-SM 800A raggiungibili da Internet. Il CERT-FR è netto: esporre un'interfaccia di gestione su Internet è contrario alle buone pratiche.

Una nave non si salva con uno scafo più spesso. Si salva con le paratie stagne: se l'acqua entra in un compartimento, resta lì. La separazione degli ambienti fa lo stesso. Non garantisce che nessuno entri mai da qualche parte; impedisce che da quel punto si arrivi a tutto il resto, cioè alle temperature, alle pompe, ai compressori.

Tre domande valgono per ogni collegamento che trovi. Serve davvero? Serve a qualcuno che sai nominare? Serve sempre, o solo quando c'è un intervento? Se una risposta è «non lo so», il collegamento si chiude finché non lo sai.

03 Le zone: dove sta cosa

Quattro zone, tre barriere sul percorso dall'esterno al campo. Dall'esterno si arriva solo alla DMZ di accesso remoto; da lì, con regole precise, si scende verso la supervisione e il campo.

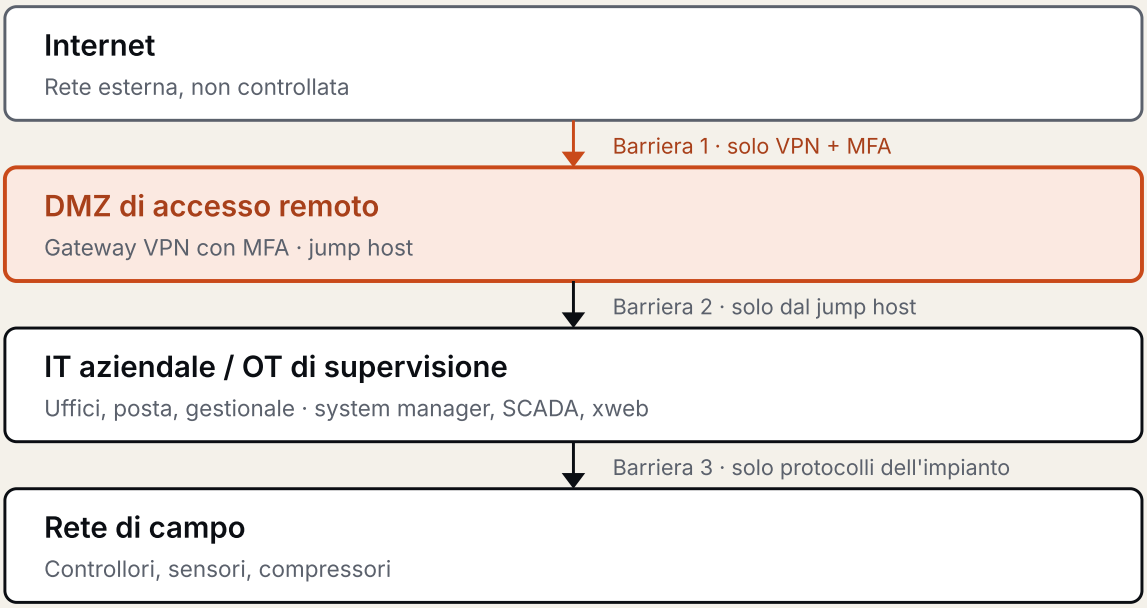


Figura 1 — Zone di rete. Quattro zone, tre barriere dall'esterno al campo. Le connessioni esterne si fermano nella zona evidenziata.

Elaborazione dell'autore.

Una zona non ne raggiunge un'altra senza che una regola lo consenta.

- **DMZ di accesso remoto.** Il solo punto in cui arrivano le connessioni dall'esterno: gateway VPN con MFA e jump host, la macchina intermedia da cui lavora il tecnico. Nessun controllore ci abita.
- **IT aziendale.** Uffici, posta, gestionale. Parla con la DMZ per i flussi autorizzati e mai direttamente con gli impianti.
- **OT di supervisione.** System manager, SCADA, supervisori come gli xweb. Non ha un indirizzo raggiungibile da Internet.
- **Rete di campo.** Controllori, sensori, compressori. Parla solo con la supervisione, con i protocolli che servono all'impianto.

> **CONSIGLIO DA CISO**
>
> Molti protocolli industriali sono nati per reti isolate. Secondo Facilities Dive, che cita un rapporto di Armis, Modbus, molto usato in Europa, spesso non prevede autenticazione né cifratura, e i Danfoss AK-SM800 e AK-SC355 lo usano. Per questi apparati la separazione di rete è la barriera che conta.

04 Le regole di traffico tra le zone

Il principio è il rifiuto per impostazione predefinita (*default deny*): ogni flusso è vietato, salvo quello che hai scritto e motivato. Lo standard IEC 62443 lo esprime con zone, gruppi di apparati con le stesse esigenze di sicurezza, e condotti, i percorsi di comunicazione tra una zona e l'altra: si progettano, si controllano e si registrano. NIST SP 800-82 Rev. 3 tratta la separazione tra rete aziendale e rete di controllo, con una DMZ in mezzo, come misura centrale dell'architettura.

Da	A	Esito	Condizione
Internet	DMZ	Solo VPN	MFA, utenti nominali
Internet	OT e campo	**Mai**	Nessuna eccezione, nemmeno temporanea
IT aziendale	DMZ	Sì	Flussi elencati e documentati
IT aziendale	OT e campo	Mai diretto	Si passa dalla DMZ
DMZ	OT	Sì	Solo dal jump host, solo i servizi necessari
OT	Campo	Sì	Solo i protocolli dell'impianto
OT	Internet	**No**	Notifiche e aggiornamenti passano da un relay o proxy in DMZ

Tabella 1 — Matrice dei flussi. Tutto ciò che non è elencato è vietato.

Elaborazione dell'autore.

Quattro regole pratiche:

- Nessun port forwarding dal router verso un controllore: è uno dei modi tipici con cui un'interfaccia finisce su Internet.
- Meglio connessioni che partono dall'interno verso un punto che controlli, che porte aperte in ingresso.
- Ogni regola ha un responsabile, una motivazione e una data di revisione. Una regola senza responsabile si toglie.
- Registra anche i traffici negati: dicono più dei permessi.

> **CONSIGLIO DA CISO**
>
> I controllori che inviano allarmi per e-mail vanno configurati su un relay di posta interno, mai su un server esterno raggiunto direttamente. Una delle falle descritte da Claroty riguardava proprio la configurazione degli allarmi via e-mail.

05 L'accesso remoto dei fornitori

Il frigorista che assiste l'impianto da remoto ha le chiavi di casa. Va trattato come chi le ha: con le regole di un dipendente e qualcuna in più.

1. **Un solo canale.** VPN sicura o rete protetta, che termina in DMZ e non dentro l'OT. Il filtro sugli IP del fornitore, per il CERT-FR, è un ripiego d'emergenza e non una soluzione stabile.
2. **Utenti nominali e MFA.** Niente account condiviso con il fornitore, niente password generiche. L'autenticazione a più fattori vale per ogni accesso remoto: la chiede anche l'ACN.
3. **Jump host.** Il tecnico non raggiunge il controllore dal proprio portatile: entra nel jump host e da lì nell'impianto. Le sessioni si registrano.
4. **Accesso a tempo.** Si apre per l'intervento concordato e si chiude alla fine. La teleassistenza sempre attiva è la prima voce da eliminare.
5. **Revoca.** Un elenco di chi ha accesso, rivisto ogni trimestre, e una procedura per toglierlo in un giorno.
6. **Contratto.** Obblighi di sicurezza, notifica degli incidenti, aggiornamento del firmware, elenco del personale autorizzato.

Prima di tagliare il collegamento dati con il frigorista controlla le condizioni dell'assicurazione, come indica il CERT-FR, e concorda un'alternativa: l'impianto deve restare assistito.

> CONSIGLIO DA CISO
>
> Se il fornitore sostiene che senza accesso permanente non può garantire il servizio, chiedi la motivazione per iscritto e proponi l'accesso su richiesta. Se il vincolo c'è davvero, mettilo nel contratto e assegna il rischio a una persona con nome e cognome.

06 Scoprire l'esposizione

Non puoi chiudere ciò che non sai di avere. Si parte dall'elenco, poi si guarda dall'esterno.

1. **Inventario.** Per ogni controllore: modello, firmware, stato di supporto, responsabile, sede e percorso di accesso remoto. Sono i dati che chiede l'ACN per il censimento.
2. **Vista dall'esterno.** Cerca nel tuo spazio di indirizzi pubblici le interfacce di gestione raggiungibili. Claroty ha misurato l'esposizione con Shodan e Censys, piattaforme che indicizzano ciò che risponde su Internet. Cerca solo sui tuoi indirizzi o su quelli per cui hai un'autorizzazione.

3. **I punti ciechi.** Router 4G installati dai manutentori, sedi periferiche, controllori acquistati in autonomia da un singolo punto vendita, collegamenti cloud del produttore. Chiedi a ogni fornitore l'elenco degli accessi che ha.
4. **Se trovi un'interfaccia esposta,** togli l'esposizione prima di aggiornare. Poi controlla la configurazione, in particolare le fasce di sbrinamento.
5. **Se sospetti una compromissione,** conserva i log e segnala l'incidente al CSIRT Italia. Un ripristino di fabbrica da solo non basta su un apparato a fine vita ancora esposto: il CERT-FR avverte che resterà vulnerabile e verrà probabilmente compromesso di nuovo.

---

07 Credenziali, patch e dispositivi a fine vita

Tre voci, tre risposte diverse.

Credenziali. Cambia le password di fabbrica e usa password diverse per sito e per apparato. Per i Danfoss il CERT-FR indica anche il livello di sicurezza «Strict».

Patch. Per l'AK-SM 800A, Claroty indica il firmware R4.3.1 o successivo (la build 4.2 corregge il bypass di autenticazione CVE-2025-41450). Prima prova su una sede pilota, salva la configurazione e prevedi il rientro. Verifica sempre le versioni sul sito del produttore.

Fine vita (EOL, *end of life*). Sono gli apparati che il produttore non aggiorna più. Danfoss ha indicato come *legacy*, tra gli altri, l'AK-SM 800 e l'AK-SC 355. Qui la patch non esiste e la difesa è la rete: isolamento, filtro degli accessi, monitoraggio e una data di sostituzione. Per il CERT-FR, lasciare in Internet un apparato senza correzioni gli dà una probabilità molto alta di essere compromesso.

Ogni apparato a fine vita è una voce nel registro dei rischi, con un responsabile e una data. Un budget di sostituzione che manca è un rischio accettato senza che nessuno l'abbia firmato.

> **CONSIGLIO DA CISO**
>
> Quando acquisti un nuovo impianto chiedi per iscritto il ciclo di vita del software: per quanti anni arrivano le correzioni di sicurezza e come si installano. È la domanda che non si fa mai e che costa di più dopo.

08 Monitoraggio e continuità

Prevenire non basta: bisogna accorgersi in fretta e sapere cosa fare nei primi trenta minuti.

Monitoraggio

- Raccogli i log di firewall, VPN e piattaforma di supervisione, come indica l'ACN.
- Imposta allarmi su tre eventi: modifica dei parametri (setpoint, fasce di sbrinamento), accessi da indirizzi sconosciuti, nuovi account.
- Confronta a intervalli regolari i parametri in uso con la configurazione di riferimento salvata.

Continuità

- Sonde di temperatura indipendenti dal controllore, con un allarme proprio e una via di comunicazione non collegata alla rete OT. Se il controllore viene alterato, la sonda continua a dire la verità.
- Una procedura manuale scritta: cosa fa il punto vendita se i banchi segnano temperature anomale, chi decide sullo scarto della merce, chi chiama chi. Il Regolamento (CE) 852/2004 chiede che la catena del freddo non si interrompa: i prodotti esposti a temperature non idonee si valutano e, se non sono sicuri, si eliminano.
- Una copia della configurazione di ogni controllore, con data e versione, conservata fuori dalla rete OT.

Incidenti. In caso di sospetta compromissione conserva i log, segnala al CSIRT Italia e avvisa l'assicurazione secondo contratto. Per i soggetti NIS valgono la pre-notifica entro 24 ore e la notifica entro 72 ore per gli incidenti significativi, operative dal 15 gennaio 2026.

> **CONSIGLIO DA CISO**
>
> Prova la procedura manuale a freddo, in un momento tranquillo. Si scoprono i numeri di telefono sbagliati e le chiavi che mancano quando costa poco scoprirli.

09 Roadmap a 90 giorni

Tre fasi di trenta giorni, ciascuna con un criterio di uscita: non si passa alla successiva finché non è soddisfatto.

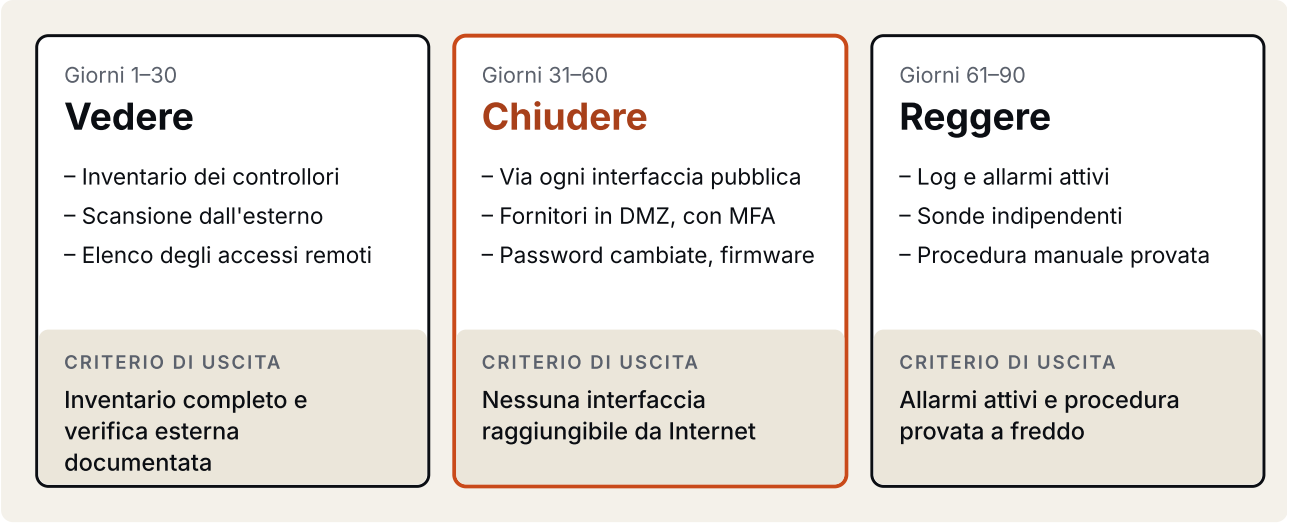


Figura 2 — Roadmap a 90 giorni. Tre fasi, tre criteri di uscita. La fase evidenziata è quella in cui l'esposizione si chiude.

Elaborazione dell'autore.

La prima fase non cambia nulla: serve a sapere. Il lavoro vero è nella seconda, evidenziata, quando l'esposizione si chiude e i fornitori passano dalla DMZ. La terza rende il risultato stabile con il monitoraggio e le prove.

10 Otto errori da evitare

1. Credere che l'impianto sia isolato senza verificarlo dall'esterno. Un router 4G o un port forwarding dimenticato bastano a smentirlo.
2. Lasciare le password di fabbrica o un account condiviso con il fornitore.
3. Mettere una VPN senza MFA, o permettere tutto a chi è entrato nella VPN.
4. Tenere la teleassistenza sempre attiva.
5. Aggiornare il firmware senza aver tolto prima l'esposizione. L'ordine indicato dal CERT-FR è uscire dalla zona di pericolo e poi rimettere in servizio.
6. Considerare il ripristino di fabbrica una soluzione.
7. Affidare sonde e allarmi allo stesso controllore che potrebbe essere alterato.
8. Tagliare i collegamenti senza controllare l'assicurazione e senza un piano per l'assistenza.

11 Checklist finale

Visibilità

- ☐ Inventario di controllori, supervisori e gateway con modello, firmware, stato di supporto, responsabile e sede
- ☐ Elenco di tutti gli accessi remoti, con chi li usa e perché
- ☐ Verifica dall'esterno dei propri indirizzi pubblici, eseguita e documentata

Esposizione

- ☐ Nessuna interfaccia di gestione raggiungibile da Internet
- ☐ Nessun port forwarding né router 4G non censito verso gli impianti

Architettura

- ☐ DMZ di accesso remoto con VPN, MFA e jump host
- ☐ Regole di traffico scritte, con responsabile e data di revisione
- ☐ Nessun collegamento diretto tra IT e OT

Accessi

- ☐ Utenti nominali con MFA, nessuna password condivisa
- ☐ Accessi dei fornitori a tempo, registrati e rivisti ogni trimestre
- ☐ Clausole di sicurezza nei contratti di assistenza

Apparati

- ☐ Password di fabbrica cambiate e livello di sicurezza più alto dove previsto
- ☐ Firmware aggiornato dove il produttore lo supporta
- ☐ Piano di sostituzione con data per ogni apparato a fine vita

Continuità

- ☐ Sonde di temperatura e allarmi indipendenti dal controllore
- ☐ Procedura manuale scritta e provata
- ☐ Configurazioni salvate fuori dalla rete OT
- ☐ Contatti pronti per un incidente: CSIRT Italia, assicurazione, fornitore

12 Fonti e riferimenti

Stato delle informazioni: 3 novembre 2026.

- CERT-FR, alert CERTFR-2026-ALE-012 (12-16 ottobre 2026)
- Claroty Team82, «Freeze the Controller, Defrost the Food» (9 agosto 2026)
- Facilities Dive, «Hack of Danfoss refrigeration controllers in Europe» (13 ottobre 2026)
- ANSA, «Attacchi hacker ai supermercati, alert Agenzia cyber in Italia» (2 novembre 2026)
- Open, «L'attacco hacker ai frigoriferi dei supermercati francesi» (13 ottobre 2026)
- Studio Quality, sintesi del bollettino ACN AL04/261013/CSIRT-ITA
- ACN, bollettino «Misure urgenti di verifica e mitigazione per operatori della distribuzione alimentare e della filie ra del freddo» (pagina non raggiungibile al momento della verifica: le indicazioni citate sono tratte da ANSA e dalla sintesi di Studio Quality)
- NIST, SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security (settembre 2023)
- Serie di standard ISA/IEC 62443 sulla sicurezza dei sistemi di automazione e controllo industriale (zone e condotti): consulta il testo ufficiale.