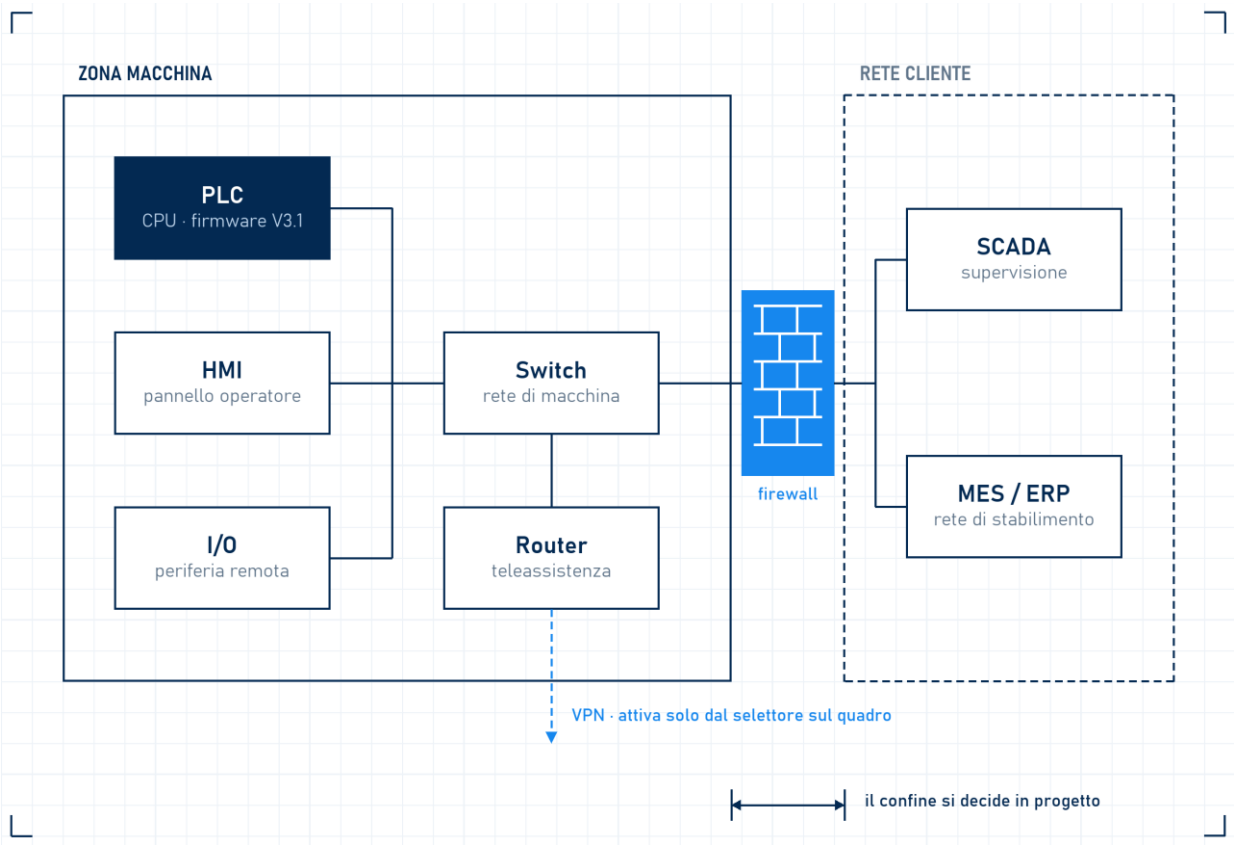
Cosa devi fare per la cybersecurity se fornisci una macchina con PLC

La guida pratica per l'ufficio tecnico: cosa cambiare nel progetto, nella rete e nella teleassistenza prima del Regolamento Macchine 2027. Scritta da chi i PLC li programma.



AUTORE	CONTENUTO	REVISIONE
Reda	Premessa e Capitolo 1	1.0
EDITORE	DESTINATARI	DATA
Mindware SRL	Uffici tecnici, costruttori, integratori	Novembre 2026

IN QUESTO ESTRATTO

00 **Premessa** 3

0.1 Se lavori in un ufficio tecnico, questa guida è per te 3

0.2 Chi sono 3

0.3 Perché ho scritto questa guida 4

0.4 Cosa troverai in questa guida 4

0.5 Come usare questa guida 4

01 **Cosa ti serve sapere in questo momento** 5

1.1 Dove ti trovi tu 5

1.2 Le tre regole che ti riguardano 6

1.3 A che punto siamo 7

1.4 Cosa significa per te 7

1.5 Un primo esempio pratico: la scelta del PLC 7

1.6 E i PLC di generazione precedente? 9

1.7 Cosa ne ricava chi progetta 10

1.8 Una domanda da porsi subito: e la PUT/GET? 11

1.9 Nel resto della guida 11

NOTA

Questa guida offre indicazioni tecniche per la progettazione. Non è una consulenza legale né una certificazione: la valutazione dei rischi della tua macchina resta a te.

Le funzioni dei dispositivi citati dipendono da modello e versione: verifica sempre sul manuale del produttore. Siemens, SIMATIC, TIA Portal e SCALANCE sono marchi di Siemens AG.

© 2026 Mindware SRL · mind-ware.eu

00

PRIMA DI INIZIARE

Premessa

0.1 Se lavori in un ufficio tecnico, questa guida è per te

Sei un progettista elettrico o software, lavori nell'ufficio tecnico di un costruttore di macchine o di un system integrator, e ultimamente ti senti chiedere sempre più spesso: “E la cybersecurity?”.

Partiamo da una convinzione molto diffusa, che è il primo punto da chiarire: la cybersecurity non riguarda solo chi scrive il software del PLC. Riguarda tutta la macchina, e quindi tutti quelli che la progettano.

Molte delle decisioni che la rendono più o meno sicura vengono prese prima che il programmatore scriva una sola riga:

- la scelta dei componenti, a partire dal PLC e dalla sua versione;
- l'architettura della rete della macchina e il modo in cui si collega a quella del cliente;
- la teleassistenza e i dispositivi che la rendono possibile;
- il quadro elettrico, gli accessi fisici e le porte di comunicazione;
- la documentazione che consegni insieme alla macchina.

Sono scelte di progettazione, e questa guida parla proprio di quelle.

0.2 Chi sono

Mi chiamo Reda e lavoro da molti anni nell'automazione industriale come programmatore PLC e SCADA. Ho seguito macchine e impianti dalla progettazione alla messa in servizio: so come si imposta un progetto, come si costruisce un quadro, come si configurano le reti e cosa succede quando la macchina arriva nello stabilimento del cliente.

Nel tempo ho costruito competenze trasversali, non limitandomi ai PLC e spingendomi a conoscere l’ambito dei software di alto livello e gestione di reti più avanzate, anche a livello di stabilimento come consulente esterno.

Questa guida nasce da quell'esperienza in campo.

0.3 Perché ho scritto questa guida

Negli ultimi mesi costruttori, integratori e colleghi mi fanno sempre la stessa domanda: “Per la cybersecurity, cosa devo fare?”.

Di documenti e indicazioni sull'argomento ne esistono molti, ma restano quasi sempre generici: spiegano le norme, raramente danno nozioni pratiche su cosa fare sulla macchina.

Intanto le regole stanno cambiando davvero. Dal 2027 la cybersecurity entra a far parte della marcatura CE, e i clienti più strutturati chiedono già ai loro fornitori garanzie di sicurezza. Questa guida vuole colmare la distanza tra le norme e il lavoro di tutti i giorni, con il linguaggio di chi lavora in automazione.

0.4 Cosa troverai in questa guida

Alla fine della lettura avrai un quadro chiaro di cosa ti viene chiesto e, soprattutto, di come tradurlo in scelte tecniche:

- quali regole riguardano te, i tuoi fornitori e i tuoi clienti, senza entrare nei dettagli giuridici;
- come scegliere PLC, versioni firmware e strumenti di sviluppo pensando anche alla sicurezza;
- come impostare la rete della macchina e separarla da quella del cliente;
- come organizzare la teleassistenza, dalle soluzioni più strutturate alle più pratiche;
- cosa considerare nel quadro elettrico e negli accessi fisici alla macchina;
- cosa consegnare al cliente e come rispondere alle sue richieste di sicurezza;
- gli errori più frequenti che si incontrano in campo, e come evitarli.

0.5 Come usare questa guida

Alcune norme tecniche di dettaglio sono ancora in fase di definizione, ma i principi su cui si basano sono già chiari e condivisi:

01	02	03	04
accessi controllati	**reti separate**	**interventi tracciabili**	**componenti aggiornabili**

Questa guida è costruita su quei principi. Seguendo le indicazioni che trovi qui, molti dei punti richiesti dalle normative li avrai già coperti, e quando arriveranno le regole definitive ti troverai con il lavoro già impostato nel modo giusto. La guida ti dà i criteri tecnici; la valutazione dei rischi della tua macchina resta il passaggio in cui li applichi.

01

CAPITOLO 1

Cosa ti serve sapere in questo momento

Per lavorare bene non serve conoscere le norme a memoria. Serve sapere chi c'è nella catena che porta una macchina in fabbrica, quale regola riguarda ciascuno e quali scadenze contano.

La confusione di questi mesi nasce dal fatto che tre regole diverse, nate per scopi diversi, arrivano nello stesso periodo e si applicano tutte, in qualche modo, alla stessa macchina. Messe in fila una alla volta, il quadro è molto più semplice di quanto sembri.

1.1 Dove ti trovi tu

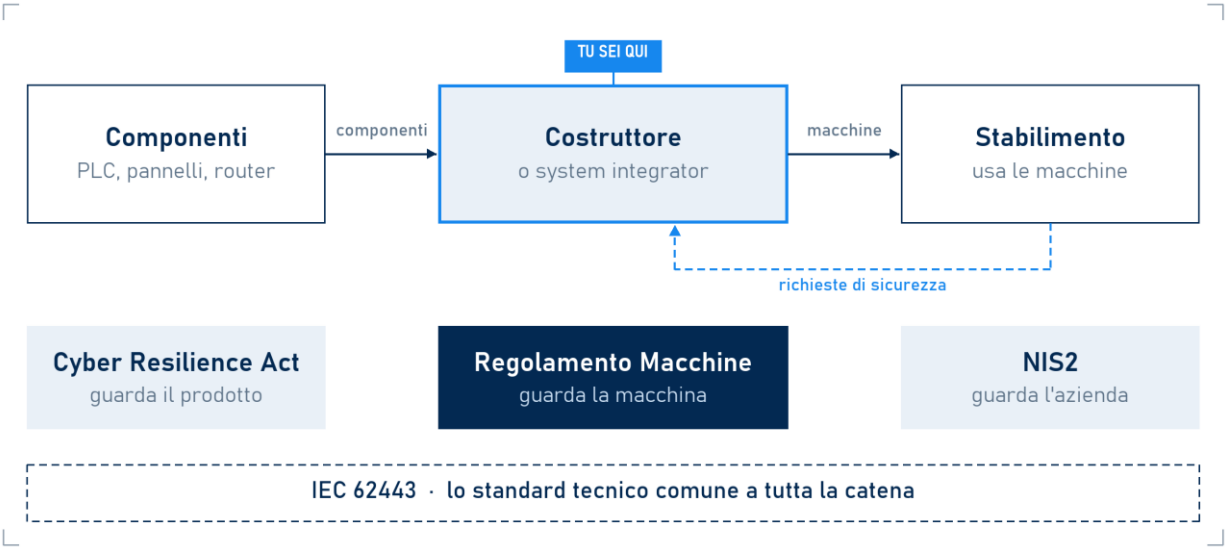


FIG. 1 La catena che porta una macchina in fabbrica: tre anelli, tre regole.

Tu sei nel mezzo: ricevi componenti che il Cyber Resilience Act renderà sempre più sicuri, rispondi del Regolamento Macchine per ciò che consegni, e ricevi dal cliente richieste di sicurezza che nascono dalla gestione del rischio della sua filiera, sempre più spesso per effetto della NIS2.

1.2 Le tre regole che ti riguardano

Ogni regola guarda una cosa diversa: il Regolamento Macchine guarda la macchina, il Cyber Resilience Act guarda il prodotto digitale, la NIS2 guarda l'azienda che usa le macchine.

REGOLA	COSA GUARDA	CHI COINVOLGE	DA QUANDO
Regolamento Macchine (UE) 2023/1230	La macchina immessa sul mercato	Il costruttore; l'integratore quando assembla più macchine	Gennaio 2027
Cyber Resilience Act (UE) 2024/2847	I prodotti con elementi digitali	Chi produce PLC, pannelli, router, software; in alcuni casi il costruttore	Segnalazioni da settembre 2026, obblighi principali da dicembre 2027
NIS2 in Italia D.Lgs. 138/2024	L'azienda e i suoi fornitori	Lo stabilimento, se rientra; di riflesso i suoi fornitori	Già in vigore

TAB. 1 Le tre regole a confronto.

Regolamento Macchine. È quella che ti riguarda più da vicino. Sostituisce la Direttiva Macchine e, per la prima volta, chiede di proteggere la macchina dalle alterazioni: un accesso non autorizzato o una connessione esterna non devono poterla rendere pericolosa, e gli interventi sul software devono lasciare traccia. In pratica, la cybersecurity entra nella valutazione dei rischi e nella marcatura CE.

Cyber Resilience Act. Riguarda chi produce componenti e software: PLC, pannelli operatore, router per la teleassistenza, applicativi. Chiede prodotti sicuri fin dalla progettazione e aggiornamenti di sicurezza per tutta la loro vita. Una parte è già in vigore: da settembre 2026 i fabbricanti devono segnalare le vulnerabilità sfruttate e gli incidenti gravi; gli obblighi principali arrivano a dicembre 2027. Per te significa componenti sempre più ricchi di funzioni di sicurezza da usare e configurare; e se fornisci con la macchina un tuo software o un tuo dispositivo, può riguardarti direttamente.

NIS2. Non parla di macchine ma di aziende: chiede a quelle medio-grandi dei settori critici, manifattura compresa, di gestire il rischio informatico e di controllare i propri fornitori. È il motivo per cui i clienti iniziano a chiederti come gestisci accessi, aggiornamenti e incidenti.

> A fare da riferimento tecnico comune c'è la serie **IEC 62443**: lo standard internazionale per la sicurezza dei sistemi di automazione, che costruttori, integratori e clienti usano per parlare la stessa lingua.

1.3 A che punto siamo

Le scadenze sono fissate e i principi sono chiari; alcuni strumenti di dettaglio sono ancora in arrivo.

GIÀ DEFINITO	Le scadenze, i principi di base (accessi controllati, reti separate, interventi tracciabili, componenti aggiornabili) e lo standard tecnico di riferimento.
DISPONIBILE DA POCO	La UNI/PdR 199, prassi di riferimento italiana sviluppata con Federmacchine, che propone un metodo per valutare le vulnerabilità delle macchine.
IN ARRIVO	La norma tecnica europea dedicata alla protezione delle macchine dalle alterazioni e la guida completa della Commissione al Regolamento Macchine.

Non c'è motivo di aspettare che tutto sia scritto: le basi su cui lavorare ci sono già, e la scadenza del 2027 resta quella.

1.4 Cosa significa per te

> *Se consegni macchine con un PLC, dal 2027 la domanda non sarà più "se" occuparti di cybersecurity, ma "come lo dimostri".*

Te lo chiederà la marcatura CE, con il Regolamento Macchine. Te lo chiederà il cliente, con le richieste che può farti per gestire il rischio della propria filiera. E te lo chiederanno sempre più spesso i fornitori dei componenti, che ti daranno prodotti con funzioni di sicurezza da configurare.

La buona notizia è che gran parte di quello che serve si decide in fase di progetto, con scelte che conosci già: quale PLC usi, come separi la rete della macchina da quella del cliente, come gestisci la teleassistenza, cosa scrivi nella documentazione che consegni. Non serve diventare esperti di informatica. **Serve fare quelle scelte con un criterio.**

1.5 Un primo esempio pratico: la scelta del PLC

Prendiamo il caso più comune, una macchina con un PLC Siemens.

Le funzioni di sicurezza che oggi un PLC mette a disposizione, come la gestione di utenti e ruoli (chi può leggere, chi può modificare), la registrazione degli eventi di sicurezza e le comunicazioni protette verso pannelli e strumenti di programmazione, non dipendono dal programma che scriverai: dipendono dalla famiglia della CPU, dalla versione del firmware e dalla versione di TIA Portal.

Qualche esempio concreto, da verificare sempre sul manuale della CPU che scegli:

S7-1500 firmware dalla V3.1 · TIA Portal V19 o successivi	Gestione di utenti e ruoli integrata, invio degli eventi di sicurezza, come gli accessi di programmazione, a un server di log tramite Syslog.
S7-1200 G2 TIA Portal V20 o successivi	La nuova generazione porta anche sulla gamma compatta la gestione di utenti e ruoli, con un unico account per programmazione, web server e OPC UA.
S7-1200 firmware V4.7	Gestione di utenti e ruoli e invio degli eventi via Syslog arrivano anche sulla generazione precedente, ma solo sulle CPU che possono essere aggiornate a questa versione.
S7-1200 firmware precedenti	Protezione con password a livelli di accesso, senza gestione di utenti e ruoli.

Una CPU presa a magazzino, con un firmware di qualche anno fa, può quindi non offrire queste funzioni anche se appartiene alla famiglia giusta. A volte basta aggiornare il firmware, a volte la CPU non lo consente: va verificato in fase di progetto, non alla messa in servizio.

TRADOTTO IN PROGETTAZIONE

01 In fase di offerta e di distinta materiali scegli una CPU che supporti queste funzioni, e annota la versione firmware con cui verrà consegnata.

02 Allinea l'ufficio tecnico su una versione di TIA Portal recente e supportata dal produttore, e usa la stessa per tutto il progetto.

03 Decidi già nello schema elettrico come la macchina si collegherà alla rete del cliente: interfacce separate, un modulo di comunicazione aggiuntivo o un router di macchina richiedono spazio, alimentazione e un costo nel quadro.

04 Tieni traccia delle versioni installate: andranno indicate nella documentazione di consegna e mantenute aggiornate nel tempo.

Per il punto 4 basta una tabella semplice, da allegare alla documentazione della macchina. Un esempio di come impostarla:

DISPOSITIVO	MODELLO E CODICE ARTICOLO	VERSIONE FIRMWARE O SOFTWARE	NOTE
CPU	S7-1500 6ES7 5xx-xxxxx-xxxx	V3.1	Utenti e ruoli attivi, log verso server Syslog
Pannello operatore	Modello e codice del pannello	Versione dell'immagine installata	Password di default cambiate
Router di teleassistenza	Modello e codice	Versione firmware	Abilitazione da selettore sul quadro
Software di progetto	TIA Portal	V19 o successiva, con update installati	Stessa versione per tutto il progetto

TAB. 2 Esempio di registro delle versioni installate, da allegare alla documentazione.

1.6 E i PLC di generazione precedente?

Non vanno esclusi. Su molte macchine, e soprattutto sugli impianti esistenti, una CPU di generazione precedente resta la scelta più sensata. Va però installata con qualche accorgimento in più, che compensa le funzioni che non ha:

- **Rete della macchina dietro un firewall.** Tra la rete della macchina e quella del cliente si mette un filtro che lascia passare solo il traffico necessario, per esempio dal sistema di supervisione del cliente verso la CPU e sulle sole porte usate. Può essere un modulo di comunicazione con firewall integrato, come la CP 1243-1 per S7-1200 o la CP 1543-1 per S7-1500, oppure un router o firewall industriale nel quadro, come la famiglia SCALANCE S di Siemens o equivalenti di altri produttori.
- **Protezione d'accesso della CPU attiva,** con password e con il livello di accesso minimo necessario per pannelli e supervisione.
- **Servizi non necessari disattivati,** a partire dal web server della CPU se non serve.
- **Teleassistenza solo attraverso il router di macchina,** abilitata da un selettore sul quadro.
- **Misure scritte nella valutazione dei rischi:** quali accorgimenti hai adottato e perché.

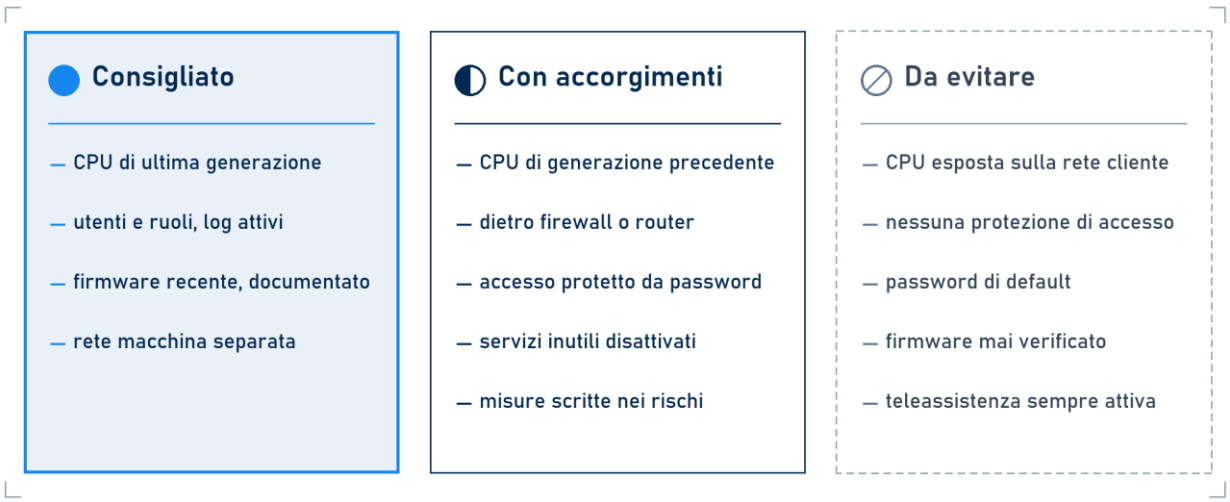


FIG. 2 Scelta della CPU: consigliato, con accorgimenti, da evitare.

1.7 Cosa ne ricava chi progetta

L'esempio parte dal PLC, ma la lezione riguarda allo stesso modo chi disegna l'impianto elettrico e chi scrive il software: le scelte giuste si fanno insieme, in fase di offerta e di progetto, non alla messa in servizio.

Se sei un progettista elettrico

- In distinta materiali indica la CPU con famiglia, generazione e versione firmware, non solo “un PLC”.
- Prevedi nel quadro spazio, alimentazione e cablaggio per firewall, router di macchina o modulo di comunicazione aggiuntivo.
- Decidi già nello schema quale interfaccia va alla rete della macchina e quale verso il cliente.
- Prevedi il selettore per abilitare la teleassistenza sul fronte quadro.
- Inserisci questi componenti nell'offerta: aggiungerli a macchina finita costa di più.

Se sei un programmatore PLC

- Prima di iniziare verifica che CPU, firmware e versione di TIA Portal supportino utenti, ruoli e registrazione degli eventi, e attivali.
- Imposta la protezione d'accesso e disattiva i servizi e le comunicazioni che la macchina non usa.
- Concorda l'architettura di rete con il progettista elettrico prima di assegnare indirizzi e collegamenti.
- Compila la tabella delle versioni installate, da consegnare con la documentazione.

La scelta del PLC è solo il primo tassello. Da sola non rende sicura una macchina, ma condiziona tutto quello che viene dopo: la rete, la teleassistenza, il quadro e la documentazione che consegnerai. Nella guida completa li mettiamo insieme, uno alla volta.

1.8 Una domanda da porsi subito: e la PUT/GET?

DOMANDA APERTA · PUT/GET

Se lavori con Siemens la conosci di sicuro: l'accesso PUT/GET è una delle funzioni più usate in assoluto, perché permette a pannelli, sistemi di supervisione e software di terze parti di leggere e scrivere direttamente nei DB del PLC.

Proprio per questo può diventare una vulnerabilità: chi riesce a raggiungere la CPU in rete può accedere ai suoi dati.

Va disattivata sempre? Si può continuare a usarla in modo sicuro? E cosa rispondi al cliente quando il suo sistema di supervisione la richiede? **Lo vediamo nella guida completa.**

1.9 Nel resto della guida

Con lo stesso metodo affrontiamo la rete della macchina, la teleassistenza, il quadro e gli accessi fisici, la documentazione di consegna e le risposte da dare ai clienti, con esempi presi dal campo e una checklist da usare prima di ogni consegna.

FINE DELL'ESTRATTO

Continua nella guida completa →

store.mind-ware.eu/cybersecurity-macchine

Mindware SRL
mind-ware.eu