

Cybersecurity OT tra NIS2, CRA e Regolamento Macchine



Parola di Cyber Ladies

Micaela Caserza Magro

Cybersecurity OT tra NIS2, CRA e Regolamento Macchine

Cosa fare oggi, con quali norme, in attesa degli standard armonizzati

A cura di Micaela Caserza Magro

Cyber security OT: dove ci troviamo?

Se nel 2026 fai il responsabile di automazione, costruisci macchine o gestisci un impianto industriale, permettimi una battuta: hai scelto un momento decisamente movimentato per farlo. Fino a pochi anni fa questo mondo era fatto di analisi dei rischi meccanici, marcature CE, manuali d'uso e, se andava bene, qualche firewall messo lì “perché non si sa mai”. Oggi ci troviamo di fronte a tre corpi normativi europei che convergono contemporaneamente sullo stesso oggetto: i sistemi di automazione e tutto quello che afferisce a questo mondo; in più tutto il trio per la prima volta tratta l'attacco informatico come un evento che può avere conseguenze reali, fisiche, sulle persone, sugli impianti e sulla produzione. Non è una moda passeggera né l'ennesimo adempimento burocratico da spuntare: è un cambio di paradigma che porta la cybersecurity dal reparto IT al reparto di produzione, e lo fa con tempistiche già scritte nel calendario.

I tre protagonisti di questa rivoluzione sono il Regolamento Macchine (UE) 2023/1230, il Cyber Resilience Act (CRA) e la direttiva NIS2 (UE) 2022/2555, recepita in Italia con il D.Lgs. 138/2024. Non sono tre alternative tra cui scegliere: sono tre lenti diverse puntate sullo stesso impianto, e capire chi deve fare cosa — e con quali strumenti tecnici — è il primo passo per non ritrovarsi a rincorrere le scadenze nell'ultimo trimestre utile, come sta già succedendo a molte organizzazioni italiane sul fronte NIS2. Da qui in avanti l'articolo lascia da parte i toni scherzosi e prova a mettere ordine tra chi è tenuto a fare cosa e con quali strumenti tecnici concreti.

Chi deve seguire cosa

Una delle fonti di confusione più frequenti, quando si parla di questi tre regolamenti nello stesso convegno, è dimenticare che si rivolgono ad attori diversi della filiera industriale, con obblighi diversi anche quando l'oggetto fisico di riferimento è lo stesso sistema di automazione, nella definizione che ne dà la normativa IEC. Distinguere questi ruoli non è un esercizio accademico: determina concretamente chi deve produrre quale documentazione, chi risponde in caso di ispezione e, soprattutto, quali norme tecniche vanno effettivamente applicate.

Il Regolamento Macchine si rivolge principalmente al fabbricante di macchine e di “prodotti correlati”, vale a dire attrezzature intercambiabili, componenti di sicurezza, accessori di sollevamento, catene, funi e cinghie e dispositivi amovibili di trasmissione meccanica. Chi progetta, costruisce e immette sul mercato una macchina è tenuto a valutarne i rischi complessivi, inclusi quelli originati da attacchi informatici che possano compromettere una funzione di sicurezza, e a documentare tutto questo nel

fascicolo tecnico che accompagna la dichiarazione di conformità e la marcatura CE. Il regolamento entrerà in applicazione il 20 gennaio 2027, ma il suo perimetro soggettivo è più ampio di quanto sembri a prima vista: riguarda anche chi apporta una “modifica sostanziale” a una macchina esistente, includendo esplicitamente le modifiche realizzate con mezzi digitali — una novità rispetto al passato, pensata proprio per intercettare gli interventi di retrofit digitale sempre più diffusi negli impianti. Chi effettua una modifica sostanziale diventa a tutti gli effetti il fabbricante della macchina modificata, con gli stessi obblighi di chi l'ha costruita da zero: nuova analisi dei rischi, nuovo fascicolo tecnico, nuova dichiarazione di conformità. Questo aspetto tocca da vicino i system integrator, che intervengono proprio in questa veste ogni volta che assemblano linee complesse integrando macchine di fornitori diversi, aggiungono un sistema di supervisione o modificano sostanzialmente la logica di controllo di un impianto esistente.

Il CRA guarda invece a un oggetto diverso: il prodotto con elementi digitali in quanto tale, indipendentemente dal fatto che sia o meno parte di una macchina. Un firewall industriale, un modulo di comunicazione wireless, un sistema di gestione di rete sono “prodotti” ai sensi del CRA anche quando vengono venduti come componenti destinati all'integrazione in impianti terzi, e chi li fabbrica e li immette sul mercato deve garantirne la sicurezza fin dalla fase di progettazione, gestirne le vulnerabilità per l'intero ciclo di vita utile — non solo al momento della vendita — e notificare exploit attivi e incidenti gravi alle autorità competenti. Il CRA è entrato in vigore il 10 dicembre 2024 e sarà pienamente applicabile dall'11 dicembre 2027, ma alcuni obblighi, in particolare quelli di notifica delle vulnerabilità sfruttate attivamente, decorrono da scadenze anticipate rispetto alla piena applicazione. I destinatari principali di questo regolamento sono i fabbricanti di componenti e sistemi digitali per l'automazione — non gli utilizzatori finali degli impianti, che qui restano sostanzialmente fuori dal perimetro degli obblighi diretti, pur beneficiando indirettamente di prodotti più sicuri.

La NIS2, infine, cambia completamente prospettiva: non regola il prodotto, ma l'organizzazione che lo utilizza. Si rivolge ai soggetti essenziali e importanti individuati in diciotto settori critici — tra cui la manifattura, con l'inclusione di numerosi comparti industriali che fino a poco tempo fa non si sentivano toccati da normative di cybersecurity e che oggi si ritrovano, spesso con sorpresa, nel perimetro applicativo del decreto. Quando un'azienda è un asset owner, un gestore di impianto o un operatore che utilizza sistemi di controllo industriale per erogare un servizio o produrre un bene in uno di questi settori, gli obblighi ricadono sull'organizzazione nel suo complesso e, in modo esplicito, sul suo consiglio di amministrazione: l'articolo 23 del decreto italiano stabilisce una responsabilità diretta degli amministratori sull'approvazione e la supervisione delle misure di gestione del rischio, con obblighi di formazione specifica e conseguenze personali in caso di inadempienza.

Il punto interessante — e la ragione per cui vale la pena leggere questi tre testi insieme piuttosto che in compartimenti stagni, come spesso accade nei percorsi di formazione settoriali — è che lo stesso identico apparato fisico può ricadere sotto più di un regime contemporaneamente, a seconda della fase del suo ciclo di vita e di chi lo sta maneggiando in quel momento. Un router industriale è un prodotto CRA quando esce dalla fabbrica del costruttore, diventa parte del fascicolo tecnico di una macchina quando un system integrator lo installa e lo configura all'interno di una linea, e contribuisce infine alla postura di rischio complessiva che un asset owner soggetto a NIS2 deve gestire, monitorare

e dimostrare quando quella linea entra in produzione e comincia a generare, gestire e trasmettere dati operativi.

Gli obblighi di alto livello: cosa chiede davvero ciascun testo

Spogliati del linguaggio giuridico, gli obblighi sostanziali dei tre regimi si possono riassumere in tre logiche piuttosto diverse tra loro, anche se tutte convergono verso lo stesso obiettivo finale: ridurre la probabilità che un attacco informatico si traduca in un danno, sia esso fisico, economico o reputazionale.

Il Regolamento Macchine chiede che il rischio cyber venga integrato nell'analisi dei rischi complessiva della macchina, secondo la stessa metodologia già familiare a chi si occupa di sicurezza funzionale. È però fondamentale un chiarimento che genera spesso equivoci anche tra addetti ai lavori: il regolamento considera il rischio cyber solo nella misura in cui un attacco informatico possa degradare una funzione di sicurezza e quindi mettere concretamente a rischio l'incolumità delle persone. Non si tratta, in altre parole, di un requisito generale di protezione della riservatezza o della disponibilità dei dati aziendali, che restano fuori dal perimetro di questo specifico regolamento e vengono invece indirizzati da altri strumenti normativi. Un attacco che rallenti una rete di ufficio senza toccare la logica di sicurezza della macchina, per quanto dannoso dal punto di vista del business, non rientra nell'ambito di applicazione di questo requisito essenziale. Oltre alla valutazione del rischio cyber, il Regolamento chiede anche che la macchina ed i suoi sistemi di sicurezza siano protetti contro la manomissione e l'alterazione, quindi chiede anche di selezionare delle contromisure adeguate al rischio e di valutarne l'efficacia.

Il CRA, al contrario, chiede un impegno molto più ampio e trasversale, che copre l'intero ciclo di vita del prodotto anziché limitarsi alle sole implicazioni di sicurezza fisica. I pilastri sono quattro: una progettazione sicura fin dall'inizio, secondo i principi di security by design e security by default su cui torneremo tra poco; una gestione strutturata delle vulnerabilità per tutta la vita utile del prodotto, non solo nella fase immediatamente successiva al lancio commerciale; la disponibilità di aggiornamenti di sicurezza per un periodo di supporto dichiarato e proporzionato al prodotto; e infine canali di segnalazione strutturati verso ENISA e i CSIRT nazionali, attivabili entro tempistiche molto strette quando viene rilevato lo sfruttamento attivo di una vulnerabilità.

La NIS2, infine, chiede un sistema di gestione del rischio cyber a tutto tondo, che nel decreto italiano viene articolato in dieci aree tematiche indicate dall'articolo 24: dall'analisi dei rischi alla gestione degli incidenti, dalla continuità operativa e dal disaster recovery alla sicurezza della catena di approvvigionamento, fino alla crittografia, al controllo degli accessi e alla formazione del personale. A questo impianto organizzativo si affiancano tempistiche di notifica degli incidenti molto stringenti verso l'ACN e un regime sanzionatorio che, per la prima volta nel diritto europeo in materia di cybersecurity, prevede conseguenze dirette e personali per gli organi di amministrazione, oltre alle sanzioni pecuniarie che possono arrivare fino a dieci milioni di euro o a una percentuale del fatturato globale.

Detto questo, tre testi di legge non bastano da soli a far funzionare nulla: dicono cosa bisogna ottenere, non come arrivarci in pratica. Ed è esattamente qui che entrano in gioco le norme tecniche.

Le implicazioni di sicurezza per il software

C'è un cambiamento specifico, meno pubblicizzato rispetto ai grandi principi generali ma con conseguenze molto concrete sul lavoro quotidiano di chi sviluppa software industriale, ed è il modo in cui sia il Regolamento Macchine sia il CRA trattano ora il software non più come un accessorio della macchina o del prodotto, ma come oggetto di regolazione a sé stante.

Il Regolamento (UE) 2023/1230 introduce, rispetto alla precedente direttiva 2006/42/CE, una novità che merita di essere sottolineata con precisione: nella definizione di “componente di sicurezza” rientrano ora esplicitamente anche i componenti digitali, software compreso. Sotto la vecchia direttiva macchine, un componente di sicurezza era pensato quasi esclusivamente in termini di hardware — un relè di sicurezza, un finecorsa, una barriera fotoelettrica — e il software veniva considerato al più come parte integrante di un sistema più ampio, raramente come oggetto autonomo di valutazione della conformità. Il nuovo regolamento cambia questa impostazione: se un software viene immesso sul mercato separatamente, con la funzione dichiarata di garantire una funzione di sicurezza — si pensi a un modulo software per un PLC di sicurezza, a una libreria di monitoraggio del moto sicuro, o a un blocco funzionale destinato a essere integrato nella logica di sicurezza di più macchine diverse — quel software è a tutti gli effetti un componente di sicurezza ai sensi dell'articolo 3 e dell'elenco indicativo dell'Allegato II, e come tale deve seguire la propria procedura di valutazione della conformità, ottenere la marcatura CE ed essere accompagnato dalla relativa documentazione tecnica, esattamente come accadrebbe per un componente fisico. Questo cambiamento si accompagna a un'altra novità dell'Allegato I, l'elenco delle categorie ad alto rischio soggette alle procedure di valutazione più rigorose: vi rientrano ora anche i componenti di sicurezza con comportamento totalmente o parzialmente auto-evolutivo, ossia quelli che utilizzano approcci di apprendimento automatico per garantire una funzione di sicurezza, e le macchine che integrano sistemi con questo stesso tipo di comportamento. Per chi sviluppa software di sicurezza destinato a più applicazioni questo significa dover pianificare fin da subito un percorso di conformità autonomo per il software stesso, e non limitarsi a considerarlo assorbito nella valutazione dei rischi della macchina finale in cui verrà installato. E poter definire che il software è sicuro implica automaticamente di avere anche per il software una security by design ed una security by default.

Il CRA affronta il tema del software da un'angolazione diversa e complementare: non tanto come componente di sicurezza da certificare, quanto come oggetto di tracciabilità e trasparenza lungo tutta la catena di fornitura. Il regolamento include esplicitamente il software tra i “prodotti con elementi digitali” che rientrano nel suo perimetro, tanto quello incorporato in un dispositivo fisico quanto quello distribuito come prodotto autonomo, e impone un obbligo che per il mondo OT rappresenta probabilmente il cambiamento più immediato da mettere in pratica: la predisposizione di un elenco strutturato dei componenti software del prodotto, il cosiddetto Software Bill of Materials o SBOM, richiesto dall'Allegato I, Parte II, punto 1 del regolamento. Questo elenco deve coprire almeno le

dipendenze di primo livello, essere prodotto in un formato leggibile da un sistema informatico e comunemente utilizzato — nella pratica gli standard di riferimento sono SPDX e CycloneDX, anche se il CRA stesso non impone un formato specifico e la Commissione non ha ancora adottato l'atto di esecuzione previsto dall'articolo 13 per definirne il contenuto in modo vincolante — e deve essere mantenuto aggiornato all'interno della documentazione tecnica del prodotto. È importante chiarire un punto spesso frainteso: l'SBOM non è un documento che il fabbricante deve pubblicare o rendere disponibile al pubblico, ma un elemento della documentazione tecnica che le autorità di vigilanza del mercato possono richiedere con motivazione specifica, quando necessario per verificare la conformità ai requisiti essenziali di cybersecurity.

Per il mondo dell'automazione industriale, dove firmware di gateway, sistemi HMI, sistemi SCADA e persino il firmware di dispositivi da campo si appoggiano ormai pesantemente a componenti open source — kernel Linux, stack di protocollo per Modbus o OPC-UA, librerie crittografiche condivise — l'obbligo di SBOM porta alla luce una superficie di rischio che fino ad oggi restava in larga parte invisibile: quando una vulnerabilità critica viene scoperta in una libreria open source ampiamente diffusa, un fabbricante senza una SBOM accurata non ha modo di sapere, se non con un'indagine manuale spesso lunga e incompleta, quali dei propri prodotti la utilizzano e quindi quali necessitano di un intervento urgente. Su questo fronte il CRA introduce anche una figura nuova, quella dell'open source steward prevista dall'articolo 24: si tratta di persone giuridiche — non individui, e non semplici manutentori occasionali — che offrono un supporto continuativo allo sviluppo di software libero e open source destinato a un uso commerciale, e per le quali il regolamento prevede un regime di obblighi più leggero rispetto a quello del fabbricante, incluse alcune esenzioni dalle sanzioni per il mancato rispetto di specifiche scadenze di segnalazione. È però essenziale non fraintendere la portata di questa distinzione: se un'azienda integra un componente open source all'interno di un proprio prodotto industriale destinato alla vendita commerciale, resta pienamente responsabile ai sensi del CRA per l'intero prodotto, incluso il componente open source integrato, indipendentemente dal fatto che il progetto open source di origine sia gestito da uno steward soggetto a un regime più leggero. L'uso di componenti open source, in altre parole, non trasferisce né riduce la responsabilità regolatoria del fabbricante che li incorpora in un prodotto commerciale.

Cosa significano davvero security by design e security by default

Prima di entrare nel merito delle norme tecniche vale la pena spendere qualche riga su due espressioni che compaiono ormai in ogni testo normativo europeo sulla cybersecurity — CRA compreso — ma che vengono spesso citate senza essere davvero spiegate, con il rischio che restino slogan piuttosto che requisiti operativi.

Security by design, sicurezza fin dalla progettazione, significa che le contromisure di sicurezza non vengono aggiunte a un prodotto già progettato, come una patch o un accessorio opzionale acquistabile a parte, ma vengono considerate come vincolo di progettazione fin dalle primissime fasi dello sviluppo, insieme ai requisiti funzionali, di costo e di prestazione. In pratica, questo significa condurre un'analisi delle minacce e della superficie di attacco prima ancora di scegliere l'architettura hardware e software

del prodotto, definire fin dall'inizio quali interfacce di comunicazione sono strettamente necessarie ed eliminare quelle superflue, scegliere protocolli e librerie crittografiche robuste anziché implementazioni proprietarie non verificate, e strutturare il codice secondo principi di minimizzazione dei privilegi e di separazione dei componenti critici da quelli non critici. Nella pratica industriale, questo si traduce ad esempio nella scelta di disabilitare di default i protocolli di comunicazione non sicuri già in fase di progetto del firmware, invece di lasciarli attivi “per compatibilità” e demandare all'integratore o all'utilizzatore finale il compito di disattivarli in un secondo momento — compito che, l'esperienza lo dimostra ampiamente, viene quasi sempre disatteso.

Security by default, sicurezza per impostazione predefinita, è un concetto complementare ma distinto: riguarda non tanto il modo in cui il prodotto viene progettato, quanto la configurazione con cui viene consegnato all'utilizzatore finale al primo avvio, prima di qualsiasi intervento di configurazione da parte sua. Un prodotto sicuro by default arriva con le funzionalità non necessarie disattivate, con credenziali di accesso che non sono uguali per ogni esemplare della stessa serie e che obbligano l'utente a un cambio password al primo utilizzo, con le porte di comunicazione non essenziali chiuse e con la configurazione più restrittiva possibile compatibile con il funzionamento di base, lasciando all'utilizzatore la scelta consapevole di allargare i permessi o le funzionalità, anziché il contrario. È esattamente l'inverso di una pratica ancora oggi molto diffusa nel mondo OT, dove numerosi dispositivi di automazione vengono ancora consegnati con credenziali amministrative standard, documentate pubblicamente nei manuali tecnici e mai cambiate una volta installate sul campo — una delle cause più ricorrenti di incidente riscontrate nelle analisi post-attacco su ambienti industriali.

Il motivo per cui il CRA insiste su entrambi i concetti, e non solo su uno dei due, è che rispondono a due momenti diversi della vita di un prodotto e a due responsabilità diverse: la progettazione sicura riguarda le scelte tecniche del fabbricante durante lo sviluppo, mentre la configurazione sicura di default riguarda ciò che l'utilizzatore riceve nelle mani. Un prodotto può essere progettato in modo ineccepibile e poi essere reso vulnerabile da una configurazione di fabbrica permissiva; viceversa, una configurazione di default prudente non compensa scelte architetture insicure a monte. Entrambi i requisiti, non a caso, ritroveranno spazio esplicito nel catalogo di controlli tecnici della futura EN 40000-1-4, ma sono già oggi principi applicabili — e verificabili in sede di audit — indipendentemente dalla pubblicazione della norma armonizzata.

Dalla legge alla pratica: il ruolo delle norme tecniche armonizzate

Per il Regolamento Macchine e per il CRA il meccanismo di raccordo tra legge e pratica tecnica è quello classico del Nuovo Approccio europeo alla regolamentazione dei prodotti: rispettare una norma armonizzata, pubblicata con riferimento in Gazzetta Ufficiale dell'Unione Europea, dà una presunzione di conformità ai requisiti essenziali corrispondenti, semplificando enormemente il compito del fabbricante nella predisposizione della documentazione tecnica e nel dialogo con gli organismi notificati. Per la NIS2 il meccanismo è strutturalmente diverso: non esiste una presunzione di conformità legata a una norma tecnica specifica, perché la direttiva non segue lo schema del Nuovo Approccio ma quello, più discrezionale, della gestione del rischio proporzionata al contesto. Ciò

nonostante, nella pratica le organizzazioni si trovano comunque a dover scegliere un framework tecnico di riferimento per dimostrare, anche solo in sede di autovalutazione o di ispezione ACN, che le misure adottate sono adeguate e proporzionate; e per l'ambito OT quel framework, di fatto, è quasi sempre la IEC 62443.

Il problema, ad agosto 2026, è che le norme armonizzate specifiche per CRA e Regolamento Macchine non esistono ancora, nemmeno nelle loro parti più avanzate. Non è un dettaglio secondario, perché significa che chi deve dimostrare oggi la propria conformità non può appoggiarsi a un elenco pubblicato in Gazzetta Ufficiale: deve costruire un percorso di conformità diretta rispetto ai requisiti essenziali del regolamento, motivando le proprie scelte tecniche con riferimento agli strumenti normativi più maturi effettivamente disponibili sul mercato.

Per il CRA, il lavoro di normazione affidato dalla Commissione Europea a CEN, CENELEC ed ETSI attraverso il mandato M/606 comprende circa quarantuno norme armonizzate complessive, suddivise in una componente orizzontale e in diverse componenti verticali dedicate a specifiche categorie di prodotto. La parte orizzontale, che si applica trasversalmente a quasi tutti i prodotti con elementi digitali indipendentemente dalla loro destinazione, prende forma nella famiglia EN 40000, sviluppata dal gruppo di lavoro WG9 del comitato tecnico congiunto CLC/JTC 13 e costruita esplicitamente sopra la serie EN 18031, norma nata a suo tempo nel contesto della Radio Equipment Directive e ora estesa e rafforzata per coprire il perimetro molto più ampio del CRA. All'interno di questa famiglia, la parte dedicata al processo e al ciclo di vita del prodotto (EN 40000-1-2) e quella dedicata alla gestione delle vulnerabilità (EN 40000-1-3) sono le più avanzate nell'iter di approvazione, mentre il vero e proprio catalogo dei requisiti tecnici generici — la EN 40000-1-4, che tradurrà in controlli concreti e verificabili i tredici sotto-requisiti elencati nell'Allegato I, Parte I, punto 2, lettere da a) a m) del regolamento — ha un orizzonte di pubblicazione decisamente più lungo, con un obiettivo indicato per l'autunno 2027, a ridosso della piena applicazione del CRA. Accanto alla famiglia orizzontale, la serie prEN 50770 copre invece specificamente le categorie di prodotto di rete elencate nell'Allegato III del regolamento, quelle considerate a maggior criticità: firewall e sistemi di rilevamento e prevenzione delle intrusioni, sistemi di gestione di rete, prodotti per reti private virtuali, router e switch. Questa serie verticale si appoggia in modo esplicito all'impianto concettuale della IEC 62443, sebbene non sia scontato che le singole parti della norma internazionale vengano citate come tali nel testo finale pubblicato in Gazzetta Ufficiale. Una proposta di emendamento della Commissione, pubblicata a luglio 2026, ha peraltro già spostato in avanti di circa due mesi le scadenze originariamente previste dal mandato di normazione, segno che il percorso, per quanto reale e concretamente avanzato, resta soggetto a un'evoluzione ancora fluida: al momento in cui scrivo, nessuna norma armonizzata del CRA risulta ancora pubblicata con riferimento in Gazzetta Ufficiale, e di conseguenza la presunzione di conformità prevista dall'articolo 27 del regolamento non è ancora invocabile da alcun fabbricante.

Per il Regolamento Macchine, il lavoro corrispondente è affidato al gruppo di lavoro WG02 del comitato tecnico CLC/TC 44X, attualmente impegnato nell'elaborazione della norma EN 50742, intitolata "Safety of Machinery – Electrotechnical aspects – Protection against corruption", basata sulla specifica tecnica IEC TS 63074 già pubblicata a livello internazionale. Questa futura norma è pensata per conferire presunzione di conformità rispetto ai requisiti essenziali di sicurezza e salute 1.1.9 e 1.2.1,

lettere a) ed f), del Regolamento (UE) 2023/1230, ovvero quelli relativi specificamente alla protezione dei sistemi di comando dalla corruzione — deliberata, nel caso di un attacco intenzionale, o accidentale, nel caso di un guasto o di un errore — che possa degradare le funzioni di sicurezza della macchina. Anche in questo caso ci troviamo nella fase di elaborazione del progetto di norma, non ancora in quella di pubblicazione ufficiale: il riferimento tecnico oggi concretamente disponibile resta quindi la specifica IEC TS 63074, non ancora convertita in norma armonizzata europea.

Per la NIS2, come già accennato, non esiste un percorso di norma armonizzata in senso proprio. In Italia il D.Lgs. 138/2024 demanda all'ACN il compito di rendere operative le misure di sicurezza richieste attraverso determinazioni tecniche periodiche — la prima, datata 14 aprile 2025, ha definito le misure di sicurezza di base e i criteri di notifica applicabili a soggetti essenziali e importanti.

Perché, in mezzo a tutto questo, la IEC 62443 resta il punto fermo

C'è un filo che tiene insieme tutta questa architettura normativa ancora incompleta, ed è la IEC 62443. Non è un caso: sia la famiglia prEN 50770 sia la EN 50742 nascono come applicazioni, a categorie di prodotto specifiche, di concetti che la IEC 62443 ha già formalizzato da anni con un dettaglio tecnico che nessun altro standard internazionale offre nello stesso modo per l'ambito dell'automazione industriale. Tra questi concetti rientrano la segmentazione della rete in zone e condotti descritta dalla parte 3-3, i livelli di sicurezza — i cosiddetti security level, una scala graduata che permette di calibrare le contromisure sul rischio effettivo anziché applicare un unico standard indifferenziato a ogni asset — i requisiti tecnici per i singoli componenti definiti dalla parte 4-2 e il processo di sviluppo sicuro descritto dalla parte 4-1, che è poi la stessa logica di security by design di cui si è parlato in precedenza, tradotta in pratiche verificabili passo per passo.

La struttura stessa della norma internazionale, articolata per attore della filiera — fabbricante di componenti e sistemi nelle parti 4-1 e 4-2, integratore di sistema nelle parti 3-2 e 3-3, gestore o asset owner nelle parti 2-1 e 2-4 — è esattamente ciò che serve per allocare correttamente le responsabilità lungo la catena costruttore-integratore-operatore che tutti e tre i regimi normativi europei, seppure con enfasi e linguaggi diversi, presuppongono e richiedono implicitamente.

Questo non significa che ogni singola parte della IEC 62443 diventerà, prima o poi, una norma armonizzata a tutti gli effetti. Alcune parti più procedurali e organizzative, come la 2-1 dedicata al programma di sicurezza dell'asset owner, resteranno probabilmente riferimenti di buona pratica riconosciuti dal mercato più che requisiti direttamente verificabili in sede di marcatura CE. Le parti più tecniche e misurabili — in particolare la 3-3, la 4-1 e la 4-2 — sono invece già oggi, prima ancora che le rispettive norme armonizzate vengano formalmente pubblicate, lo strumento più solido e più difendibile a disposizione di chi deve costruire un percorso di conformità credibile e documentabile.

Cosa fare da subito, senza aspettare la Gazzetta Ufficiale

L'assenza delle norme armonizzate non è un alibi per rimandare: gli obblighi essenziali di CRA, Regolamento Macchine e NIS2 sono già vigenti, o lo saranno a scadenze ormai vicine, indipendentemente dalla disponibilità futura della presunzione di conformità. Chi gestisce un impianto e ricade sotto la NIS2 può fin da ora utilizzare la IEC 62443-2-1 per mappare il proprio programma di sicurezza rispetto alle dieci aree richieste dall'articolo 24 del decreto italiano, e la segmentazione in zone e condotti della IEC 62443-3-2 per ridisegnare l'architettura di rete OT/IT in modo coerente con quanto le determinazioni ACN già richiedono operativamente. Chi costruisce componenti o sistemi di automazione destinati, un giorno, a rientrare nella prEN 50770 può appoggiarsi già oggi alla IEC 62443-4-2 per i requisiti tecnici di prodotto e alla 4-1 per strutturare il processo di sviluppo sicuro: è la strada più vicina a ciò che la futura norma armonizzata richiederà, e riduce in modo significativo il lavoro da rifare quando la presunzione di conformità diventerà finalmente disponibile. Chi costruisce macchine può integrare fin da subito la valutazione dei rischi cyber nell'analisi dei rischi meccanica complessiva — la versione 2025 della ISO 12100 va proprio in questa direzione, rendendo la valutazione del rischio cyber parte integrante del processo anziché un allegato facoltativo — utilizzando la IEC TS 63074 e i livelli di sicurezza della IEC 62443-3-3 come riferimento tecnico per le funzioni di sicurezza effettivamente coinvolte, anche prima che la EN 50742 venga pubblicata. Su un fronte trasversale a tutti e tre i regimi normativi, infine, vale la pena costruire fin da ora processi solidi di gestione delle vulnerabilità e di notifica, appoggiandosi alla pratica di security management descritta dalla IEC 62443-4-1: è l'area normativa più matura nell'iter di approvazione del CRA ed è già, allo stesso tempo, un obbligo pienamente vigente per i soggetti NIS2, il che significa che ogni investimento fatto in questa direzione lavora contemporaneamente su due tavoli regolatori distinti.

Il filo conduttore, in definitiva, è che documentare oggi il proprio percorso di conformità con il linguaggio e la struttura della IEC 62443 — inventario degli asset, valutazione del rischio, livello di sicurezza target confrontato con quello effettivamente raggiunto, evidenze di verifica raccolte e conservate nel tempo — non è un esercizio prematuro né un rischio da evitare in attesa di indicazioni più definitive. È, molto semplicemente, imparare in anticipo la lingua tecnica che le norme armonizzate parleranno non appena verranno pubblicate, e arrivare pronti al momento in cui quella pubblicazione, finalmente, arriverà.