QUADRA
Consulenza e Formazione

Protezione dall'alterazione: tra cyber security e safety

Ernesto Cappelletti

10 giugno 2025

Quadra s.r.l. | **www.quadrasrl.net**
via Mazzini, 32/A – Cornate d'Adda (MB)
Tel. 0396060383 | 0396060351

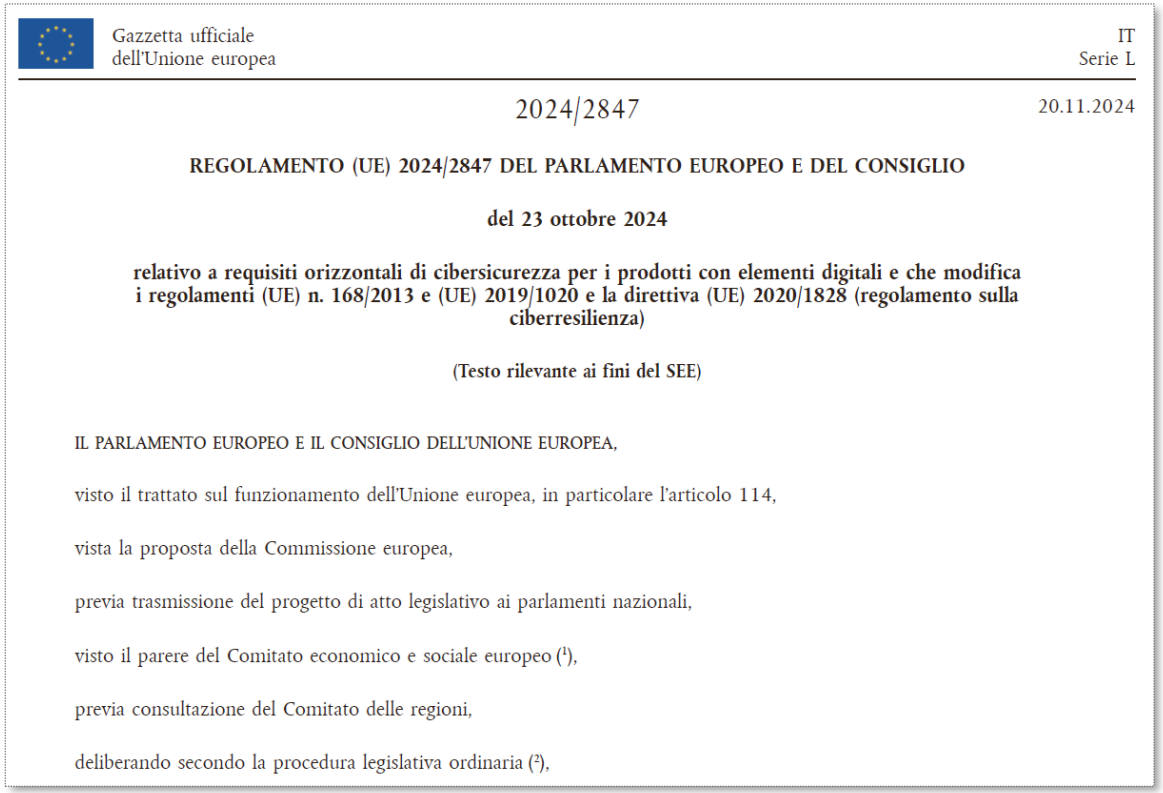
Cibersicurezza per i prodotti con elementi digitali (ciberresilienza)

Regolamento (UE) 2024/2847

Ambito di applicazione e requisiti

Regolamento (UE) 2024/2847 (articolo 2 e articolo 6)

- Il regolamento (UE) 2024/2847 si applica ai **prodotti con elementi digitali** messi a disposizione sul mercato la cui finalità prevista o il cui utilizzo ragionevolmente prevedibile include una **connessione dati logica o fisica diretta o indiretta a un dispositivo o a una rete**.
- I prodotti con elementi digitali devono **soddisfare i requisiti di cibersicurezza** relativi alle proprietà dei prodotti con elementi digitali (allegato I, parte I).
- I fabbricanti devono mettere in atto **processi per la gestione delle vulnerabilità** (allegato I, parte II).



Gazzetta ufficiale dell'Unione europea — IT Serie L

2024/2847 — 20.11.2024

REGOLAMENTO (UE) 2024/2847 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

del 23 ottobre 2024

relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica i regolamenti (UE) n. 168/2013 e (UE) 2019/1020 e la direttiva (UE) 2020/1828 (regolamento sulla ciberresilienza)

(Testo rilevante ai fini del SEE)

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 114,

vista la proposta della Commissione europea,

previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,

visto il parere del Comitato economico e sociale europeo ([1]),

previa consultazione del Comitato delle regioni,

deliberando secondo la procedura legislativa ordinaria ([2]),

Prodotti rientranti nel regolamento (UE) 2023/1230

Regolamento (UE) 2024/2847 (considerando 53)

- I prodotti con elementi digitali che rientrano nel campo di applicazione del regolamento (UE) 2023/1230 devono **rispettare i requisiti di entrambi i regolamenti**.
  - *I fabbricanti di prodotti che rientrano nell'ambito di applicazione del regolamento (UE) 2023/1230 del Parlamento europeo e del Consiglio […] che sono anche prodotti con elementi digitali come definiti nel presente regolamento dovrebbero rispettare sia i requisiti essenziali di cui al presente regolamento sia i requisiti essenziali di cibersicurezza di cui al presente regolamento e di tutela della salute di cui al regolamento (UE) 2023/1230. […] La conformità ai requisiti essenziali di cibersicurezza di cui al presente regolamento potrebbe pertanto* ***facilitare la conformità ai requisiti essenziali*** *che coprono anche determinati rischi di cibersicurezza* ***di cui al regolamento (UE) 2023/1230****, in particolare quelli riguardanti la protezione contro la corruzione e la sicurezza e l'affidabilità dei sistemi di controllo di cui all'allegato III, sezioni 1.1.9 e 1.2.1, di tale regolamento.*

Obblighi dei fabbricanti

Regolamento (UE) 2024/2847 (articolo 13)

- Se viene individuata una **vulnerabilità** in un **componente integrato** nel prodotto con elementi digitali i fabbricanti:
  - **segnalano la vulnerabilità** al soggetto che si occupa della fabbricazione o della manutenzione del componente;
  - **correggono la vulnerabilità** conformemente ai requisiti di gestione delle vulnerabilità di cui all'allegato I, parte II;
  - qualora abbiano sviluppato una **modifica del software o dell'hardware** per affrontare la vulnerabilità di tale componente, **condividono** il codice o la documentazione pertinenti con il soggetto che si occupa della fabbricazione o della manutenzione del componente, se del caso in un formato leggibile da un dispositivo automatico.
- I fabbricanti determinano il **periodo di assistenza** in modo che rifletta la **durata di utilizzo prevista del prodotto** con elementi digitali e garantiscono che le **vulnerabilità** del prodotto con elementi digitali, compresi i suoi componenti, siano **gestite in modo efficace** durante il periodo di assistenza.
- Il periodo di assistenza è di **almeno cinque anni** o pari alla durata di utilizzo prevista se inferiore a cinque anni.

Obblighi dei fabbricanti

Regolamento (UE) 2024/2847 (articolo 13)

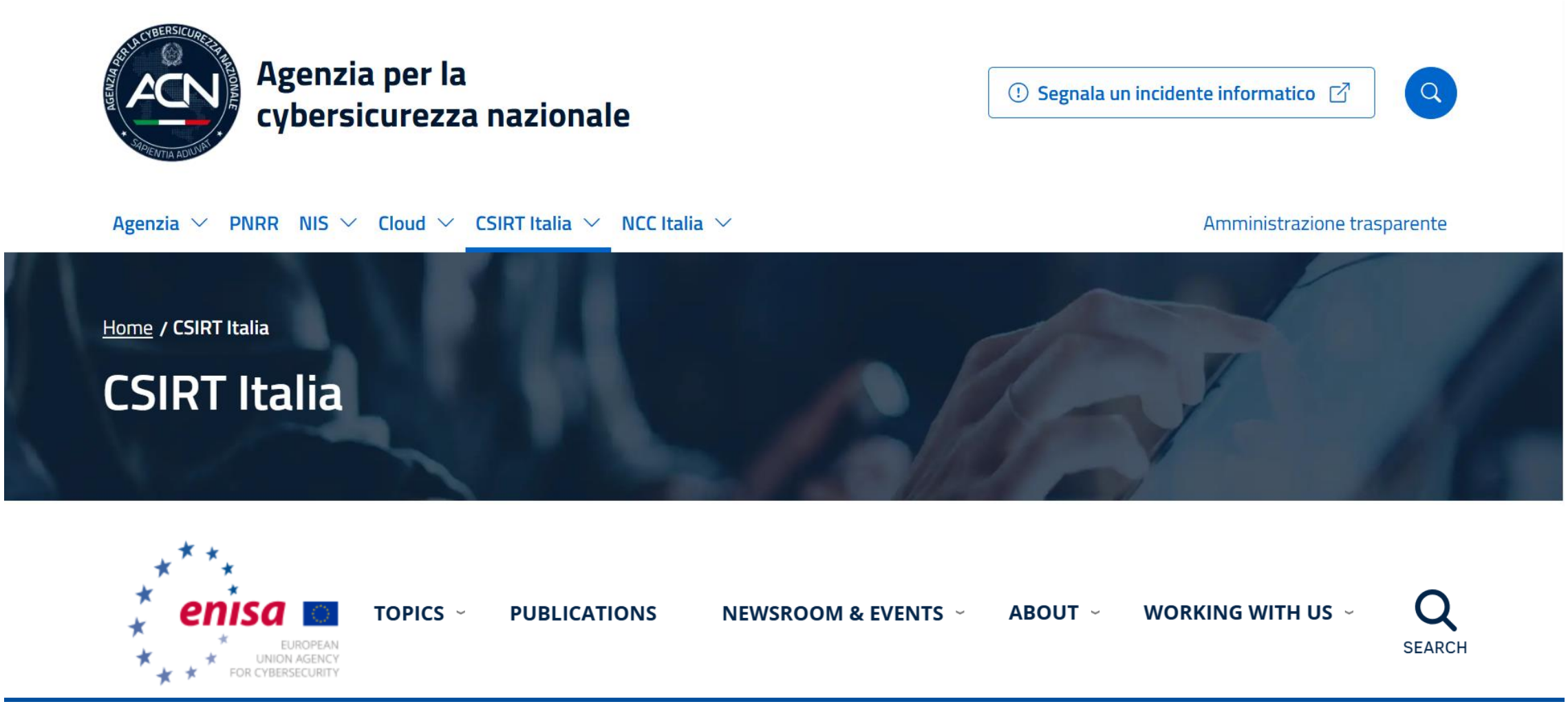
- Prima di immettere un prodotto con elementi digitali sul mercato i fabbricanti:
  - redigono la **documentazione tecnica**;
  - eseguono o fanno eseguire le **procedure di valutazione della conformità**;
  - redigono la **dichiarazione di conformità UE**;
  - appongono la **marcatura CE**.
- I prodotti con elementi digitali devono essere accompagnati dalle informazioni e dalle **istruzioni per l'utilizzatore**:
  - in **forma cartacea o elettronica**;
  - redatte in una **lingua facilmente comprensibile** dagli utilizzatori e dalle autorità di vigilanza del mercato;
  - se fornite online, devono essere **accessibili**, di facile uso e **disponibili online** per un periodo di almeno **dieci anni** dalla data di immissione sul mercato del prodotto o per il **periodo di assistenza**, se quest'ultimo è superiore.

Obblighi di segnalazione dei fabbricanti
Regolamento (UE) 2024/2847 (articolo 14)

- I fabbricanti **notificano simultaneamente** all'ENISA e al CSIRT designato come coordinatore dello Stato membro in cui hanno lo stabilimento principale nell'Unione europea:
  - qualsiasi **vulnerabilità attivamente sfruttata** contenuta nel prodotto con elementi digitali di cui vengono a conoscenza;
  - qualsiasi **incidente grave** che abbia un impatto sulla sicurezza del prodotto di cui viene a conoscenza.
- Le segnalazioni avvengono tramite la **piattaforma unica di segnalazione** istituita a norma dell'articolo 16 del regolamento (UE) 2024/2847 e devono essere:
  - una **notifica di preallarme** entro 24 ore dal momento in cui il fabbricante ne è venuto a conoscenza;
  - una **notifica delle vulnerabilità o dell'incidente** entro 72 ore dal momento in cui il fabbricante ne è venuto a conoscenza;
  - una **relazione finale**:
    - entro 14 giorni dalla messa a disposizione di una misura correttiva o di attenuazione della vulnerabilità attivamente sfruttata;
    - entro un mese dalla trasmissione della notifica di incidente.

ENISA e CSIRT Italia

Siti internet



Sanzioni

Regolamento (UE) 2024/2847 (articolo 64)

- Le sanzioni sono **fissate dagli Stati membri** e devono essere effettive, proporzionate e dissuasive.
- Non conformità ai **requisiti essenziali** di cibersicurezza e agli **obblighi dei fabbricanti** e agli obblighi di **segnalazione** dei fabbricanti:
  - sanzioni amministrative pecuniarie fino a € 15.000.000 o, se l'autore del reato è un'impresa, fino al 2,5% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.
- Non conformità agli obblighi dei **rappresentanti autorizzati**, degli **importatori**, dei **distributori**, della persona che apporta una **modifica sostanziale** a un prodotto con elementi digitali, della **dichiarazione di conformità** UE, della **marcatura CE**, della **documentazione tecnica**, delle **procedure di valutazione della conformità**:
  - sanzioni amministrative pecuniarie fino a € 10.000.000 o, se l'autore del reato è un'impresa, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.
- Fornitura di **informazioni inesatte, incomplete o fuorvianti** agli organismi notificati e alle autorità di vigilanza del mercato:
  - sanzioni amministrative pecuniarie fino a € 5.000.000 o, se l'autore del reato è un'impresa, fino all'1% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

Disposizioni transitorie, entrata in vigore e applicazione

Regolamento (UE) 2024/2847 (articoli 69 e 71)

- Il regolamento (UE) 2024/2847 **si applica** a partire dall'**11 dicembre 2027**.
- L'articolo 14 (**obblighi di segnalazione dei fabbricanti**) si applica a decorrere dall'**11 settembre 2026**.
- Il capo IV (notifica degli organismi di valutazione della conformità) si applica a decorrere dall'11 giugno 2026.
- I prodotti con elementi digitali **immessi sul mercato prima dell'11 dicembre 2027** sono soggetti ai requisiti stabiliti nel regolamento (UE) 2024/2847 solo se, a decorrere da tale data, tali prodotti sono **soggetti a una modifica sostanziale**.
- Gli obblighi di cui all'articolo 14 (**obblighi di segnalazione dei fabbricanti**) **si applicano a tutti i prodotti** con elementi digitali che rientrano nell'ambito di applicazione del regolamento (UE) 2024/2847 e **che sono stati immessi sul mercato prima dell'11 dicembre 2027**.

Requisiti essenziali di sicurezza e di tutela della salute

Regolamento (UE) 2023/1230

Rischi provocati da attacchi informatici

Regolamento (UE) 2023/1230 (considerando 25)

- I rischi provocati da **attacchi informatici** devono essere tenuti in considerazione **solamente** per gli aspetti che incidono sulla **sicurezza delle macchine**.
  - *(25) Altri rischi relativi a nuove tecnologie digitali sono quelli provocati da **terzi malintenzionati** che **incidono sulla sicurezza** dei prodotti rientranti nell'ambito di applicazione del presente regolamento. A tale proposito i fabbricanti dovrebbero essere tenuti ad adottare **misure proporzionate che si limitano alla protezione della sicurezza dei prodotti** rientranti nell'ambito di applicazione del presente regolamento. Ciò **non preclude** l'applicazione ai prodotti rientranti nell'ambito di applicazione del presente regolamento di **altri atti giuridici** dell'Unione che affrontano specificamente aspetti di **cibersicurezza**.*

Protezione dall'alterazione

Regolamento (UE) 2023/1230 (allegato III, §1.1.9)

- Il **collegamento** alla macchina **di un altro dispositivo** non deve determinare una situazione pericolosa.
- I **componenti hardware** che permettono l'**accesso al software legato alla sicurezza** devono essere **protetti da alterazioni** accidentali o intenzionali.
- La macchina deve **raccogliere prove** in merito a **interventi legittimi o illegittimi** su tali componenti.
  - *La macchina o il prodotto correlato devono essere progettati e costruiti in modo tale da fare sì che il **collegamento ad essi di un altro dispositivo**, tramite qualsiasi caratteristica del dispositivo connesso stesso o tramite qualsiasi **dispositivo remoto** che comunica con la macchina o il prodotto correlato, non determini una situazione pericolosa.*
  - *I **componenti hardware che trasmettono segnali o dati**, importanti per il collegamento o l'accesso a software che sono fondamentali affinché la macchina o il prodotto correlato rispettino i pertinenti requisiti essenziali di sicurezza e di tutela della salute, devono essere progettati in modo tale da essere adeguatamente **protetti da un'alterazione accidentale o intenzionale**.*
  - *La macchina o il prodotto correlato devono **raccogliere prove in merito a un intervento legittimo o illegittimo** su tali componenti hardware, se importante per il collegamento o l'accesso al software critico per la conformità della macchina o del prodotto correlato.*

Protezione dall’alterazione

Regolamento (UE) 2023/1230 (allegato III, §1.1.9)

- Software e dati critici per la sicurezza devono essere individuati come tali e **protetti da alterazioni** accidentali o intenzionali.
- **Informazioni** su questi software devono essere **facilmente disponibili** in qualsiasi momento.
- La macchina deve **raccogliere prove** in merito a **interventi legittimi o illegittimi** su tali software.
  - ***Software e dati critici*** *per il rispetto da parte della macchina o del prodotto correlato dei pertinenti requisiti essenziali di sicurezza e di tutela della salute devono essere* ***individuati come tali*** *e devono essere adeguatamente* ***protetti da un’alterazione accidentale o intenzionale****.*
  - *La macchina o il prodotto correlato devono* ***individuare il software installato sullo stesso****, necessario per il suo funzionamento in condizioni di sicurezza, e devono essere in grado di* ***fornire tali informazioni in qualsiasi momento*** *in un formato facilmente accessibile.*
  - *La macchina o il prodotto correlato devono* ***raccogliere prove di un intervento legittimo o illegittimo sul software*** *o di una modifica del software installato sulla macchina o sul prodotto correlato o della sua configurazione.*

Sicurezza ed affidabilità dei sistemi di comando
Regolamento (UE) 2023/1230 (allegato III, §1.2.1)

- I sistemi di comando devono resistere a **influssi esterni intenzionali** o meno, compresi **tentativi deliberati ragionevolmente prevedibili da parte di terzi** che generano situazioni pericolose.
- Per dimostrare la conformità della macchina alle autorità nazionali competenti deve essere tenuta traccia **per 5 anni** delle **versioni del software di sicurezza** caricato sulla macchina.
  - *I sistemi di comando devono essere progettati e costruiti in modo tale che:*
    - *a) riescano a resistere, se del caso, a circostanze e rischi, a previste sollecitazioni di servizio e ad **influssi esterni intenzionali o meno**, compresi **tentativi deliberati ragionevolmente prevedibili da parte di terzi** che conducono a una situazione pericolosa;*
    - *[…]*
    - *f) la **registrazione di tracciamento** dei dati generati in relazione a un intervento e delle **versioni del software di sicurezza** caricato dopo l'immissione sul mercato o la messa in servizio della macchina o del prodotto correlato sia consentita **per cinque anni** dopo tale caricamento, esclusivamente al fine di dimostrare la conformità della macchina o del prodotto correlato rispetto al presente allegato **a fronte di una richiesta** motivata da parte **di un'autorità nazionale competente**.*

Disposizioni transitorie e finali

Regolamento (UE) 2023/1230 (articoli 51, 52 e 54) e rettifica del 4 luglio 2023

- Il regolamento (UE) 2023/1230 **verrà applicato** a partire dal **20 gennaio 2027**.
- La direttiva 2006/42/CE sarà **abrogata** a decorrere dal **20 gennaio 2027**.
- **Non sarà possibile emettere dichiarazioni** di conformità UE o dichiarazioni di incorporazione UE ai sensi del regolamento (UE) 2023/1230 prima del 20 gennaio 2027.
- È possibile immettere sul mercato prodotti conformi alla direttiva 2006/42/CE prima del 20 gennaio 2027.
- Fino al 19 gennaio 2027 i prodotti dovranno essere **dichiarati conformi alla direttiva 2006/42/CE**.

La normazione sulla sicurezza informatica delle macchine

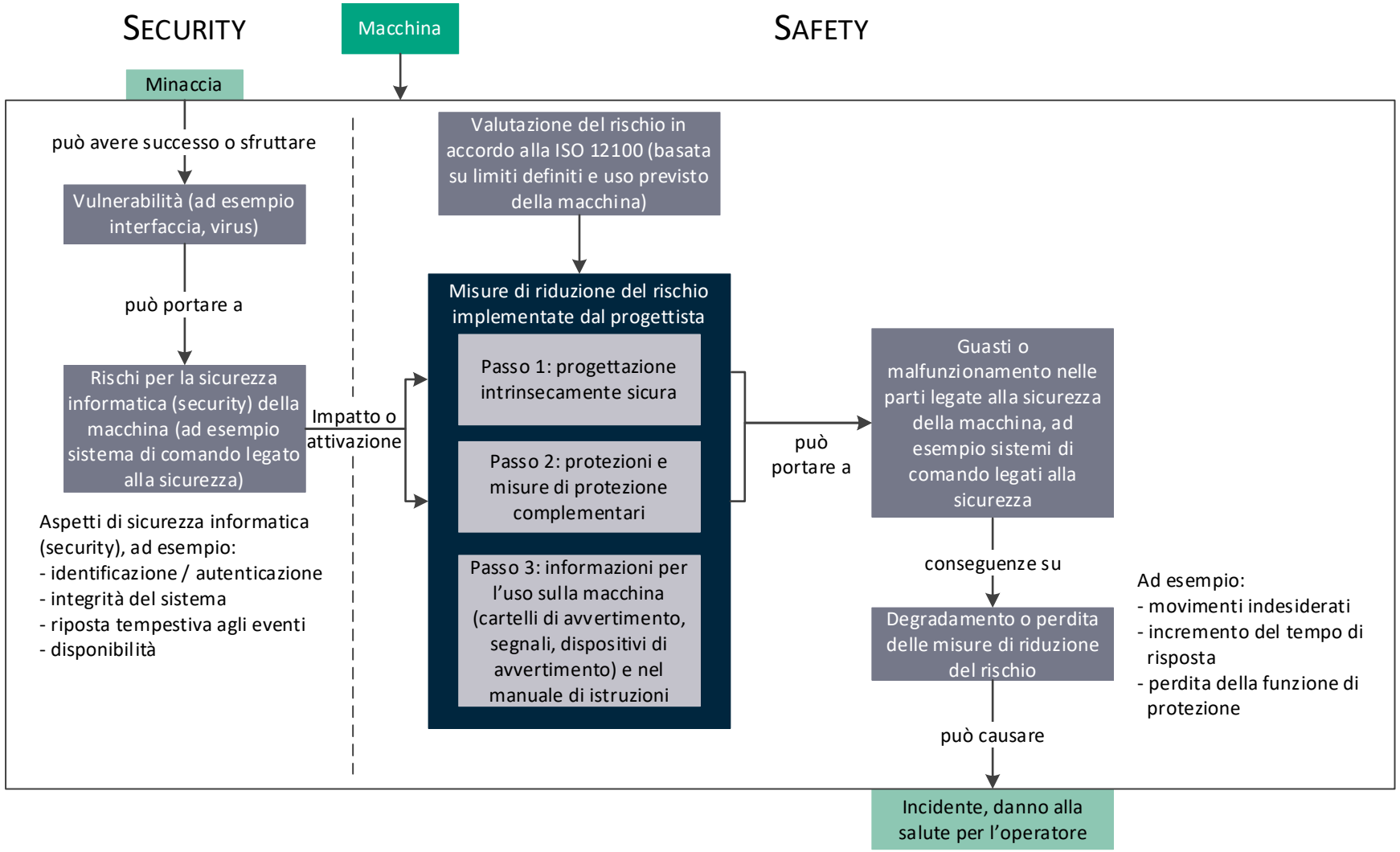
UNI CEN ISO/TR 22100-4:2021

Relazione tra security e safety
UNI CEN ISO/TR 22100-4:2021 (§6)

- La **valutazione del rischio** per una macchina secondo **UNI EN ISO 12100:2010** deve essere **effettuata prima** di qualsiasi considerazione relativa alla sicurezza informatica.
- Le risultanti:
  - misure di progettazione intrinsecamente sicure e
  - misure di salvaguardia e riduzione del rischio

  di una macchina dovrebbe quindi essere analizzate rispetto alle possibili vulnerabilità contro le minacce alla sicurezza informatica.
- Il termine paragonabile a “mitigazione del rischio” è il termine “riduzione del rischio” utilizzato nella sicurezza delle macchine.
- L’accesso non autorizzato ad un sistema informatico può anche comportare **conseguenze non volute dall’attaccante**.

Relazione tra security e safety
UNI CEN ISO/TR 22100-4:2021 (§6)



Caratteristiche degli attacchi informatici

- I metodi di **attacco informatico evolvono in continuazione**, quindi non è possibile per il fabbricante della macchina assicurare che non sia vulnerabile solamente per mezzo delle misure di cui la macchina è dotata al momento della sua messa in servizio.
- Le **misure di protezione** contro gli attacchi informatici della macchina **devono evolvere** per tutto il ciclo di vita della macchina.
- Queste misure di protezione devono comprendere **componenti hardware e software**.

Parti coinvolte
UNI CEN ISO/TR 22100-4:2021 (§7)

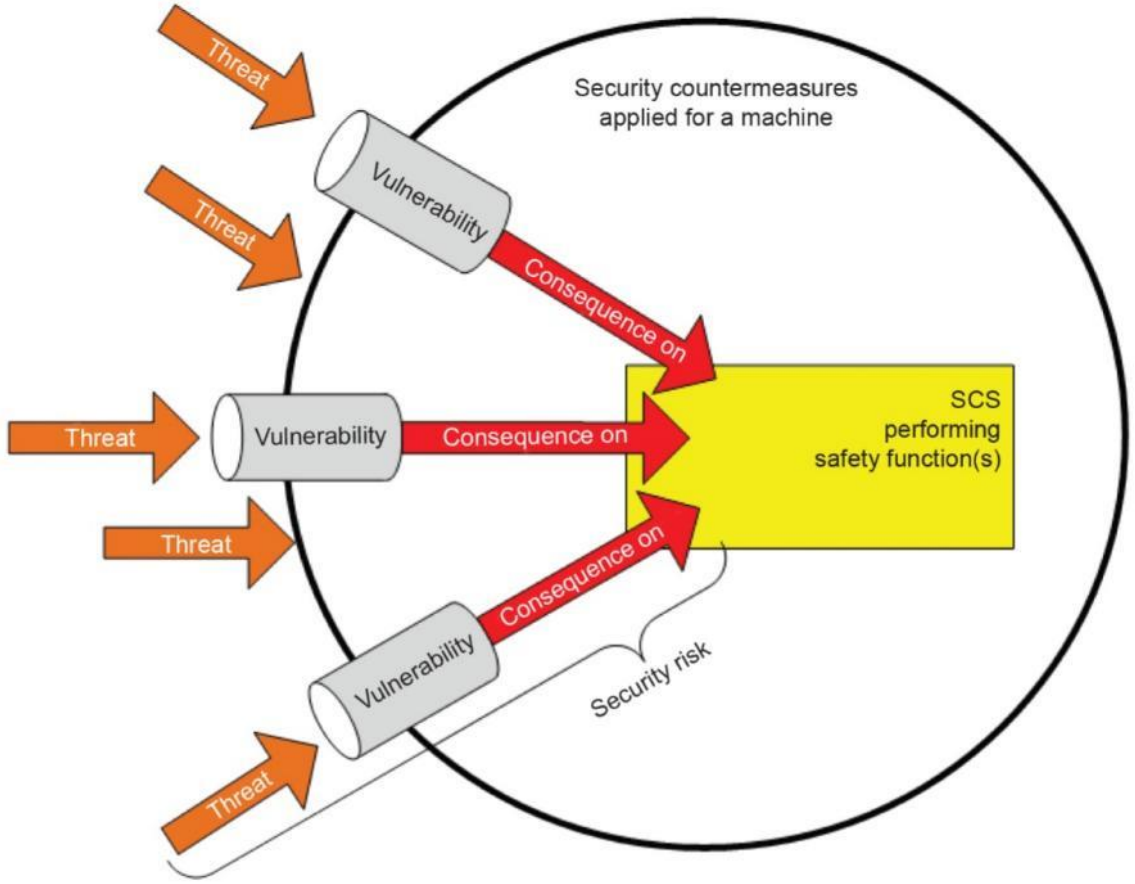
- Le minacce e le vulnerabilità della sicurezza informatica richiedono la cooperazione ed il coordinamento tra i fornitori di componenti, il fabbricante della macchina, l'integratore di sistema e l'utilizzatore.
- Nessuna parte può assumere che un'altra parte sia totalmente responsabile della sicurezza informatica.
- Allo stesso tempo, nessuna delle parti ha a disposizione tutte le informazioni necessarie per affrontare efficacemente le minacce e le vulnerabilità della sicurezza informatica durante le fasi del ciclo di vita della macchina.
- Parte della valutazione dovrebbe includere la comunicazione alle altre parti delle minacce e delle vulnerabilità che non possono affrontare completamente da sole o che hanno implicazioni per le altre parti.
- A seconda degli accordi contrattuali tra le parti, l'attribuzione dei ruoli alle singole parti potrebbe essere diversa.

La normazione sulla sicurezza informatica delle macchine

CEI CLC/IEC/TS 63074:2024

Obiettivi della sicurezza informatica
CEI CLC/IEC/TS 63074:2024 (§4)

- Una **valutazione dei rischi** per la sicurezza informatica si basa su un prodotto o sistema nel suo ambiente in cui vengono identificate **minacce** e **vulnerabilità note**.
- Lo scopo di questa attività è di **definire contromisure** di sicurezza informatica pertinenti applicate a una macchina per soddisfare gli obiettivi di sicurezza informatica generali.
- Nel contesto della sicurezza delle macchine, le contromisure di sicurezza informatica sono tese a proteggere la capacità di **mantenere un funzionamento sicuro** di una macchina e la loro implementazione non deve **influire negativamente** su alcuna **funzione di sicurezza**.



Contromisure di sicurezza informatica contro l’alterazione
CEI CLC/IEC/TS 63074:2024 (§6.3)

- **Autenticazione a più fattori**: ad esempio, utilizzando differenti percorsi di trasmissione oppure trasmettendo i fattori di autenticazione in tempi separati sullo stesso percorso di trasmissione.
- **Architettura di rete**: ad esempio, **dividendo la rete** in zone o segmentandola con **firewall**.
- **Dispositivi portatili**: dove per i dispositivi portatili si utilizzino comunicazioni relative alla sicurezza è opportuno applicare contromisure di sicurezza informatica quali l’autenticazione a più fattori.
- **Comunicazioni wireless**: è indispensabile la **modifica delle password standard** con altre di lunghezza sufficiente; la **distanza di copertura** della comunicazione wireless non dovrebbe essere più lunga del necessario; laddove si utilizzi una comunicazione correlata alla sicurezza, si devono prendere in considerazione contromisure di sicurezza, ad esempio utilizzando la **crittografia** o l’autenticazione a più fattori.

Contromisure di sicurezza informatica contro l'alterazione

CEI CLC/IEC/TS 63074:2024 (§6.3)

- **Accesso da remoto**: possono essere implementate contromisure di sicurezza quali una connessione tramite rete privata virtuale (**VPN**), la **crittografia** end-to-end, la **disabilitazione** della connessione dopo un **intervallo di tempo** predefinito, la **conferma locale** della **modifica dei parametri** legati alla sicurezza.
- Attacco tramite **connessione fisica diretta**: esempi di mezzi che possono essere sfruttati sono una **scheda SD**, una **porta USB**, una porta di rete; le porte inutilizzate del sistema di controllo della macchina (ad esempio porte USB, porte di rete, ecc.) devono essere **disabilitate** per ridurre al minimo la possibilità di accesso non autorizzato.

La futura normazione sulla sicurezza informatica delle macchine

prEN 50742:2025

Nuovo progetto di norma ‘Protection against corruption’

prEN 50742

CENELEC

TC44X/Sec0362/INF
February 2024

EUROPEAN COMMITTEE FOR ELECTROTECHNICAL STANDARDISATION
TECHNICAL COMMITTEE 44X – SAFETY OF MACHINERY – ELECTROTECHNICAL ASPECTS

Announcement of
Establishment of a New Working Group under CLC/TC 44X
titled ‘Protection against corruption’
& Call for Experts

Dear Members,

We are pleased to inform you that, following a **Decision (D2024/007)** taken at the CLC/TC 44X Plenary held on 5 February 2024 in Milan, Italy (TC44X/Sec0360/DL), **a new working group WG02 titled ‘Protection against corruption’ has now been established to develop a new homegrown work item prEN 50742.**

With this circular, we are calling for nomination of experts from all our members to join this new Working Group, CLC/TC 44X WG2.

QUADRA
Consulenza e Formazione

Grazie per l'attenzione

Ernesto Cappelletti

Quadra s.r.l. | **www.quadrasrl.net**
via Mazzini, 32/A – Cornate d'Adda (MB)
Tel. 0396060383 | 0396060351