UNI/PdR XXX:2026	Linee di indirizzo per la protezione dall'alterazione dei sistemi informatici delle macchine *Guidelines for the protection of computer systems of machines from tampering*
Sommario	La Prassi di Riferimento fornisce linee di indirizzo per la protezione dall'alterazione dei sistemi informatici dei prodotti che può incidere sulla sicurezza dei prodotti stessi. In tale contesto, il documento definisce un approccio metodologico strutturato per l'analisi delle vulnerabilità che possono essere sfruttate dalle minacce, individuando, dove necessario, misure di mitigazione adeguate e coerenti con lo stato dell'arte, al fine di garantire un livello di sicurezza accettabile per il contesto in cui il prodotto è destinato ad essere utilizzato. Le minacce informatiche che interessano nell'ambito della presente trattazione sono quelle che possono generare rischi di lesioni o danno alle persone.
Data	26-01-2026

Avvertenza

Il presente documento è un progetto di Prassi di Rifermento (UNI/PdR) sottoposta alla fase di consultazione, da utilizzare solo ed esclusivamente per fini informativi e per la formulazione di commenti.

Il processo di elaborazione delle Prassi di Riferimento prevede che i progetti vengano sottoposti alla consultazione sul sito web UNI per raccogliere i commenti del mercato: la UNI/PdR definitiva potrebbe quindi presentare differenze rispetto al documento messo in consultazione.

Questo documento perde qualsiasi valore al termine della consultazione, cioè il: 28 febbraio 2026.

UNI non è responsabile delle conseguenze che possono derivare dall'uso improprio del testo dei progetti di Prassi di Riferimento in consultazione.

Via Sannio 2 – 20137 Milano
Telefono 02 700241
www.uni.com – uni@uni.com

PREMESSA

La prassi di riferimento UNI/PdR XXX:2026 non è una norma nazionale, ma è un documento pubblicato da UNI, come previsto dal Regolamento (UE) n. 1025/2012, che raccoglie prescrizioni relative a prassi condivise all'interno del seguente soggetto firmatario di un accordo di collaborazione con UNI:

FEDERMACCHINE

Federazione nazionale delle associazioni dei produttori di beni strumentali e loro accessori destinati allo svolgimento di processi manifatturieri dell'industria e dell'artigianato

Via Fulvio Testi, 128 – 20092 Cinisello Balsamo (MI)

La presente prassi di riferimento è stata elaborata dal Tavolo "Linea guida sulla cybersafety applicabile al settore delle macchine" condotto da UNI, costituito dai seguenti esperti:

Ugo Gecchelin – Project Leader (Team 4.0 Srl)

Enrico Annacondia (FEDERMACCHINE)

Alvise Biffi (Probest Service SpA)

Alessio Bolognesi (FEDERUNACOMA)

Ernesto Cappelletti (Quadra Srl)

Giorgio Caramori (Studio Legale)

Nicodemo De Amicis (IMQ SpA)

Emanuele De Francesco (UCIMU – SISTEMI PER PRODURRE)

Vincenzo Delacqua (ICIM SpA)

Luciano di Donato (INAIL)

Fabio Guasconi (Risc3 Srl)

Luca Landi (Università degli Studi di Perugia)

Matteo Marconi (A.C.& E. Srl)

Francesca Merighi (SACMI Group)

Giuliano Rosati (Team 4.0 Srl)

SOMMARIO

0 INTRODUZIONE

L'evoluzione digitale dei macchinari industriali apre nuove opportunità in termini di efficienza, produttività e integrazione nelle macchine interconnesse con i sistemi informatici aziendali[1]. Tuttavia, questa trasformazione comporta anche significative implicazioni di sicurezza, legate in particolare alla cibersicurezza, oggi riconosciuta come componente imprescindibile della sicurezza generale dei macchinari.

Con l'adozione crescente di tecnologie digitali e la connessione in rete dei macchinari, il rischio legato alla sicurezza informatica diventa un fattore critico da considerare nella progettazione, produzione e utilizzo dei macchinari. L'interazione uomo-macchina, la dipendenza da software, la connessione a sistemi remoti o cloud e la potenziale esposizione a minacce esterne – come accessi non autorizzati o malware – richiedono un approccio ampliato alla gestione del rischio.

È quindi essenziale individuare e valutare tempestivamente i rischi legati alla cibersicurezza industriale, integrandoli nel processo di valutazione dei rischi già previsto dalla Direttiva Macchine [2] e, prossimamente, dal Regolamento (UE) 2023/1230 [3].

Il Regolamento (UE) 2023/1230 [3] cita i Requisiti Essenziali di Salute e Sicurezza (RESS) per prodotti, considerando la protezione dall'alterazione dei sistemi informatici al fine di non compromettere la sicurezza (safety). Vengono stabiliti obblighi specifici per gli operatori economici, considerando sia la progettazione sicura di hardware e software, che la gestione delle vulnerabilità, tracciabilità delle modifiche, che la conformità a norme armonizzate.

In Appendice A (informativa) sono riportate opportune considerazioni su RESS e Cibersicurezza nel Regolamento (UE) 2023/1230 [3] per la protezione dall'alterazione dei sistemi informatici.

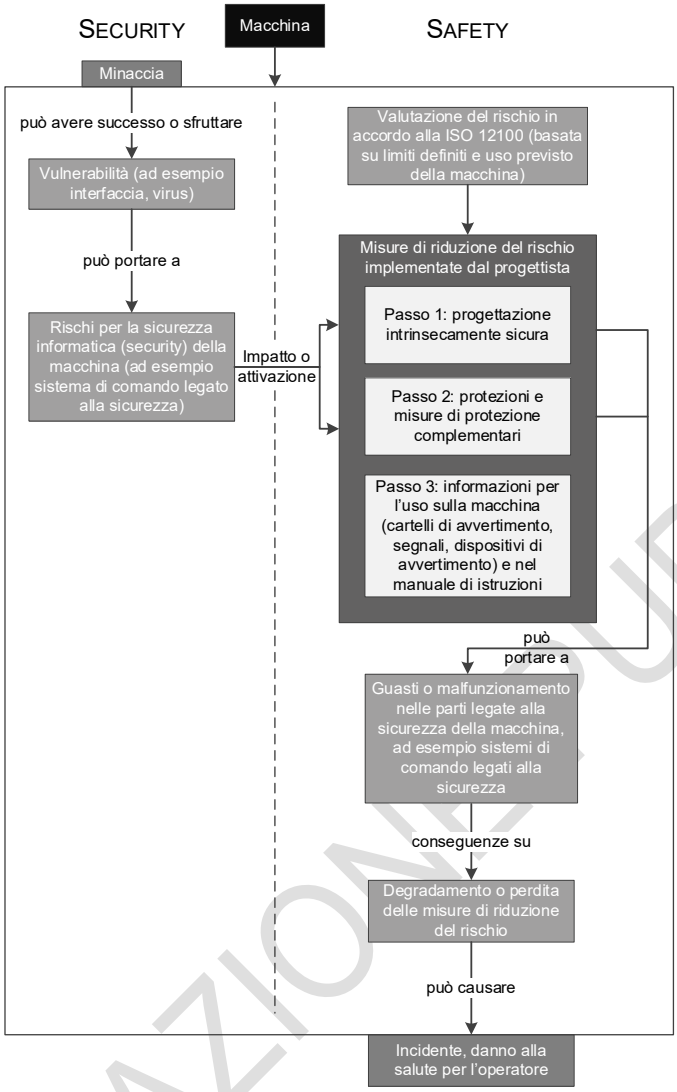
Ciò implica l'integrazione tra sicurezza funzionale e protezione dall'alterazione dei sistemi informatici, per garantire che anche anomalie legate alla "dimensione informatica" non possano compromettere la sicurezza degli operatori (vedere figura 1).

La relazione tra gli aspetti di safety e di security è basata sul principio secondo cui una macchina è dotata di adeguate misure di protezione e le contromisure di security applicate a una macchina devono essere tali da evitare il degrado delle prestazioni delle misure di protezione che implementano le funzioni di sicurezza (safety), inclusi i dati legati alla sicurezza.

Nota: vedere anche il punto 4.1 della CEI CLC/IEC/TS 63074:2024

[1] Per maggiori informazioni, vedere la Circolare 4/E del 30 marzo 2017 dell'Agenzia delle Entrate e del Ministero dello Sviluppo Economico [1] e la UNI/TR 11749:2020.

Figura 1: Relazione tra security e safety (UNI CEN ISO/TR 22100-4:2021, figura 3)



I sistemi di automazione e controllo industriale (cosiddetti IACS) utilizzano sempre più dispositivi commerciali, direttamente connessi in rete, economici, efficienti, altamente automatizzati e facilmente integrabili con protocolli di largo impiego pronti all'uso.

I sistemi di controllo del prodotto sono inoltre sempre più interconnessi con reti aziendali non IACS per ragioni aziendali. L'insieme di questi dispositivi e delle reti interconnesse offrono una crescente opportunità di attacco informatico verso il sistema hardware/software IACS, che può portare a perdite delle funzioni di sicurezza implementate sul prodotto.

In questa prassi di riferimento l'analisi si ferma alle vulnerabilità che, se sfruttate accidentalmente od intenzionalmente, portano a possibili riduzioni nel soddisfacimento dei RESS di un prodotto e quindi ad un aggravio del rischio per l'utilizzatore finale. In genere, ogni risorsa degli IACS o collegata agli IACS può essere bersaglio di attacco informatico, ma non tutti gli attacchi informatici portano alle condizioni descritte sopra in quanto sono mirate, ad esempio, al furto di informazioni che non sono oggetto di questa prassi di riferimento.

Nota: le tecnologie senza fili (wireless) per la comunicazione bidirezionale sono utilizzate spesso dai sensori introdotti dal paradigma 4.0, il tipico protocollo Wi-Fi (IEC 802.11 e successive modifiche) è stato affiancato nelle tecnologie abilitanti da altri protocolli, ad esempio Bluetooth, Zigbee ed MQTT che permettono differenti tipi di infrastrutture di rete e collegamento multiplo dei dispositivi.

Affrontare queste sfide richiede un approccio multidisciplinare, che combini competenze tecniche, legali, informatiche e di gestione del rischio.

È pertanto necessario fornire indicazioni concrete e aggiornate ai fabbricanti di macchinari, affinché progettino e realizzino prodotti dotati di misure tecniche idonee a contrastare le minacce digitali. Allo stesso tempo, è fondamentale informare gli utilizzatori dei macchinari circa i nuovi obblighi derivanti dalla digitalizzazione, affinché possano adottare misure coerenti in termini di organizzazione, manutenzione e formazione del personale.

In tale prospettiva, FEDERMACCHINE ha assunto un ruolo di primo piano promuovendo la redazione della Prassi di Riferimento, sviluppata in collaborazione con UNI e con il contributo di primari esperti del settore, al fine di fornire un quadro metodologico e operativo per valutare e gestire i rischi di natura informatica durante l'intero ciclo di vita del macchinario, promuovendo un allineamento con le migliori pratiche internazionali.

Viene così nuovamente sottolineato il ruolo fondamentale di FEDERMACCHINE, svolto attraverso la Prassi di Riferimento e determinante per promuovere e garantire standard elevati di qualità, sicurezza dei macchinari e tutela della salute e sicurezza sul posto di lavoro.

1 SCOPO E CAMPO DI APPLICAZIONE

La Prassi di Riferimento fornisce linee di indirizzo per la protezione dall'alterazione dei sistemi informatici dei prodotti[2] che può incidere sulla sicurezza dei prodotti stessi.

In tale contesto, il documento definisce un approccio metodologico strutturato per l'analisi delle vulnerabilità che possono essere sfruttate dalle minacce, individuando, dove necessario, misure di mitigazione adeguate e coerenti con lo stato dell'arte, al fine di garantire un livello di sicurezza accettabile per il contesto in cui il prodotto è destinato ad essere utilizzato. Le minacce informatiche che interessano nell'ambito della presente trattazione sono quelle che possono generare rischi di lesioni o danno alle persone.

2 RIFERIMENTI NORMATIVI

Nel presente documento non ci sono riferimenti normativi.

3 TERMINI, DEFINIZIONI E ACRONIMI

3.1 GENERALI

3.1.1 **Attacco**: Tentativo di ottenere un accesso non autorizzato ai servizi di un sistema, risorse o informazioni

[UNI CEN ISO/TR 22100-4:2021, punto 3.2]

3.1.2 **Cibersicurezza**: Insieme delle attività necessarie per proteggere rete e sistemi informatici, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche.

Nota 1: traduzione letterale in italiano di "cyber security"

Nota 2: Le azioni di cibersicurezza, pertanto, hanno quale obiettivo l'individuazione e la mitigazione delle "minacce informatiche".

3.1.3 **Codice portabile**: programma trasferito da un sistema remoto, potenzialmente "non attendibile", attraverso una rete o tramite un supporto rimovibile che può essere eseguito

[2] Alla data di pubblicazione, è in vigore la Direttiva Macchine 2006/42/CE [2], che sarà sostituita dal Regolamento Macchine (UE) 2023/1230 [3]. La prassi di riferimento non prende in considerazione i requisiti del Regolamento (UE) 2024/2847 [6] e il Cybersecurity Act (Regolamento (UE) 2019/881) [4].

senza modifiche su un sistema locale senza installazione o esecuzione esplicita da parte del destinatario.

Nota: esempi di codice portabile includono JavaScript, VBScript, applet Java, controlli ActiveX, animazioni Flash, filmati Shockwave e macro di Microsoft Office.

[CEI EN IEC 62443-3-3:2020, punto 3.1.32]

3.1.4 **Condotto:** Raggruppamento logico di canali di comunicazione, che collegano due o più zone, che condividono requisiti comuni di sicurezza.

Nota: ad un condotto è consentito attraversare una zona purché sia garantito che la sicurezza dei canali contenuti all'interno del condotto stesso non sia influenzata dalla zona.

[CEI EN IEC 62443-3-3:2020, punto 3.1.12]

3.1.5 **Contesto di sicurezza**: Sicurezza fornita alla macchina dall'ambiente in cui è destinata ad essere utilizzata.

3.1.6 **Sistema di Automazione e Controllo Industriale (IACS)**: Insieme di personale, hardware e software che possono influenzare o influire sul funzionamento sicuro, protetto e affidabile di un processo industriale.

Nota 1: questi sistemi includono, a titolo esemplificativo ma non esaustivo:

- sistemi di controllo industriale, compresi sistemi di controllo distribuito (DCS), controllori logici programmabili (PLC), unità terminali remote (RTU), dispositivi elettronici intelligenti, controllo di supervisione e acquisizione dati (SCADA), rilevamento e controllo elettronico in rete e sistemi di monitoraggio e diagnostica; in questo contesto, i sistemi di controllo del processo includono le funzioni del sistema di controllo del processo di base (CN) e del sistema correlato con le funzioni di sicurezza (SRP/CS) che possono essere fisicamente separati o coesistere in una logica cosiddetta Safety Integrated;

- sistemi informativi associati quali: controllo avanzato o multivariabile, ottimizzatori online (ad esempio CAM/CAE), monitor di apparecchiature specifiche, interfacce grafiche, storici dei processi in corso e passati, sistemi di esecuzione della produzione e sistemi di gestione delle informazioni di impianto;

- interfacce interne, umane, di rete o interfacce di macchina associate utilizzate per fornire controllo, sicurezza e funzionalità operativa di produzione per processi continui, batch, discreti e talvolta finanche alcuni processi ausiliari (reti distribuzione gas, rete elettrica aziendale, sistema di aspirazione fumi, rete aria compressa, ecc.).

Nota 2: in Figura 2 sono riportati i tipici elementi rilevanti per le risorse IACS; nella figura sono stati previsti condotti e zone specifiche per i prodotti riguardanti questa prassi di riferimento, pur non costituendo un requisito necessario per l'efficace riduzione dei rischi. Nella stessa Figura 2 sono indicati, ad alto livello, i principali processi industriali manifatturieri con esempi di zona appositamente costituita dall'utilizzatore finale per un singolo reparto produttivo; ogni prodotto nella stessa figura comprende differenti risorse IACS integrate dal fabbricante.

[IEC/TS 62443-1-1:2009, punto 3.2.57, modificato. La nota 1 è stata modificata ed è stata aggiunta la nota 2.]

3.1.7 **Minaccia**: circostanza o evento avente il potenziale di influire negativamente su operazioni (inclusa missione, funzioni, immagine o reputazione), beni, sistemi di controllo o individui tramite accesso non autorizzato, distruzione, divulgazione, modifica dei dati e/o negazione del servizio.

[CEI EN IEC 62443-3-3:2020, punto 3.1.44]

3.1.8 **Minaccia informatica**: qualsiasi circostanza, evento o azione che potrebbe danneggiare, perturbare o avere un impatto negativo di altro tipo sulla rete e sui sistemi informativi, sugli utenti di tali sistemi e altre persone.

[Regolamento (UE) 2019/881 [4], articolo 2, punto 8]

3.1.9 **Misura di protezione (MP)**: Mezzo fisico o logico che è in grado, da solo o in combinazione con altri, di ridurre efficacemente il rischio correlato alla riduzione delle condizioni di soddisfacimento dei RESS di un prodotto dovute ad un attacco informatico.

3.1.10 **Pericolo**: Potenziale sorgente di danno.

Nota: il termine "pericolo" può essere qualificato al fine di definire la sua origine (per esempio, pericolo di natura meccanica, elettrica) o la natura del danno potenziale (per esempio, pericolo di elettrocuzione, pericolo di taglio, pericolo tossico, pericolo di incendio).

[UNI EN ISO 12100:2010, punto 3.6 modificato. Le note 2 e 3 sono state rimosse.]

3.1.11 **Prodotto**: Macchina, quasi-macchina e prodotto correlato.

Nota: nella costituzione del prodotto sono state assemblate ed integrate diverse risorse hardware e software che fanno parte del prodotto stesso e, quindi, sono entrate a far parte delle risorse aziendali dopo la messa a disposizione del prodotto all'utente finale.

[Regolamento (UE) 2023/1230, articolo 3]

3.1.12 **Rischio**: Combinazione della probabilità di accadimento di un danno e della gravità di quel danno.

[UNI EN ISO 12100:2010, punto 3.12]

3.1.13 **Risorsa:** Oggetto fisico o logico avente un valore percepito o reale per la sicurezza del prodotto facente parte del prodotto stesso o del sistema di automazione e controllo industriale (IACS) che può portare, tramite attacco informatico, a riduzione delle condizioni di soddisfacimento dei RESS del prodotto.

3.1.14 **Safety**: assenza di rischi non tollerabili.

[ISO/IEC Guide 51:2014, punto 3.14]

3.1.15 **Sistema esterno**: Ambiente esterno al prodotto che si collega allo stesso sia dal punto di vista hardware che da quello software.

3.1.16 **Sistema informatico**: Mezzi o dispositivi che contribuiscono o partecipano alla trasmissione o allo scambio di dati.

3.1.17 **Vulnerabilità**: debolezza di un sistema di controllo di una macchina o di una contromisura che può essere sfruttata da una o più minacce per violare l'integrità del sistema di controllo della macchina

[CEI CLC/IEC/TS 63074:2024, punto 3.1.26]

3.1.18 **Zona:** Raggruppamento di risorse logiche e/o fisiche che hanno requisiti di sicurezza comuni.

[CEI EN IEC 62443-3-3:2020, punto 3.1.47]

3.2 SOGGETTI COINVOLTI

3.2.1 **Fabbricante**: qualsiasi persona fisica o giuridica che:

- fabbrichi prodotti o che faccia progettare o fabbricare tali prodotti e li commercializzi con il proprio nome o con il proprio marchio; oppure
- fabbrichi prodotti e li metta in servizio per uso proprio.

[Regolamento (UE) 2023/1230, articolo 3, punto 18]

3.2.2 **Fornitore di componenti**: Colui che fornisce, a vario titolo, componenti per l'integrazione dei prodotti e/o risorse delle IACS.

3.2.3 **Utente**: Persona fisica, processi software e dispositivi che interagiscono con una o più risorse delle IACS rilevanti per la sicurezza dei prodotti.

3.2.4 **Utilizzatore**: Persona fisica che impiega un prodotto nell'esercizio della sua attività, professionale o meno.

Nota: col termine impiego si intente ad esempio la manutenzione, la regolazione, l'uso, la programmazione, la ricerca guasti, ecc.

3.2.5 **Utilizzatore professionale**: Persona fisica che utilizza o gestisce un prodotto nell'esercizio della sua attività professionale o del suo lavoro.

[Regolamento (UE) 2023/1230, articolo 3, punto 36]

3.3 LIVELLI DI SICUREZZA

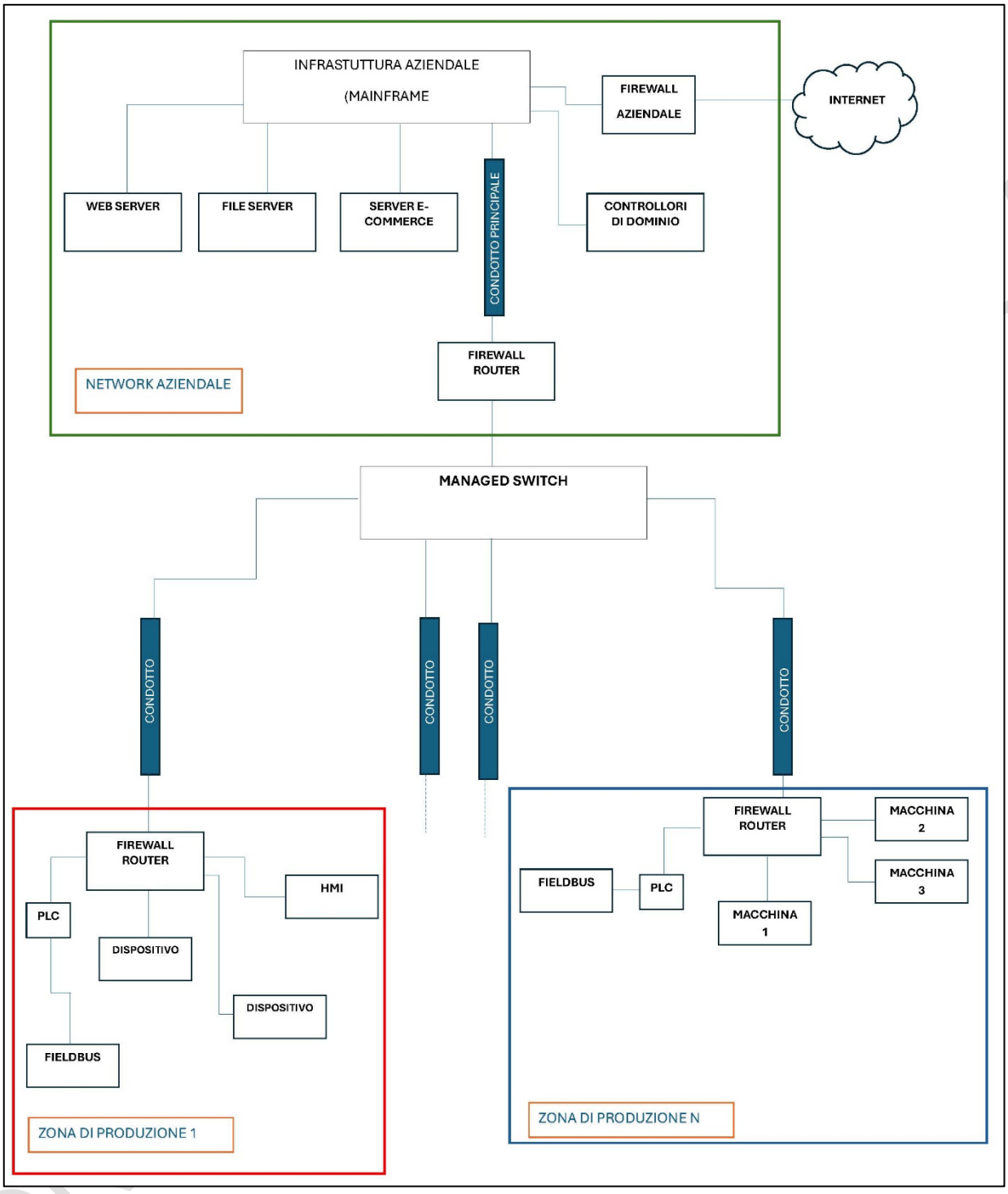
3.3.1 **SL_1s**: Livello 1 di sicurezza per la mitigazione dei rischi degli attacchi informatici accidentali sul prodotto, che possono incidere sulla sicurezza dei prodotti stessi.

Nota: gli attacchi informatici accidentali possono avvenire sia per errori (ad esempio, input di un dato sbagliato) che per inconsapevolezza di recare una minaccia al prodotto (ad esempio, inserimento di dispositivo esterno USB contenente virus o trojan).

3.3.2 **SL_2s**: Livello 2 di sicurezza per la mitigazione dei rischi degli attacchi informatici intenzionali sul prodotto, condotti utilizzando mezzi semplici con scarse risorse, competenze generiche e bassa motivazione che possono incidere sulla sicurezza dei prodotti stessi.

3.3.3 **SL_3s**: Livello 3 di sicurezza per la mitigazione dei rischi degli attacchi informatici intenzionali sul prodotto, condotti utilizzando mezzi sofisticati con risorse moderate, con specifiche competenze sui sistemi IACS aziendali e motivazione moderata che possono incidere sulla sicurezza dei prodotti stessi.

Figura 2: Rappresentazione dei principali processi industriali manifatturieri



4 PRINCIPIO

Il presente documento si articola in alcune fasi, successive, indicate negli specifici punti:

1) identificazione delle vulnerabilità che possono essere sfruttate dalle minacce (punto 5);
2) valutazione del rischio di alterazione dei sistemi informatici delle macchine (vedere punto 6);
3) eventuali misure di mitigazione dei rischi informatici (punto 7).

5 IDENTIFICAZIONE DELLE VULNERABILITÀ CHE POSSONO ESSERE SFRUTTATE DALLE MINACCE

Il fabbricante deve identificare le vulnerabilità del prodotto, che possono essere sfruttate dalle minacce in grado di alterare l'integrità della sicurezza dei sistemi di controllo legati alla sicurezza per ciascuna fase del ciclo di vita del prodotto.

Gli utilizzatori, sulla base delle istruzioni ricevute dai fabbricanti, devono attuare le misure per mitigare i rischi, aggiornando periodicamente le misure di mitigazione in funzione dello sviluppo tecnologico e delle mutate minacce.

L'identificazione delle misure appropriate per ridurre il rischio di sicurezza informatica deve iniziare con l'analisi delle vulnerabilità presenti al fine di eliminare tali vulnerabilità o, se non è possibile, mitigare con appropriate misure di sicurezza informatica il rischio che le minacce possano sfruttare tali vulnerabilità causando l'alterazione della integrità della sicurezza dei sistemi di controllo utilizzati ai fini della sicurezza.

Il primo passo per l'accertamento del rischio "sicurezza informatica" consiste nell'identificazione delle vulnerabilità che possono essere sfruttate dalle minacce per compromettere la sicurezza funzionale del prodotto. Il processo di identificazione delle vulnerabilità si deve sviluppare mediante:

- l'identificazione dei dispositivi del prodotto che posso presentare vulnerabilità;
- per ogni dispositivo precedentemente individuato, l'identificazione delle vulnerabilità potenzialmente sfruttabili da una o più minacce che possono condurre ad un rischio della "sicurezza informatica" in grado di compromettere la sicurezza funzionale del prodotto. Quanto sopra comporta, prima di tutto, l'individuazione delle funzioni di sicurezza che possono essere alterate da ogni minaccia in grado di sfruttare le vulnerabilità individuate.

  Nota: le vulnerabilità che possono essere sfruttate da minacce possono essere già presenti sui dispositivi del prodotto o nascere dopo un guasto di uno o più di tali dispositivi
- l'identificazione delle parti dei dispositivi che presentano delle vulnerabilità che necessitano, attraverso l'intervento sull'hardware o sul software di tali dispositivi, dell'applicazione di contromisure per eliminare le vulnerabilità identificate o, nel caso ciò non sia possibile, mitigare il rischio di sicurezza informatica riducendolo al di sotto del valore tollerabile mediante la valutazione del rischio sicurezza informatica (vedere il punto 6).

Per valutare se lo sfruttamento di una vulnerabilità da parte di una minaccia possa compromettere la sicurezza funzionale, si devono conoscere le specifiche di ogni funzione di sicurezza potenzialmente alterabile dalla minaccia ed individuare in che modo tale minaccia possa alterare il funzionamento del circuito di sicurezza che la realizza, ma prendendo in considerazione solo le alterazioni che possano compromettere l'integrità della sicurezza di tale funzione.

Si riportano di seguito esempi di dispositivi installati nel prodotto che possono introdurre potenziali vulnerabilità sfruttabili da minacce:

- sistemi di accesso quali ad esempio:
  - porte USB;
  - porte RJ45;
  - porte seriali (RS 232, RS 485, ecc.);
  - unità CD-ROM;
  - unità di memoria esterne (hard disk, memory card, ecc.);

- pannelli operatore dove sia possibile abilitare o disabilitare funzioni di sicurezza o inserire password per accesso a funzioni di sicurezza (ad esempio parametri di configurazione);
- porte di programmazione dei PLC (sia di processo che di sicurezza);
- dispositivi di comando senza cavo (ad esempio radiocomandi);
- dispositivi con interfacce Wi-Fi o Bluetooth collegati al prodotto (ad esempio per configurare il dispositivo);
- dispositivi che contengono porte previste per la connessione a reti industriali accessibili dalla rete internet (ad esempio per ragioni di raccolta dati o supervisione).

Per comprendere se una minaccia possa sfruttare una vulnerabilità del prodotto, al fine di alterare le relative funzioni di sicurezza, si deve valutare se le conseguenze possano compromettere la corretta funzionalità e l'integrità delle stesse funzioni. Un elenco di possibili conseguenze pur non esaustivo, è il seguente:

- disattivazione di una funzione di sicurezza, ossia rendere tale funzione di sicurezza non più in grado di rilevare la richiesta di attivazione della stessa, in corrispondenza di un evento pericoloso che ne richiede l'intervento;
- cambiamento di parametri nei dispositivi programmabili, tale da modificare i limiti di funzionamento sicuro;
- dilatazione dei tempi di risposta della funzione di sicurezza, compromettendone l'integrità;
- blocco del rilevamento dei dispositivi di ingresso della funzione di sicurezza, impedendone l'attivazione alla richiesta di intervento di tale funzione;
- impedimento dell'attivazione delle uscite di sicurezza di un circuito di sicurezza, nel caso in cui venga richiesto l'arresto sicuro delle macchine o di parti di esse;
- alterazione della logica del sistema di sicurezza (tramite manipolazione e modifica dei dati in memoria), inducendola a credere di essere costantemente in uno stato sicuro, impedendo così alla funzione di sicurezza di intervenire quando necessario;
- impedimento dell'attivazione della funzione di arresto di sicurezza da parte dell'operatore, nel caso di pressione del pulsante di emergenza, di apertura di ripari mobili interbloccati, di intercettazione di barriere immateriali, ecc.
- attivazione della funzione di muting verso un dispositivo elettrosensibile di protezione anche se nessun oggetto per il quale la funzione di muting debba essere attivata sta chiedendo la sua attivazione.

Per l'identificazione delle vulnerabilità che possono essere sfruttate dalle minacce può essere utilizzato un modello a matrice riportato in Appendice B.

L'identificazione delle vulnerabilità di un prodotto deve essere effettuata per ogni fase del ciclo di vita dello stesso, considerando ogni singola funzione di sicurezza che interessa la specifica fase del ciclo di vita in esame.

Qualora una vulnerabilità, nella specifica fase del ciclo di vita del prodotto, possa essere sfruttata da una minaccia allo scopo di compromettere la sicurezza funzionale, tale minaccia deve essere identificata elencando le potenziali conseguenze e se tali conseguenze possano portare alla perdita della funzione di sicurezza.

Nota: una minaccia che sfrutta una vulnerabilità può produrre più di una conseguenza sulla funzione di sicurezza.

Se la conseguenza di una vulnerabilità/minaccia è la perdita di integrità della funzione di sicurezza, nella successiva valutazione del rischio sicurezza informatica si deve valutare se tale vulnerabilità sia eliminabile o, qualora non lo fosse, determinare le misure di mitigazione del rischio da adottare (vedere il punto 7).

Esempi di pericoli di natura informatica, Interni al prodotto, interni all'organizzazione ed esterni, sono riportati in Appendice D.

6 VALUTAZIONE DEL RISCHIO DI ALTERAZIONE DEI SISTEMI INFORMATICI DELLE MACCHINE

6.1 PROCESSO DI VALUTAZIONE DEL RISCHIO

La valutazione del rischio di un prodotto è un processo sistematico volto a identificare, analizzare e valutare i rischi relativi alla cibersicurezza associati al suo utilizzo, con l'obiettivo di valutare se possano avere influenza sulla safety del prodotto.

Esistono diverse norme di riferimento per la sicurezza industriale in materia di cibersicurezza, in particolare la serie IEC 62443, che rappresenta il punto di riferimento globale per la sicurezza dei sistemi di automazione e controllo industriale (IACS).

Nota: la norma CEI EN IEC 62443-3-2:2021 fornisce indicazioni specifiche e strutturate per la valutazione del rischio e nella presente prassi di riferimento sono utilizzati i principi fondamentali di tale norma come linee di indirizzo per condurre una valutazione del rischio.

La valutazione del rischio si compone delle seguenti fasi:

- raccolta della documentazione e identificazione del prodotto;
- analisi iniziale del prodotto;
- identificazione dei rischi;
- stima dei fattori di rischio;
- stima del rischio complessivo;
- definizione di misure di mitigazione del rischio.

6.2 RACCOLTA DELLA DOCUMENTAZIONE E IDENTIFICAZIONE DEL PRODOTTO

La prima fase di valutazione dei rischi consiste nell'identificazione e nella descrizione del prodotto oggetto di analisi. Questa fase viene effettuata dal fabbricante e può coinvolgere l'utilizzatore. Si deve documentare, ove applicabile e pertinente:

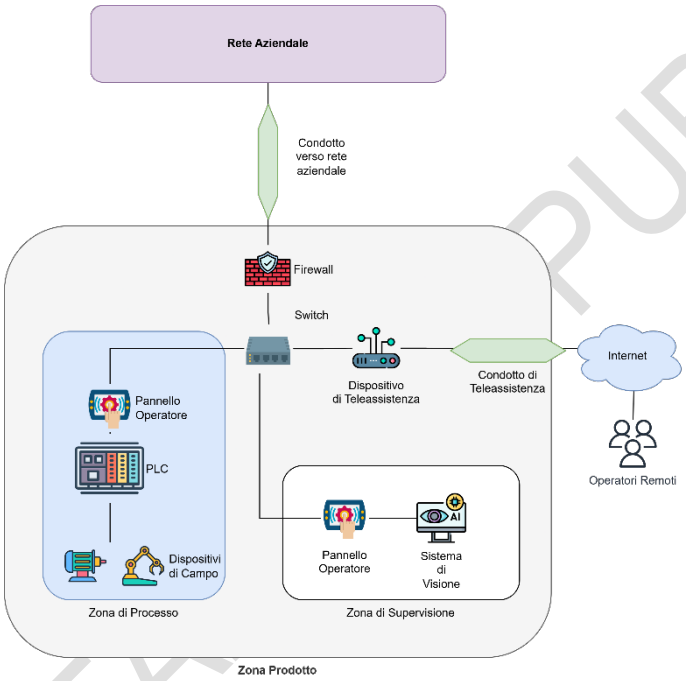
- inventario delle risorse del prodotto: elenco e descrizione delle risorse, inclusi hardware, software, dispositivi di rete e applicazioni. Un esempio di informazioni da raccogliere per ogni risorsa è riportato in Appendice F;
- definizione del perimetro di sicurezza: descrizione del prodotto contenente una mappa chiara del perimetro di sicurezza, delimitando le risorse e i sistemi da proteggere rispetto all'ambiente esterno;
- documentazione delle risorse: devono essere identificate e documentate le risorse pertinenti richieste per le attività relative alle fasi del ciclo di vita del prodotto e alle altre attività correlate (*identificazione delle componenti e dei processi critici*);
- dati: devono essere identificate e documentate le informazioni in merito alle risorse dati utilizzate dal prodotto;

- schemi elettrici e di rete: devono essere identificati e documentati i diagrammi e le mappe dettagliate della configurazione fisica e logica delle infrastrutture di rete e degli impianti elettrici del prodotto;
- risorse umane: devono essere identificate e documentate le informazioni circa le risorse umane, comprese le loro competenze, utilizzate nelle fasi operative, manutentive e di smantellamento del prodotto.

6.3 ANALISI DELLE INTERAZIONI DEL PRODOTTO

Si devono analizzare le modalità di interazione tra le stesse risorse e realizzare un diagramma di rete adottando il concetto di suddivisione in Zone e Condotti (vedere, a titolo di esempio, la figura 3).

Figura 3: Esempio di schema di zone e condotti



6.4 STIMA DEI RISCHI

6.4.1 Generalità

In questa fase si devono stimare i rischi, utilizzando la seguente formula:

Rischio = Probabilità × Impatto

Per identificare le minacce, si deve definire il *Threat Model*, che rappresenta i potenziali scenari di attacco in grado di compromettere il prodotto. Il *Threat Model* include le seguenti informazioni:

- le vulnerabilità presenti nel prodotto, come definito nel punto 5;
- le minacce (Threats) che possono colpire il prodotto;
- gli attori (Actors) che potrebbero rappresentare una minaccia, specificandone le caratteristiche, come competenze;
- le risorse coinvolte e le relative conseguenze e impatti in caso di sfruttamento delle vulnerabilità da parte delle minacce.

6.4.2 Probabilità

La probabilità di accadimento di un evento potenzialmente pericoloso deve essere valutata due volte nel processo di valutazione del rischio. Inizialmente, la probabilità deve essere valutata senza considerare le contromisure esistenti, per stimare il rischio non mitigato. Successivamente, deve essere rivalutata tenendo conto delle contromisure in essere, al fine di determinare il rischio residuo. Il prospetto 1 fornisce un esempio di scala per definire la probabilità di accadimento dell'evento in valutazione.

Prospetto 1: Esempio di scala di probabilità

Scala	Probabilità	Descrizione	Stima di probabilità
5	Certo	Quasi certo	Evento imminente, probabilmente entro un mese
4	Probabile	Probabile che si verifichi	L'evento si verifica probabilmente più di una volta per anno
3	Possibile	Abbastanza possibile o non insolito che si verifichi	L'evento si verifica probabilmente in un periodo tra 1 e 5 anni
2	Improbabile	Possibile, ma molto improbabile che si verifichi	L'evento si verifica probabilmente in un periodo tra 5 e 10 anni
1	Raro	Così improbabile che si può presumere che non si verifichi	L'evento si verifica probabilmente in un periodo superiore ai 10 anni

6.4.3 Impatti e conseguenze

Devono poi essere identificate le conseguenze e gli impatti relativi al rischio.

La conseguenza è il risultato indesiderato di un incidente, solitamente descritto in termini di effetti sulla salute e sicurezza, impatti ambientali, perdita di proprietà e costi di interruzione delle attività, derivanti da un determinato evento. Dato il campo di applicazione del presente documento, le uniche conseguenze da tenere in considerazione sono quelle che hanno effetti sulla sicurezza del prodotto.

L'impatto è la misura della perdita o del danno finale associato a una conseguenza e può essere espresso in termini di entità delle lesioni fisiche o dei danni alla salute, entità del danno ambientale e/o entità delle perdite, come danni alla proprietà, perdita di materiali, perdita di proprietà intellettuale, riduzione della produzione, perdita di quota di mercato e costi di ripristino. Dato il campo di applicazione del presente documento, gli unici impatti da tenere in considerazione sono quelli che possono generare lesioni fisiche o danni alla salute delle persone.

Un esempio di metodo per la stima dell'impatto è riportato nel prospetto 2.

Prospetto 2: Esempio di impatti e conseguenze

Scala	Impatto	Impatto sulla salute/safety
1	**Trascurabile**	Nessuna conseguenza per l'operatore, nessuna esposizione a pericoli
2	**Minore**	Conseguenze trascurabili per l'operatore (es. possibile esposizione a bassi livelli di rumore o vibrazioni)
3	**Moderato**	Conseguenze rilevanti per la salute dell'operatore, esposizione a condizioni di lavoro non ottimali (es. rumorosità elevata, surriscaldamento)
4	**Grave**	Lesioni gravi per l'operatore (es. esposizione a sostanze nocive o parti in movimento pericolose)
5	**Critico**	Conseguenze rilevanti per la vita dell'operatore, esposizione a pericoli letali come scariche elettriche, crolli strutturali, esplosioni

6.4.4 Stima del rischio complessivo

Il rischio complessivo si determina combinando la probabilità e le conseguenze all'interno di una matrice, utilizzando le scale precedentemente definite. Per categorizzare la severità del rischio, si deve stabilire una scala di valutazione adeguata. Un esempio di scala di rischio è riportato nel prospetto 3.

Prospetto 3: Esempio di scala di rischio

Scala di Rischio	Valore
da 1 a 5	basso
da 6 a 10	medio
da 12 a 15	alto
da 16 a 20	critico
25	estremo

Un esempio di matrice di rischio è riportato nel prospetto 4.

Prospetto 4: Esempio di Matrice del Rischio[3]

		Probabilità				
		1 Raro	2 Improbabile	3 Possibile	4 Probabile	5 Certo
Impatto	1 Trascurabile	**1**	**2**	**3**	**4**	**5**
	2 Minore	**2**	**4**	**6**	**8**	**10**
	3 Moderato	**3**	**6**	**9**	**12**	**15**
	4 Grave	**4**	**8**	**12**	**16**	**20**
	5 Critico	**5**	**10**	**15**	**20**	**25**

Un esempio di prospetto per la valutazione del rischio è riportato in Appendice G.

6.5 DEFINIZIONE DI MISURE DI MITIGAZIONE DEL RISCHIO

Una volta valutati i rischi, si devono intraprendere azioni correttive per mitigarli. Questo processo deve essere adeguatamente documentato per garantire tracciabilità e conformità alle normative. Un esempio di "mapping" fra misure di mitigazione, soggetti coinvolti e livelli di sicurezza raggiungibili è riportato in Appendice C. La strategia della gestione del rischio deve seguire i seguenti passi, nell'ordine indicato:

- eliminare le vulnerabilità: evitare che il rischio possa manifestarsi eliminando le vulnerabilità che possono essere sfruttate dalle minacce;
- mitigare: implementare misure di mitigazione per ridurre la probabilità o l'impatto del rischio;
- gestire il rischio residuo: indicare nelle istruzioni per l'uso sia i rischi residui presenti dopo l'adozione delle misure di mitigazione sia le modalità di gestione da parte dell'utilizzatore.

[3] Il valore 25 non viene considerato nel campo di applicazione del presente documento.

7 EVENTUALI MISURE DI MITIGAZIONE DEI RISCHI INFORMATICI

7.1 LIMITI DEL SISTEMA SOTTO OSSERVAZIONE

Per eseguire una valutazione e l'eventuale successiva mitigazione dei rischi dovuti agli attacchi informatici rivolti ad un prodotto, si deve estendere l'analisi a tutti i componenti relativi al sistema di automazione e controllo industriale del prodotto in esame e delle risorse.

7.2 COMPETENZE DELLE PARTI COINVOLTE

Poiché i metodi di attacco informatico evolvono in continuazione e molto rapidamente, anche le misure di mitigazione (contro gli attacchi informatici) di cui è dotato il prodotto devono adattarsi continuamente in tutto il ciclo di vita del prodotto.

Non è, dunque, possibile proteggere il prodotto solamente per mezzo delle misure adottate dal fabbricante prima della sua messa in servizio; i rischi per la sicurezza informatica possono essere adeguatamente mitigati solamente attraverso gli sforzi combinati di tutte le parti coinvolte, ovvero:

- fornitori di componenti, che devono dotare, per quanto possibile, di misure di protezione allo stato dell'arte i singoli componenti rilevanti per la sicurezza informatica;
- fabbricante del prodotto, che deve:
  - scegliere componenti adeguati;
  - adottare opportune misure di protezione, sia hardware che software;
  - fornire all'utilizzatore tutte le necessarie informazioni su come affrontare i problemi di sicurezza informatica durante l'uso del prodotto;
- utilizzatore professionale, che deve mettere in atto i comportamenti adeguati a prevenire e a reagire alle minacce informatiche.

Nessuna parte coinvolta può assumere che un'altra parte sia totalmente responsabile della sicurezza informatica. Allo stesso tempo, nessuna delle parti coinvolte ha a disposizione tutte le informazioni necessarie per affrontare efficacemente le minacce e le vulnerabilità della sicurezza informatica, durante tutte le fasi del ciclo di vita del prodotto.

Ciascuna parte coinvolta dovrebbe, quindi, comunicare alle altre parti le informazioni relative alle minacce e alle vulnerabilità che non possono affrontare completamente da sole o che hanno implicazioni per le altre parti. Ciò comporta, anche, la stipulazione di accordi contrattuali nei quali viene definito il contesto di sicurezza in cui il prodotto è destinato ad essere utilizzato.

Nota: una guida molto ampia e generale sui sistemi di sicurezza delle reti aziendali e sui livelli di sicurezza raggiungibili (SL) tramite l'implementazione di misure di mitigazione è riportata nella CEI EN IEC 62443-3-3:2020.

7.3 MISURE DI MITIGAZIONE CONTRO I RISCHI DI NATURA INFORMATICA

7.3.1 Generalità

Le misure attuabili contro i rischi di natura informatica includono la mitigazione dei rischi intollerabili per la sicurezza informatica mediante:

- l'eliminazione dei rischi in fase di progettazione per la sicurezza informatica;
- l'adozione di misure di protezione contro i rischi di natura informatica;
- la comunicazione di informazioni sui rischi per la sicurezza informatica ritenuti tollerabili e accettabili.

Le misure di mitigazione contro i rischi di natura informatica devono comprendere la capacità di prevenire, limitare o contenere l'impatto di un potenziale attacco alla sicurezza informatica del prodotto. In generale, le suddette misure sono implementabili su tre distinti livelli di mitigazione:

- livello generale aziendale;
- livello di sistema; si definiscono, ad esempio, attraverso l'esplicitazione di zone e condotti con requisiti comuni;

  Nota 1: in accordo a IEC/TS 62443-1-1:2009.

- livello di componente.

Nei punti da 7.3.2 a 7.3.10 sono riportate alcune misure utilizzabili efficacemente per la riduzione dei rischi per tutti e tre i livelli.

Nota 2: le informazioni sul mapping fra misure di mitigazione, soggetti coinvolti e livelli di sicurezza raggiungibili si trovano in Appendice C.

7.3.2 Protezione delle comunicazioni (MP1_x)

I sistemi di comunicazione, locale e remota, possono essere utilizzati dall'attaccante per accedere alle risorse del prodotto. Per questo motivo, devono essere messe in atto misure che riducano la possibilità che tali sistemi vengano sfruttati per portare attacchi informatici al prodotto, con misure di protezione quali:

- **MP1_1**: disconnessione del prodotto dalle reti di comunicazione esterne, tranne per i periodi strettamente necessari, limitando temporalmente la possibilità di accesso al prodotto;
- **MP1_2**: realizzazione di connessioni in sola lettura ogni qualvolta possibile; inoltre, realizzazione di connessioni monodirezionali soltanto dal sistema IACS ai sistemi non IACS ogni qualvolta possibile senza abilitare la connessione in ingresso al sistema IACS;
- **MR1_3**: utilizzo di comunicazioni crittografate; in particolare per le comunicazioni del prodotto verso il mondo esterno;
- **MR1_4**: monitoraggio delle connessioni; ad esempio, utilizzando reti private virtuali (VPN);
- **MR1_5**: sistemi di identificazione, *deny of service* e reportistica degli utenti non autorizzati ed in special modo degli utenti wireless non riconosciuti;
- **MR1_6**: limitazione al numero massimo di connessioni concorrenti per uno specifico utente;
- **MR1_7:** sistema per la terminazione temporizzata delle connessioni, qualora ci sia accesso da parte di una persona fisica.

Nello specifico, deve essere prestata particolare attenzione alle politiche di registrazione e autenticazione delle reti wireless, nonché all'autenticazione ad esse di tutti gli utenti (umani, processi software e dispositivi, si veda la definizione di utente); questa protezione del sistema wireless aziendale è a cura dell'utilizzatore professionale.

Nota: vedere in proposito il CR 2.2, punto 6.4 della CEI EN IEC 62443-4-2:2019.

7.3.3 Autenticazione (MP2_x)

I mezzi di autenticazione per il controllo degli accessi da parte delle persone possono comprendere:

Nota 1: vedere anche i punti 5.3 e 5.5 della CEI EN IEC 62443-3-3:2020.

- **MP2_1**: sistemi di password, che devono essere adeguatamente gestiti dall'utilizzatore (segretezza, modifica periodica, complessità delle password, impedimento al riutilizzo di password già usate, ecc.) e sistemi biometrici, che utilizzano caratteristiche fisiche o

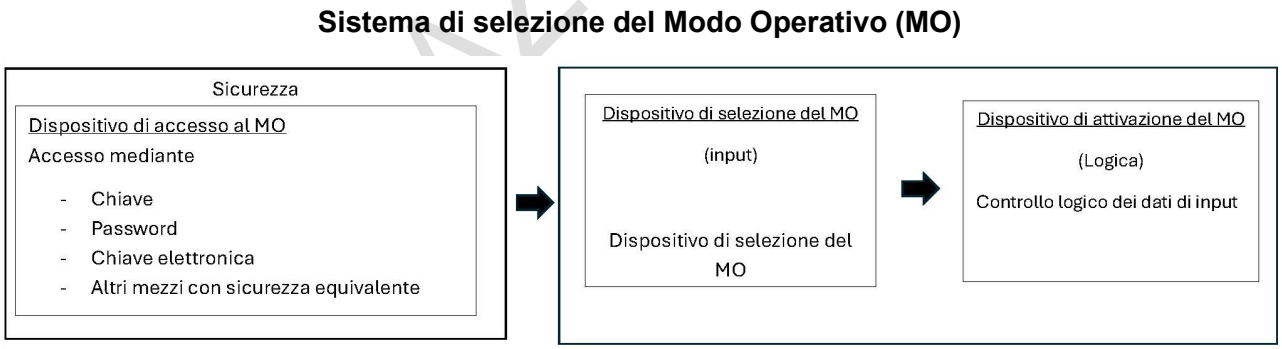
comportamentali uniche (es. impronte digitali, riconoscimento facciale, iride, voce) per autenticare l'identità di un individuo e sono basati su sensori, algoritmi di elaborazione e confronto con database;

- **MP2_2**: autenticazione a fattori multipli (MFA), ad esempio password dell'utente e OTP (One-Time Password) reperibile su un dispositivo a disposizione dell'utente;
- **MP2_3**: lettori di badge/schede e tag (RFID, NFC, ecc.) e QR-code (ottici);
- **MP2_4**: mezzi per limitare il numero di autenticazioni fallite prima di disabilitare l'accesso, sistemi di notifica dell'autenticazione;
- **MP2_5**: sistemi di autenticazione "ristretti" per accessi di utenti da reti non affidabili;
- **MP2_6**: override dell'autenticazione da parte di supervisore;
- **MP2_7**: mezzi e sistemi di autenticazione di macchina basati, su dispositivi di security fisici (ad esempio chiavi o dispositivi di abilitazione fisica) che richiedano intervento diretto dell'operatore per l'abilitazione del dato servizio (vedere Figura 4);
- **MP2_8**: limitazione dei privilegi degli utenti a quelli strettamente indispensabili per il compito a cui devono adempiere, in modo da ridurre al minimo la possibilità di intervento sui sistemi informatici (*"least privilege*").

Nota 2: in accordo con il punto 3.1.31 della CEI EN IEC 62443-3-3:2020.

Nota 3: il collegamento di dispositivi al prodotto, specialmente se permanentemente installati sullo stesso, dovrebbe essere possibile solamente a seguito di autenticazione del dispositivo che si vuole connettere; ciò dovrebbe valere per qualsiasi tipo di dispositivo (computer, sensore, interfaccia uomo-macchina, ecc.) e per qualsiasi modalità di connessione (cablata, tramite rete dati, wireless, ecc.).

Figura 4: Relazione fra security e safety in sistema di abilitazione modale di macchina (figura 1 della UNI EN ISO 16090-1:2023)



7.3.4 Mezzi fisici di protezione (MP3_x)

Le connessioni fisiche ai sistemi informatici possono essere utilizzate per sferrare attacchi, ad esempio collegandosi ad una porta di rete o ad una porta USB.

I mezzi per prevenire attacchi di questo tipo possono essere:

- **MP3_1**: protezione degli accessi fisici ai punti di connessione del prodotto, ad esempio racchiudendo il prodotto all'interno di involucri apribili solo mediante chiavi oppure ostruendo l'accesso ad una porta di rete attraverso un dispositivo rimovibile con chiave;
- **MP3_2**: disconnessione di tutte le porte, le interfacce e i servizi esterni non utilizzati, quali ad esempio porte USB di computer che controllano il prodotto.

7.3.5 Mezzi di protezione hardware (MP4_x)

Devono essere utilizzati mezzi di protezione hardware, quali:

- **MP4_1**: firewall che limitino la possibilità di accesso alle risorse e specificamente al loro software legato alla sicurezza da parte di utenti non autorizzati;
- **MP4_2**: test funzionali di sicurezza per i prodotti; alcuni di questi test possono essere un valido ausilio alla verifica periodica delle risorse del prodotto correlato alla sicurezza e più in generale delle zone e dei condotti delle risorse rilevanti delle IACS;
- **MP4_3**: separazione delle reti dati (tra utilizzo interno, per utilizzo di interconnessione/integrazione dati, e accessi esterni, per utilizzo della teleassistenza); a tale proposito, vedere anche MP6_2 e MP6_4.

7.3.6 Mezzi di protezione software (MP5_x)

I sistemi software possono contribuire in modo determinante alla protezione contro gli attacchi di natura informatica, con misure di protezione quali:

- **MP5_1**: sistemi automatici di verifica delle funzionalità dei sistemi di sicurezza (ad esempio routine di validazione automatica dei software di sicurezza dopo le fasi manutentive o di aggiornamento delle policy aziendali di security);
- **MP5_2**: aggiornamento periodico dei software di protezione del prodotto (ad esempio, software antivirus), a cura dell'utilizzatore;
- **MP5_3**: aggiornamento periodico dei software di controllo del prodotto (ad esempio, sistemi operativi) o del firmware, in modo da mantenere allo stato dell'arte le misure di protezione implementate dal fornitore del software;
- **MP5_4**: restrizione all'installazione ed esecuzione dei codici portabili;
- **MP5_5**: sistemi di log (tracciamento) degli eventi di sicurezza consultabili solo in lettura per prevenire la modifica malevola degli accessi; l'accesso completo al sistema dovrebbe avvenire solo attraverso connessione locale;
- **MP5_6**: sistemi di autenticazione dei dispositivi e dei software principali utilizzati dalle IACS prima di abilitare lo scambio dati.

Nota: utili informazioni specifiche al supporto da fornire in funzione delle risorse durante gli aggiornamenti dei software di protezione e di controllo si trovano in CR 3.11, punto 7.13 della CEI EN IEC 62443-4-2:2019. In particolare, vedere le indicazioni in CR 3.10, punto 7.12 della CEI EN IEC 62443-4-2:2019, specifiche per i fornitori di componenti che richiedono aggiornamenti del software.

7.3.7 Architettura delle IACS (MP6_x)

La progettazione delle IACS può contribuire alla protezione dagli attacchi di natura informatica, ad esempio mediante misure quali:

- **MP6_1**: riduzione della complessità del sistema informatico del prodotto, in modo da poter affrontare meglio le possibili minacce informatiche e le criticità di gestione dell'archiviazione;
- **MP6_2**: realizzazione della topologia del sistema informatico del prodotto con livelli multipli e indipendenti, ad esempio la separazione del sistema informatico rilevante per la sicurezza del prodotto dal sistema informatico generale; per la rete aziendale la segmentazione della rete in più zone ed in particolare la differenziazione delle zone in cui ci sono risorse IACS da quelle informative aziendali non IACS; a tale proposito, vedere anche MP4_3;

- **MP6_3**: le funzioni essenziali di sicurezza per le singole zone della IACS dovrebbero essere autonomamente mantenute per prevenire che un attacco informatico ad una singola zona si propaghi a tutto il sistema;
- **MP6_4**: partizione delle applicazioni a livello di zona; le applicazioni ed i servizi di rete rilevanti per la sicurezza dovrebbero essere gestiti ed assicurati attraverso dispositivi fisici e/o logici differenti; a tale proposito, vedere anche MP4_3;
- **MP6_5**: impiego di mezzi per il management delle risorse del prodotto in modo da privilegiare le risorse necessarie per la sicurezza del prodotto e quelle necessarie a prevenire gli attacchi informatici.

7.3.8 Reazione delle risorse agli attacchi (MP7_x)

La reazione delle risorse agli attacchi informatici può comprendere:

- **MP7_1**: validazione dei valori in ingresso al sistema informatico per accertare che siano all'interno degli intervalli di valori ammessi, ad esempio controllo di soglie per i parametri di processo legati alla sicurezza;
- **MP7_2**: mezzi che portino la risorsa in uno stato sicuro, ad esempio lo arrestino nel caso del prodotto o ne inibiscano il funzionamento o l'accesso, nel caso in cui una risorsa essenziale per la sicurezza del prodotto non funzioni correttamente;
- **MP7_3**: mezzi per prendere localmente il controllo della risorsa del sistema IACS che prevalgano sui comandi da remoto;
- **MP7_4**: mezzi per poter arrestare i movimenti pericolosi del prodotto in caso di malfunzionamento causato da un attacco informatico, ad esempio comandi di arresto di emergenza;
- **MP7_5**: mezzi per il monitoraggio e la gestione dei carichi di rete da e verso il prodotto (ad esempio limitare i transfer rate in ingresso ed in uscita dal prodotto) per prevenire ed attenuare gli effetti di malfunzionamenti causati da attacco informatico.

7.3.9 Altre misure di protezione (MP8_x)

Altre misure di protezione contro gli attacchi informatici possono comprendere:

- **MP8_1**: mezzi diagnostici per rilevare componenti del sistema informatico essenziali per la sicurezza non funzionanti correttamente;
- **MP8_2**: restrizione ai sistemi di comunicazione condivisi tra utenti (ad esempio social network, repository di immagini fra utenti, chat, ecc.) in special modo fra persone ricadenti nella componente aziendale e soggetti esterni all'organizzazione; in generale questi tipi di comunicazione andrebbero permesse soltanto fra dispositivi "trusted" (ovvero ritenuti affidabili) dentro la rete aziendale;

  Nota 1: in accordo a SR 5.3, punto 9.5.2 della CEI EN IEC 62443-3-3:2020.

- **MP8_3:** sistemi di controllo legati alla sicurezza in grado di mitigare le conseguenze di una minaccia informatica, ad esempio mediante il monitoraggio e la limitazione sicuri dei valori limite di grandezze rilevanti per la sicurezza, quali velocità o temperature massime.

  Nota 2: in accordo alle norme UNI EN ISO 13849-1:2023 o CEI EN IEC 62061:2023.

7.3.10 Istruzioni per l'uso

Le istruzioni per l'uso dei prodotti devono comprendere tutte le informazioni necessarie all'utilizzatore finale per affrontare i rischi di natura informatica durante l'impiego dei prodotti.

A titolo esemplificativo e non necessariamente esaustivo, possono essere riportate le seguenti informazioni:

- requisiti delle reti di comunicazione dati a cui il prodotto viene collegato;
- gestione delle credenziali di accesso da parte degli utenti e dei sistemi di autenticazione (ad esempio, autenticazione a fattori multipli);
- aggiornamento dei software di controllo del prodotto, ad esempio sistemi operativi;
- aggiornamento dei software di protezione del prodotto, ad esempio software antivirus;
- aggiornamento del firmware del prodotto e dei suoi componenti;
- controlli sul corretto funzionamento (test funzionali) dei componenti del sistema informatico del prodotto;
- gestione delle modalità di connessione da remoto al prodotto, ad esempio in caso di telediagnosi, telemanutenzione o telecontrollo;
- modalità di risposta ad attacchi informatici.

Un esempio di protezione dall'alterazione del software e della tracciabilità, relativo al software del PLC o CNC, è riportato in Appendice E.

8 ESEMPIO DI MITIGAZIONE DEL RISCHIO

Esaminando le possibili minacce dovute ai sistemi di accesso (vedere punto 5), si identifica la chiavetta USB come possibile vulnerabilità.

Nel processo di valutazione del rischio di cibersicurezza (vedere punto 6), relativamente al rischio specifico di installazione di malware tramite chiavetta USB, sono assunti i seguenti parametri:

- Impatto: Grave (4);
- Probabilità: Probabile (4).

Utilizzando la formula definita nel punto 6.4:

Rischio = Probabilità x Impatto = 4 x 4 = 16

Il rischio risulta quindi non accettabile e devono essere considerate misure di mitigazione fra quelle previste al punto 7.

In questo caso sono da considerare i mezzi fisici di protezione al punto 7.3.3, ed in particolare:

- **MP3_1**: protezione degli accessi fisici ai punti di connessione del prodotto e/o
- **MP3_2**: disabilitazione di tutte le porte USB,

devono essere implementare le mitigazioni rilevanti descritte nel prospetto C.3 per raggiungere il livello SL_2s o SL_3s a seconda delle caratteristiche del contesto aziendale.

Queste misure riducono la probabilità da Probabile (4) a Raro (1) e quindi il rischio residuo diventa:

Rischio residuo = Probabilità x Impatto = 1 x 4 = 4

Pertanto, il rischio residuo è di livello basso; rimangono quindi da descrivere nella documentazione aziendale le procedure e/o le informazioni per la gestione del rischio residuo.

Appendice A (informativa) - Considerazioni su RESS e cibersicurezza nel Regolamento (UE) 2023/1230 per la protezione dall'alterazione dei sistemi informatici

Nota: Nella presente appendice, il testo in italico è estratto dal Regolamento (UE) 2023/1230 [3], dal D.Lgs. 81/2008 [6] o dal Regolamento (EU) 2024/2847 [5].

La preoccupazione del legislatore comunitario per la considerazione del tema in discussione si è concretizzata, con riferimento alle macchine, nel Regolamento (UE) 2023/1230 [3], che, preliminarmente, al considerando n. 25 spiega che "*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*".

Su queste premesse, il regolamento in discorso ha previsto alcune disposizioni immediatamente impattanti sul piano degli obblighi degli "operatori economici"[4], sotto il profilo della conformità delle macchine, inserendo specifici requisiti essenziali di sicurezza e di tutela della salute relativi alla progettazione e alla costruzione di prodotti (per brevità "RESS"), come descritti nell'allegato III del Regolamento (UE) 2023/1230 [3], con riferimento agli aspetti di cibersicurezza nel senso sopra individuato.

RESS 1.1.9. – Protezione dall'alterazione

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.

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 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.

RESS 1.2 – Sistemi di comando

[4] Con tale accezione il Regolamento (UE) 2023/1230 [3], all'articolo 3 n. 22 intende individuare il fabbricante, il mandatario, l'importatore o il distributore.

1.2.1. Sicurezza ed affidabilità dei sistemi di comando

I sistemi di comando devono essere progettati e costruiti in modo da evitare l'insorgere di situazioni pericolose.

I sistemi di comando debbano 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;

…omissis…

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.

Il tema centrale che si pone per gli operatori economici e, in particolare, per i fabbricanti di prodotti, è di comprendere attraverso quali strumenti di normazione giuridica e/o tecnica sia possibile garantire il rispetto dei RESS ora riportati, e quindi, la conformità del prodotto con riferimento agli aspetti di sicurezza come sopra delineati.

Una prima indicazione viene data proprio dal Regolamento (UE) 2023/1230 [3], il quale, all'articolo. 20 comma 9, prevede che *"Le macchine e i prodotti correlati che sono stati certificati o per i quali è stata emessa una dichiarazione di conformità nell'ambito di un sistema di certificazione della cibersicurezza adottato conformemente al regolamento (UE) 2019/881 e i cui riferimenti sono stati pubblicati nella Gazzetta ufficiale dell'Unione europea, sono considerati conformi ai requisiti essenziali di sicurezza e di tutela della salute di cui all'allegato III, punti 1.1.9 e 1.2.1, per quanto concerne la protezione contro la corruzione e la sicurezza e l'affidabilità dei sistemi di controllo nella misura in cui tali requisiti siano contemplati dal certificato di cibersicurezza o dalla dichiarazione di conformità o da loro parti."*

Quindi, un primo riferimento per gli operatori economici è quello dei sistemi di certificazione della cibersicurezza, indicato dal Regolamento (EU) 2024/2847 [5], definiti come una serie completa di regole, requisiti tecnici, norme e procedure elaborati e adottati rispettivamente a livello di Unione europea, o da un'autorità pubblica nazionale e che si applicano alla certificazione o alla valutazione della conformità dei prodotti TIC, servizi TIC e processi TIC[5].

Rimanendo nell'ambito dei riferimenti legislativi rilevanti ai fini del tema oggetto della presente prassi di riferimento, si ritiene di dover porre l'attenzione su altre disposizioni legislative che possano essere di supporto per gli operatori nella ponderazione della conformità dei prodotti con riferimento agli aspetti di *safety* di cui si discute.

Il Regolamento (EU) 2024/2847 [5] prescrive requisiti essenziali di cibersicurezza per la progettazione e la fabbricazione di prodotti con elementi digitali e obblighi per gli operatori economici in relazione a tali prodotti per quanto riguarda gli aspetti di cibersicurezza, ovviamente rilevanti anche sotto il profilo della *safety*.

Nello stesso regolamento si prevede, inoltre, che i fabbricanti debbano elaborare processi di

[5] TIC: acronimo per "tecnologie dell'informazione e della comunicazione" (Considerando 1 Regolamento (UE) 2019/881 [4]).

gestione delle vulnerabilità per garantire la cibersicurezza dei prodotti con elementi digitali durante il periodo in cui si prevede che i prodotti siano in uso. In particolare, è previsto che (all'articolo 13, comma 2) "*i fabbricanti effettuano una valutazione dei rischi di cibersicurezza associati a un prodotto con elementi digitali e tengono conto dei risultati di tale valutazione durante le fasi di pianificazione, progettazione, sviluppo, produzione, consegna e manutenzione del prodotto con elementi digitali, allo scopo di ridurre al minimo i rischi di cibersicurezza, prevenire gli incidenti e ridurne al minimo il loro impatto, anche in relazione alla salute e alla sicurezza degli utilizzatori."*

Ancora, (all'art. 13, comma 18) *"i fabbricanti provvedono affinché i prodotti con elementi digitali siano accompagnati dalle informazioni e dalle istruzioni per l'utilizzatore di cui all'allegato II in forma cartacea o elettronica. Tali informazioni e istruzioni sono fornite in una lingua facilmente comprensibile dagli utilizzatori e dalle autorità di vigilanza del mercato. Sono chiare, comprensibili, intelligibili e leggibili."*

Il tema della cibersicurezza delle macchine riferita al tema della sicurezza ha rilevanza in termini di "conformità" ai RESS della normativa di armonizzazione dell'Unione europea anche sotto altri profili: ci riferiamo, in particolare, alle norme di rilevanza penale che prescrivono il divieto di immettere sul mercato macchine non conformi alla normativa di prodotto: l'articolo 23 ("*Obblighi dei fabbricanti e dei fornitori*") del D.Lgs. 81/2008 [6] vieta "*la fabbricazione, la vendita, il noleggio e la concessione in uso di attrezzature di lavoro, dispositivi di protezione individuali ed impianti non rispondenti alle disposizioni legislative e regolamentari vigenti in materia di salute e sicurezza sul lavoro*", prevedendo specifiche sanzioni[6].

Considerato poi il tema della manutenzione, e, in particolare, della cosiddetta assistenza tecnica da remoto, il tema della sicurezza informatica diventa più evidente nella misura in cui il collegamento/connessione digitale può costituire occasione per alterazioni anche solo involontarie del sistema di funzionamento del prodotto tali da comprometterne la sicurezza.

La sicurezza informatica dei prodotti, con riferimento agli aspetti di *safety*, coinvolge obblighi e responsabilità non solo del fabbricante, ma anche di altre figure, tra cui i datori di lavoro (come definiti dalla normativa sulla sicurezza dei luoghi di lavoro e sulla prevenzione degli infortuni), e, sotto profili diversi, gli importatori e i distributori.

Quanto al datore di lavoro, occorre ricordare l'obbligo principale del datore di lavoro con riferimento ai prodotti, che è quello di mettere a disposizione dei lavoratori prodotti conformi alle "*specifiche disposizioni legislative e regolamentari di recepimento delle Direttive comunitarie di prodotto*"[7] che devono essere "*idonee ai fini della salute e sicurezza e adeguate al lavoro da svolgere o adattate a tali scopi che devono essere utilizzate conformemente alle disposizioni legislative di recepimento delle Direttive comunitarie*"[8]: ovviamente, tale obbligo riguarda anche la conformità dei prodotti con riferimento alla sicurezza informatica, per gli aspetti sopra delineati.

Per quanto riguarda gli importatori, considerando la cibersicurezza ai fini di sicurezza come requisito per la valutazione della conformità delle macchine, all'articolo 13 il Regolamento (UE) 2023/1230 [3] prevede che essi debbano immettere sul mercato soltanto macchine o prodotti correlati conformi, disponendo anche che *"L'importatore che ritenga o abbia motivo di ritenere che una macchina o un prodotto correlato non sia conforme al presente regolamento, non lo immette sul mercato fino a quando non sia stato reso conforme. Inoltre, laddove la macchina o il prodotto correlato presentino un rischio per la salute e la sicurezza delle persone e, ove opportuno, degli*

[6] Alla data di pubblicazione della presente prassi di riferimento, vige l'articolo 57 del D.Lgs. 81/2008 [6] che prevede l'arresto da tre a sei mesi o ammenda da 14.238,38 a 56.953,56 euro.
[7] Testo tratto dall'articolo 70 del D.Lgs. 81/2008 [6].
[8] Testo tratto dall'articolo 71 del D.Lgs. 81/2008 [6].

animali domestici nonché la tutela dei beni e, se del caso, dell'ambiente, l'importatore ne informa il fabbricante e le autorità di vigilanza del mercato."

All'articolo 15 il Regolamento (UE) 2023/1230 [3] prevede che anche i distributori abbiano l'obbligo di verificare che il fabbricante (o l'importatore) abbia adempiuto agli obblighi normativi di sua competenza, al momento della immissione sul mercato di macchine, prevedendo altresì che *"Il distributore che ritenga o abbia motivo di ritenere che la macchina o il prodotto correlato non siano conformi al presente regolamento, non mette la macchina o il prodotto correlato a disposizione sul mercato fino a quando non siano stati resi conformi. Inoltre, laddove la macchina o il prodotto correlato presentino un rischio per la salute e la sicurezza delle persone e, ove opportuno, degli animali domestici nonché per la tutela dei beni e, se del caso, dell'ambiente, il distributore ne informa il fabbricante o l'importatore e le autorità di vigilanza del mercato."*

Come è trattato nella presente prassi di riferimento, la conformità dei sistemi informatici di macchine ai fini della *safety* può essere supportata da strumenti di normazione tecnica per la sua materiale attuazione, al fine di consentire agli operatori di conseguire la presunzione di conformità: presunzione che è prevista anche dal Regolamento (EU) 2024/2847 [5], il quale, all'articolo 27, comma 1, così si esprime: *"I prodotti con elementi digitali e i processi messi in atto dal fabbricante che sono conformi alle norme armonizzate o a parti di esse i cui riferimenti sono stati pubblicati nella Gazzetta ufficiale dell'Unione europea si presumono conformi ai requisiti essenziali di cibersicurezza di cui all'allegato I oggetto di tali norme o parti di esse."*

Appendice B (informativa) - Identificazione delle vulnerabilità che possono essere sfruttate dalle minacce

Il prospetto B.1 riporta un esempio di tabella utile a identificare le vulnerabilità che possono essere sfruttate dalle minacce

Prospetto B.1: Esempio di elenco delle possibili vulnerabilità che possono essere sfruttate dalle minacce

Prodotto:								
Funzione di sicurezza								
Descrizione funzionamento della funzione di sicurezza								
Riferimento	**Fase del ciclo di vita**	**Dispositivi coinvolti nella realizzazione della funzione di sicurezza**	**Identificazione vulnerabilità**	**La vulnerabilità può essere sfruttata da una minaccia?**		**Descrizione della minaccia che può sfruttare la vulnerabilità**	**Conseguenze dello sfruttamento della vulnerabilità da parte della minaccia.**	**Alterazione della funzione di sicurezza da parte della minaccia?**	
				Sì	**No**			**Sì**	**No**
1)									
2)									
3)									
4)									
5)									
6)									
7)									
8)									

Appendice C (informativa) - Mapping fra misure di mitigazione, soggetti coinvolti e livelli di sicurezza raggiungibili

Allo stato attuale delle conoscenze e secondo quanto riportato nel punto 3.3, si ritiene che nei contesti aziendali usuali gli attacchi informatici intenzionali effettuati con mezzi sofisticati non siano primariamente condotti per rendere inefficace la sicurezza del prodotto, ma per raggiungere obiettivi di cibercrimine più generali come, ad esempio, l'impossessarsi di informazioni o bloccare la macchina a fini estorsivi. In questi casi, per lo scopo di questa prassi di riferimento – ad eccezione delle aziende che trattano prodotti particolari, ad esempio, militari e aereo-spaziali, nucleari e infrastrutture critiche, per le quali si verifichino esigenze particolari da parte degli utilizzatori finali del prodotto – si ritiene che, ai fini della mitigazione dei rischi che possono portare a riduzione delle condizioni di soddisfacimento dei RESS del prodotto, il massimo livello di sicurezza raggiungibile sia SL_2s.

Un mapping completo dell'efficacia e della necessità di intraprendere le misure di protezione applicabili in funzione della complessità dell'intenzionalità o meno dei vettori di attacco è riportato nella tabella B.1 della CEI EN IEC 62443-3-3:2020 e tabella B.1 della CEI EN IEC 62443-4-2:2019. Si ritiene che questa tabella sia soltanto parzialmente trasponibile ai prodotti trattati in questa prassi di riferimento in quanto, ad esempio, la protezione delle informazioni in genere non fa parte dello scopo di questa prassi di riferimento.

Pertanto, i prospetti da C.1 a C.8 riportano un mapping fra misure di mitigazione, soggetti coinvolti e livelli di sicurezza raggiungibili allineato ai contenuti di questa prassi di riferimento.

Nei prospetti:

- "norma A" indica la CEI EN IEC 62443-3-3:2020;
- "norma B" indica la CEI EN IEC 62443-4-2:2019;
- "○" azione efficace e potenzialmente applicabile per raggiungere il livello considerato;
- "✦" parte necessariamente coinvolta nel processo.

Prospetto C.1: Protezione delle comunicazioni

Misura di mitigazione	SL_1s	SL_2s	SL_3s	Fabbricante e/o fornitore di componenti	Utilizzatore professionale	Note ed esempi
MP1_1 disconnessione del prodotto dalle reti esterne	Non sempre necessario ○	○	○	✦		SR 2.6 e SR 3.8 punti 6.7.3 e 7.10 della norma A.
MP1_2: realizzazione di connessioni in sola lettura	○	○	○	Applicabile solo in alcuni casi ✦	✦	SR 6.1 punto 10.3.1 della norma A, per utilizzatore professionale (eventualmente con interfaccia dedicata per IACS aziendali); CR 3.9 punto 7.11.3 della norma B, per costruttore del prodotto o fornitore componenti.
MR1_3: utilizzo di comunicazioni crittografate			Necessaria per raggiungere questo livello ○	Talvolta necessario per aggiornamenti software rilevanti ✦	✦	SR 3.1 punto 7.3 della norma A; CR 4.3 punto 8.5.2 della norma B.
MR1_4: monitoraggio delle connessioni		Necessaria per raggiungere questo livello ○	Necessaria per raggiungere questo livello ○		✦	SR 6.2 punto 10.4 della norma A.
MR1_5: sistemi di identificazione, deny of service e reportistica		○	○		✦	SR 5.2 RE1 punto 9.4.3 della norma A.
MR1_6: limitazione al numero massimo di connessioni			Necessaria per raggiungere questo livello ○		✦	SR 2.7 punto 6.9 della norma A; CR 2.7, punto 6.9 della norma B.

Misura di mitigazione	SL_1s	SL_2s	SL_3s	Fabbricante e/o fornitore di componenti	Utilizzatore professionale	Note ed esempi
MR1_7: terminazione temporizzata delle connessioni		Necessaria per raggiungere questo livello ○	Necessaria per raggiungere questo livello ○	✦	✦	CR 2.5 punto 6.7 della norma B.

Prospetto C.2: Autenticazione

Mezzo di protezione	SL_1s	SL_2s	SL_3s	Fabbricante e/o fornitore di componenti	Utilizzatore professionale	Riferimenti utili ed esempi
MP2_1: sistemi di password e sistemi biometrici	○	Con modifica periodica per raggiungere questo livello ○	Con modifica periodica e verifica complessità per raggiungere questo livello ○	✦	✦	SR 1.7, punto 5.9 della norma A CR 1.3, punto 5.5 norma B CR 1.7, punto 5.9 norma B
MP2_2: autenticazione a due fattori			Necessaria per raggiungere questo livello ○	✦	✦	SR 2.1 RE 4, punto 6.3.3.4 della norma A CR 1.14 punto 5.16 norma B per autenticazione con “chiavi simmetriche”
MP2_3 lettori di badge/schede e tag e QR-code			Alternativo a MP2_2 per raggiungere questo livello ○	✦	✦	SR 2.1 RE 4 punto 6.3.3.4 della norma A.

Mezzo di protezione	SL_1s	SL_2s	SL_3s	Fabbricante e/o fornitore di componenti	Utilizzatore professionale	Riferimenti utili ed esempi
MP2_4: limitazione del numero di autenticazioni fallite e sistemi di notifica delle autenticazioni		○	○	✦	✦	SR 1.12 punto 5.14 della norma A; CR 1.11 punto 5.13.1 della norma B; CR 1.12 punto 5.14.1 della norma B.
MP2_5: autenticazione “ristretta” per accessi da reti non affidabili	○	○	○		✦	SR 1.13 punto 5.15.3 della norma A; CR 1.13 punto 5.15 della norma B.
MP2_6: override dell’autenticazione			○	Funzioni tipicamente manutentive ✦	✦	SR 2.1 RE 3 punto 6.3.3.3 della norma A.
MP2_7: mezzi e sistemi di autenticazione di macchina basati, se necessario, su dispositivi di security fisici	○	○	○	✦	✦	SR 1.1 punto 5.3.3 della norma A; CR 1.1 punto 5.3 della norma B.
MP2_8: privilegi degli utenti limitati a quelli strettamente indispensabili		○	○	Dipendenza dall’uso corretto del prodotto e addestramento specifico ✦	✦	SR 2.1 RE1 punto 6.3.3.1 della norma A; CCSC 3 Punto 4.4 della norma B.

Prospetto C.3: Mezzi fisici di protezione

Mezzo di protezione	SL_1s	SL_2s	SL_3s	Fabbricante e/o fornitore di componenti	Utilizzatore professionale	Riferimenti utili ed esempi
MP3_1: protezione degli accessi fisici ai punti di connessione del prodotto	Se MP5_4 non implementata ○	○	○	✦	Gestione delle politiche di conservazione dei mezzi da parte dell'utente finale ✦	SR 3.2 RE1 punto 7.4.3.1 della norma A.
MP3_2 disabilitazione di tutte le porte, le interfacce e i servizi esterni non utilizzati		○	Inefficace se accesso intenzionale	✦	✦	SR 3.2 RE1 punto 7.4.3.1 della norma A.

Prospetto C.4: Mezzi di protezione hardware

Mezzo di protezione	SL_1s	SL_2s	SL_3s	Fabbricante e/o fornitore di componenti	Utilizzatore professionale	Riferimenti utili ed esempi
MP4_1: firewall	○	○	○		✦	SR 3.2 RE1 punto 7.4.3.1 della norma A.
MP4_2: test funzionali	○	○	SR 3.3 RE1 necessario per raggiungere questo livello ○	Per validazione hardware del prodotto e/o del componente ✦	Per test funzionali delle IACS ✦	SR 3.3 RE1 punto 7.5.3 della norma A, per utilizzatore professionale. CR 3.3 punto 7.5.2 e RESS 1.1.2 e) Regolamento (UE) 2023/1230 per costruttore e/o fornitore di componenti.

Prospetto C.5: Mezzi di protezione software

Mezzo di protezione	SL_1s	SL_2s	SL_3s	Fabbricante e/o fornitore di componenti	Utilizzatore professionale	Riferimenti utili ed esempi
MP5_1: sistemi automatici di verifica delle funzionalità dei sistemi di sicurezza	○	○	SR 3.3 RE1 necessario per raggiungere questo livello ○	✦	Se applicabile alle risorse del prodotto ✦	SR 3.3 punto 7.5.3 della norma A per utente finale.
MP5_2: aggiornamento periodico dei software di protezione del prodotto	necessaria per questo livello ○	necessaria per questo livello ○	NECESSARIA PER questo livello ○		✦	SR 3.2 punto 7.4 della norma A per utente finale.
MP5_3: aggiornamento periodico dei software di controllo del prodotto	○	○	Necessaria per raggiungere questo livello ○	Consenso da parte del costruttore del prodotto ✦	✦	
MP5_4: restrizione alla installazione ed esecuzione dei codici portabili	○	○	Aggiungere controllo di integrità del codice prima dell'esecuzione per raggiungere questo livello ○	✦	✦	SR 2.4 punto 6.6 della norma A per utente finale. CR 2.4 punto 6.6 della norma B.
MP5_5: sistemi di log degli eventi di sicurezza	○	○	Aggiungere monitoraggio continuo SR 6.2 per raggiungere questo livello ○	✦	✦	SR 6.1 punto 10.3 della norma A per utilizzatore professionale. RESS 1.1.9 Regolamento (UE) 2023/1230 per costruttore e/o fornitore di componenti.

Mezzo di protezione	SL_1s	SL_2s	SL_3s	Fabbricante e/o fornitore di componenti	Utilizzatore professionale	Riferimenti utili ed esempi
MP5_6: sistemi di autenticazione dei dispositivi e dei software			Necessario per raggiungere questo livello ○	✦	✦	SR 1.2 punto 5.4 della norma A per utilizzatore professionale. RESS 1.1.9 Regolamento (UE) 2023/1230 per costruttore e/o fornitore di componenti.

Prospetto C.6: Architettura delle IACS

Mezzo di protezione	SL_1s	SL_2s	SL_3s	Fabbricante e/o fornitore di componenti	Utilizzatore professionale	Riferimenti utili ed esempi
MP6_1: riduzione della complessità del sistema informatico del prodotto	○	○	Aggiungere avvisi di raggiungimenti di soglia per raggiungere questo livello ○	✦	✦	CR 2.9 punto 6.11 della norma B, soglie di avviso punto 6.11.3 della norma B.
MP6_2: realizzazione della topologia del sistema informatico	○	○	Aggiungere SR5.1 RE2 per raggiungere questo livello ○	✦	✦	SR 5.1 RE1 punto 9.3.3.1 della norma A e CR 5.1 punto 9.3 della norma B per utilizzatore professionale. UNI EN ISO 13849-1:2023 per costruttore.
MP6_3: le funzioni essenziali di sicurezza per le singole zone della IACS (*)	○	○	Aggiungere SR5.1 RE2 per raggiungere questo livello ○	✦		SR 5.2 punto 9.4 della norma A per utilizzatore professionale.
MP6_4: partizione delle applicazioni a livello di zona	○	○	○		✦	SR 5.4 punto 9.6 della norma A. CR 5.4 punto 9.6 della norma B.

Mezzo di protezione	SL_1s	SL_2s	SL_3s	Fabbricante e/o fornitore di componenti	Utilizzatore professionale	Riferimenti utili ed esempi
MP6_5: mezzi per il management delle risorse del prodotto	○	○	○	✦	precedenza ai i codici/servizi real time di macchina ✦	SR 7.2 punto 11.4.1 della norma A. CR 7.2 punto 11.4 della norma B.
(*) La chiusura della comunicazione fra zone può essere efficacemente utilizzata in tutti i livelli come reazione del sistema IACS industriale per preservare le funzionalità di zone non ancora attaccate.						

Prospetto C.7: Reazione delle risorse agli attacchi

Mezzo di protezione	SL_1s	SL_2s	SL_3s	Fabbricante e/o fornitore di componenti	Utilizzatore professionale	Riferimenti utili ed esempi
MP7_1: validazione dei valori in ingresso al sistema informatico	○	○	○	✦	✦	SR 3.5 punto 7.7.1 della norma A per utilizzatore professionale. CR 3.5 punto 7.6.4 della norma B.
MP7_2: mezzi che portino la risorsa in uno stato sicuro	○	○	○	✦	✦	SR 3.6 punto 7.8 della norma A per utilizzatore professionale e CEI EN 60204-1:2018 categorie di arresto per il costruttore.
MP7_3: controllo locale	○	○	○	✦	✦	Ad esempio per il wireless: CR 2.2 punto 6.4 della norma B per utilizzatore e CEI EN 62745:2017 per costruttore del prodotto.
MP7_4: mezzi per arrestare i movimenti pericolosi del prodotto	○	○	○	✦		UNI EN ISO 13850:2015 per costruttore.
MP7_5: mezzi per il monitoraggio e la gestione dei carichi di rete da e verso il prodotto		○	Necessario per raggiungere questo livello ○		✦	Vedere SR7.1 RE1 punto 11.3.3.1 della norma A

Prospetto C.8: Altre misure di protezione

Mezzo di protezione	SL_1s	SL_2s	SL_3s	Fabbricante e/o fornitore di componenti	Utilizzatore professionale	Riferimenti utili ed esempi
MP8_1: mezzi diagnostici	○	○	○	✦	✦	CR 2.8 punto 6.10 della norma B.
MP8_2: restrizione ai sistemi di comunicazione condivisi tra utenti	○	○	Proibizione necessaria per raggiungere questo livello ○		✦	SR 5.3 punto 9.5.2 della norma A. CR 5.3 punto 9.5 della norma B.
MP8_3: sistemi di controllo legati alla sicurezza	○	○	○	✦		UNI EN ISO 13849-1:2023 o CEI EN IEC 62061:2023.

Appendice D (informativa) - Esempi di pericoli di natura informatica

Nella presente appendice viene riportata una lista non esaustiva con esempi di pericoli (cioè di vulnerabilità che possono essere sfruttate dalle minacce) di natura informatica (riassunti nel prospetto D.1) e una loro rappresentazione in forma matriciale:

1) pericoli interni al prodotto: riguardano i componenti direttamente installati sul prodotto che possono essere soggetti a vulnerabilità:
   a. dispositivi di controllo: HMI (Human-Machine Interface), PLC (Programmable Logic Controller), Drive, Switch e altri componenti critici;
   b. sensori e attuatori: possibile manipolazione dei segnali o guasti che compromettono la sicurezza e il funzionamento del prodotto;
2) pericoli interni all'organizzazione: questi pericoli derivano dall'interconnessione tra macchinari e altri sistemi aziendali:
   a. macchine collegate tra loro: reti di macchine che condividono dati e comandi, con il rischio di propagazione di guasti o attacchi informatici;
   b. integrazione con i sistemi aziendali: scambio di dati tra i prodotti e l'infrastruttura IT aziendale, come SCADA (Supervisory Control and Data Acquisition), MES (Manufacturing Execution System), ERP (Enterprise Resource Planning). La comunicazione tra questi sistemi può introdurre vulnerabilità;
3) pericoli esterni: minacce derivanti da connessioni con servizi e infrastrutture esterne:
   a. servizi cloud e raccolta dati: possibili esposizioni derivanti dall'invio di dati di produzione a piattaforme di analisi o gestione remota;
   b. teleassistenza e accessi remoti: connessioni per manutenzione da remoto che, se non adeguatamente protette, possono costituire un punto d'ingresso per attacchi informatici.

Prospetto D.1: Esempio di tabella riassuntiva dei pericoli

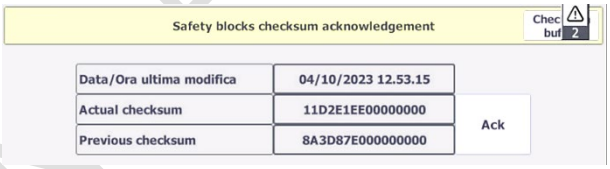
Rif.	Tipo o gruppo	Origine	Esempi di possibili conseguenze
1	interni al prodotto	porta USB	attacco malware
		porta di rete	attacco DoS
		protocollo Modbus	attacco *man-in-the-middle*
		firmware	vulnerabilità sfruttabile per exploit
		memoria PLC	manipolazione dei parametri di controllo
		protocollo Ethernet IP	intercettazione, malware
		comunicazione tra più PLC (macchine collegate tra loro)	malware, accesso illegittimo, malfunzionamento
		sistema di sicurezza in autoapprendimento	accesso illegittimo, malfunzionamento
		software di gestione macchina	accesso illegittimo, dati corrotti

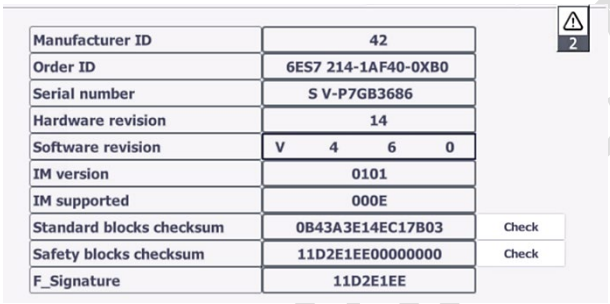
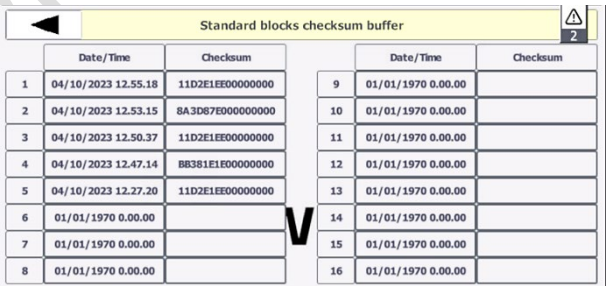
Rif.	Tipo o gruppo	Origine	Esempi di possibili conseguenze
2	interni alla organizzazione	operatori umani	phishing, propagazione malware alla macchina, danneggiamento macchina, errore umano
		comunicazione tra più PLC (macchine collegate tra loro)	accesso illegittimo
		account con privilegi eccessivi	possibile abuso o accesso non autorizzato
		firewall	configurazione errata, accesso involontario a sistemi critici
		rete dati interna	accesso illegittimo
		software di gestione sistema	accesso illegittimo, dati corrotti
3	esterni	teleassistenza	propagazione malware
		connessione con MES	intercettazione di informazioni, malware
		interconnessione con fornitori terzi	malware
		servizi cloud	esfiltrazione di dati sensibili
		rete esterna (es. infrastruttura, WAN)	malware, DoS, accesso illegittimo

Appendice E (informativa) - Esempio di protezione dall'alterazione del software e della tracciabilità

Il Regolamento Macchine (UE) 2023/1230 [3] riporta due specifici RESS per questo specifico ambito: il RESS 1.1.9 e il RESS 1.2.1. Nel Prospetto E.1 sono riportati alcuni estratti dei RESS ed esempi di soluzioni tecniche applicabili.

Prospetto E.1: Esempi di protezione dall'alterazione del software e della tracciabilità

Estratti del Regolamento Macchine (UE) 2023/1230	**Esempi di soluzioni tecniche applicabili**
RES 1.1.9 Protezione dall'alterazione	
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.	
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 devono essere individuati come tali e devono essere adeguatamente protetti da un'alterazione accidentale o intenzionale.	Tutto il software del prodotto legato alla sicurezza è protetto da password, si consiglia l'implementazione di una password forte e con un checksum o codice univoco di identificazione della versione.  Una password forte è una combinazione di caratteri difficile da indovinare o decifrare, progettata per proteggere gli account, le informazioni o software da accessi non autorizzati. Ecco le caratteristiche principali di una password forte: • lunghezza: dovrebbe essere lunga almeno tra 8 e 12 caratteri, ma più è lunga, meglio è. • complessità: dovrebbe includere una combinazione di lettere maiuscole e minuscole, numeri e simboli speciali. • unicità: non dovrebbe contenere parole di uso comune, informazioni personali (come date di nascita o nomi) o sequenze facilmente prevedibili. • casualità: i caratteri dovrebbero essere disposti in modo casuale, senza seguire schemi o sequenze logiche.
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.	La funzione da implementare può verificare ad intervalli di tempo definiti, ad esempio ogni 8 ore o al successivo riavvio, il codice univoco o la versione del software, sia safety che standard, installati nel prodotto. In caso di discrepanza tra le versioni, il software, ad esempio con un messaggio sul pannello operatore, potrebbe richiedere un consenso esplicito, con un livello di user e password idoneo, per validare la modifica e quindi l'uso della nuova versione software (pulsante "Ack" della prima immagine di esempio). Senza questa conferma, il prodotto rimane bloccato in stato sicuro.

Estratti del Regolamento Macchine (UE) 2023/1230	Esempi di soluzioni tecniche applicabili
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.	Il software del PLC, CNC o IPC può raccogliere e visualizzare a pannello operatore la versione Hardware, Numero di serie, Firmware e versione del software standard e di sicurezza, installato sul prodotto. 
RES 1.2.1 Sicurezza ed affidabilità dei sistemi di comando	
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.	Il prodotto registra, in un log di sistema protetto, tutte le versioni dei software di sicurezza modificate nel tempo, in uno spazio di archiviazione. Questo log, identificato anche con data e versione, permette di monitorare le modifiche che sono state apportate durante gli aggiornamenti del prodotto. Questo sistema di log deve consentire di archiviare le informazioni, nella propria memoria e per tutto il ciclo di vita del prodotto o, almeno, per un periodo minimo di 5 anni e deve essere protetto da alterazioni. 

Appendice F (informativa) - Inventario delle Risorse

Per creare un inventario completo ed esaustivo delle risorse del prodotto, è consigliato raccogliere le seguenti informazioni per ciascuna classe di risorse. Le indicazioni fornite di seguito sono da intendersi come esemplificative e non vincolanti:

- Hardware: per le risorse hardware, come PLC, HMI, router e workstation, si dovrebbero includere:
  - nome del dispositivo o sistema;
  - ID della risorsa;
  - tipo di dispositivo;
  - funzione;
  - interfaccia/e di rete;
  - indirizzo/i di rete;
  - produttore;
  - modello;
  - numero di serie;
  - versione del sistema operativo e del firmware;
  - organizzazione o persona responsabile;
  - posizione fisica;
  - note.

- Macchine Virtualizzate: per le risorse virtualizzate, come le macchine virtuali (VM), si dovrebbero includere:
  - nome della VM;
  - tipo di VM;
  - funzione;
  - interfaccia di rete;
  - indirizzo di rete;
  - nome/ID dell'host;
  - tipo di host;
  - sistema operativo e versione;
  - organizzazione o persona responsabile;
  - responsabile amministrativo;
  - note.

- Software: per i software applicativi, si dovrebbero includere:
  - nome del software;
  - tipo di software (es. sistema operativo, applicazione, database, firmware);
  - funzione del software;
  - nome/ID dell'host associato;
  - tipo di host (fisico o virtuale; server, workstation, dispositivo di rete, controller, ecc.);
  - fornitore;
  - versione;
  - persona o organizzazione responsabile;
  - informazioni sulla licenza;
  - numero di licenze disponibili;

- localizzazione della licenza (installazione o archivio);
- scadenza della licenza;
- stato di aggiornamento/patch.

Appendice G (informativa) - Esempio di valutazione del rischio

Il prospetto G.1 propone un modello utile per strutturare il risultato di valutazione del rischio.

Prospetto G.1: Modello di valutazione del rischio

Rif.	IDENTIFICAZIONE RISCHI							RISCHIO NON MITIGATO			Misure protettive implementate	RISCHIO RESIDUO			
	Tipo o gruppo	Origine	Vettore di attacco	Evento	Ciclo di vita	Operatore	Conseguenza	Impatto	Probabilità	Entità di rischio		Impatto	Frequenza	Totale	SL-A
1															
2															
3															

BIBLIOGRAFIA

1) Circolare 4/E del 30 marzo 2017 dell'Agenzia delle Entrate e del Ministero dello Sviluppo Economico, Industria 4.0 - Articolo 1, commi da 8 a 13, della legge 11 dicembre 2016, n. 232 - Proroga, con modificazioni, della disciplina del c.d. "super ammortamento" e introduzione del c.d. "iper ammortamento"

2) Direttiva 2006/42/CE del Parlamento Europeo e del Consiglio del 17 maggio 2006 relativa alle macchine e che modifica la direttiva 95/16/CE (rifusione) pubblicato il 29 giugno 2023 sulla Gazzetta Ufficiale dell'Unione Europea

3) Regolamento (UE) 2023/1230 del Parlamento Europeo e del Consiglio del 14 giugno 2023, relativo alle macchine e che abroga la direttiva 2006/42/CE del Parlamento europeo e del Consiglio e la direttiva 73/361/CEE del Consiglio, pubblicato il 29 giugno 2023 sulla Gazzetta Ufficiale dell'Unione Europea

4) Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza»), pubblicato il 7 giugno 2019 sulla Gazzetta Ufficiale dell'Unione Europea

5) Regolamento (UE) 2024/2847 del Parlamento Europeo e del Consiglio del 23 ottobre 2024 (Regolamento sulla Ciberresilienza – Cyber Resilience Act), 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, pubblicato il 20 novembre 2024 sulla Gazzetta Ufficiale dell'Unione Europea

6) D. Lgs. 9 aprile 2008, n. 81, Testo unico sulla salute e sicurezza sul Lavoro, attuazione dell'articolo 1 della Legge 3 agosto 2007, n. 123 in materia di tutela della salute e della sicurezza nei luoghi di Lavoro

UNI/TR 11749:2020, Tecnologie Abilitanti per Industry 4.0 - Integrazione ed interconnessione: aspetti principali ed esempi

UNI EN ISO 11161:2010, Sicurezza del macchinario - Sistemi di fabbricazione integrati – Requisiti di base

UNI EN ISO 12100:2010, Sicurezza del macchinario - Principi generali di progettazione - Valutazione del rischio e riduzione del rischio

UNI EN ISO 13849-1:2023, Sicurezza del macchinario - Parti dei sistemi di comando legate alla sicurezza - Parte 1: Principi generali per la progettazione

UNI EN ISO 13850:2015, Sicurezza del macchinario - Funzione di arresto di emergenza - Principi di progettazione

UNI EN ISO 16090-1:2023, Sicurezza delle macchine utensili - Centri di lavoro, fresatrici, macchine transfer - Parte 1: Requisiti di sicurezza

UNI CEN ISO/TR 22100-4:2021, Sicurezza del macchinario - Relazione con la ISO 12100 - Parte 4: Guida ai fabbricanti di macchinari per la considerazione degli aspetti relativi alla sicurezza IT (sicurezza informatica)

IEC/TS 62443-1-1:2009, Industrial communication networks - Network and system security - Part

1-1: Terminology, concepts and models

ISO/IEC Guide 51:2014, Safety aspects — Guidelines for their inclusion in standards

CEI EN 60204-1:2018, Sicurezza del macchinario - Equipaggiamento elettrico delle macchine Parte 1: Regole generali

CEI EN IEC 62061:2023, Sicurezza del macchinario - Sicurezza funzionale dei sistemi di comando e controllo relativi alla sicurezza

CEI EN IEC 62443-3-2:2021, Sicurezza dei sistemi di automazione industriale e controllo - Parte 3-2: Valutazione del rischio di sicurezza nel progetto di sistema

CEI EN IEC 62443-3-3:2020, Reti di comunicazione industriale - Sicurezza di rete e di Sistema - Parte 3-3: Requisiti per la sicurezza informatica e i livelli di sicurezza informatica di sistema

CEI EN IEC 62443-4-2:2019, Sicurezza dei sistemi di automazione industriale e di controllo - Parte 4-2: Requisiti tecnici di sicurezza per componenti IACS

CEI EN 62745:2017, Sicurezza del macchinario - Prescrizioni per i sistemi di comando e controllo senza fili del macchinario

CEI CLC/IEC/TS 63074:2024: Sicurezza del macchinario - Aspetti di sicurezza relativi alla sicurezza funzionale dei sistemi di controllo correlati alla sicurezza