QUADRA
Consulenza e Formazione

Cybersecurity applicata alle macchine

Ernesto Cappelletti

21 novembre 2024

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

Rischi provocati da attacchi informatici

Regolamento (UE) 2023/1230 (considerando 25)

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

Protezione dall'alterazione

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

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

Protezione dall'alterazione

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

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

Sicurezza ed affidabilità dei sistemi di comando

Regolamento (UE) 2023/1230 (allegato III, §1.2.1)

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

CEI CLC/IEC/TS 63074:2024

N O R M A I T A L I A N A C E I

Norma Italiana

CEI CLC/IEC/TS 63074

La seguente Norma è identica a: CLC/IEC/TS 63074:2024-02

Data Pubblicazione

2024-04

Titolo

Sicurezza del macchinario - Aspetti di sicurezza relativi alla sicurezza funzionale dei sistemi di controllo correlati alla sicurezza

Title

Safety of machinery - Security aspects related to functional safety of safety-related control systems

UNI CEN ISO/TR 22100-4:2021

RAPPORTO TECNICO

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)

UNI CEN ISO/TR 22100-4

MARZO 2021

Safety of machinery - Relationship with ISO 12100 - Part 4: Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects

Il rapporto tecnico fornisce una guida ai fabbricanti di macchine sui potenziali aspetti di sicurezza in relazione alla sicurezza del macchinario quando si mette in servizio o si immette sul mercato una macchina per la prima volta. Esso fornisce informazioni essenziali per identificare e affrontare le minacce alla sicurezza IT che possono influenzare la sicurezza del macchinario.
Il rapporto tecnico fornisce una guida ma non fornisce specifiche dettagliate su come affrontare gli aspetti di sicurezza informatica che possono influenzare la sicurezza del macchinario.
Il rapporto tecnico non affronta il bypass o il fallimento delle misure di riduzione del rischio attraverso la manipolazione fisica.

Campo di applicazione
UNI CEN ISO/TR 22100-4:2021 (§1)

- Il rapporto tecnico UNI CEN ISO/TR 22100-4:2021 fornisce indicazioni ai fabbricanti di macchine per **identificare e affrontare le minacce alla sicurezza informatica** che potrebbero influenzare la **sicurezza delle macchine**.
- Il documento fornisce una guida ma **non specifiche dettagliate** su come affrontare gli aspetti di sicurezza informatica che potrebbero influenzare la sicurezza delle macchine.

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

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

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

Stima del rischio (safety)
UNI EN ISO 12100:2010

- Il rischio associato ad una particolare situazione pericolosa dipende dai seguenti elementi:
  - la gravità del danno;
  - la probabilità che si verifichi tale danno, che è in funzione della:
    - esposizione della(e) persona(e) al pericolo;
    - accadimento di un evento pericoloso; e
    - possibilità tecniche e umane per evitare o limitare il danno.

Elementi del rischio (security)
UNI CEN ISO/TR 22100-4:2021 (§4.2)

RISCHIO

correlato alla minaccia considerata

è una funzione di

POSSIBILE IMPATTO NEGATIVO

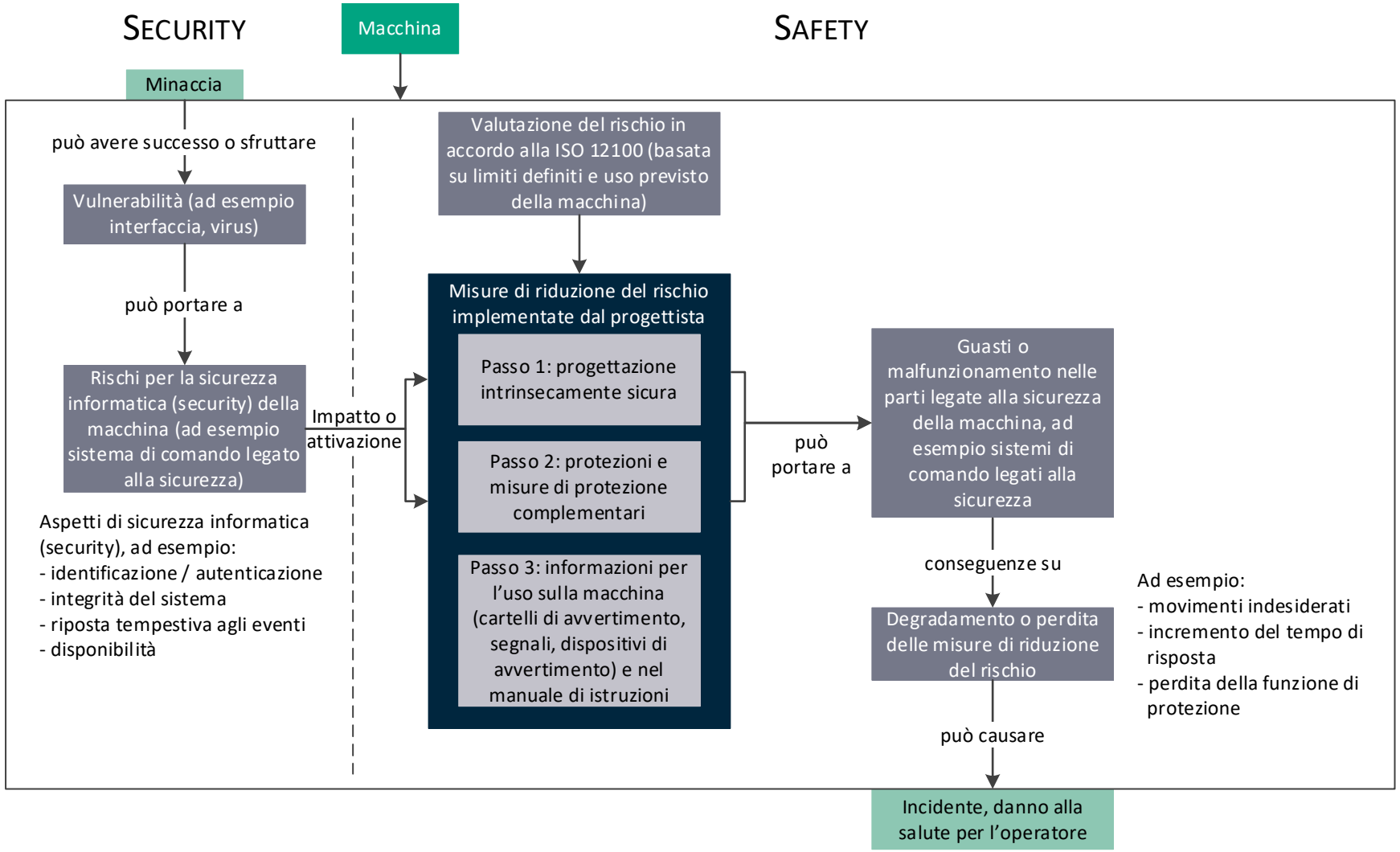
che può derivare dalla minaccia

e

PROBABILITÀ DI QUESTO IMPATTO NEGATIVO

in relazione alle vulnerabilità esistenti che possono essere sfruttate dalla minaccia

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



Caratteristiche degli attacchi informatici

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

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

- Rispondere alle seguenti domande può aiutare a limitare o restringere le minacce e le vulnerabilità della sicurezza informatica:
  - Deve essere collegato?
  - Deve essere sempre connesso (in modo continuo)?
  - La connessione è monitorata [ad esempio utilizzando una rete privata virtuale (VPN)]?
  - La connessione è configurabile (ad esempio accesso permesso solo a persone autorizzate)?
  - La connessione può essere limitata alla modalità “sola lettura” (senza possibilità di modifica)?

Metodologia di mitigazione
UNI CEN ISO/TR 22100-4:2021 (§6)

- I rischi per la sicurezza informatica possono essere mitigati attraverso gli sforzi combinati dei fornitori di componenti, del fabbricante della macchina, dell'integratore di sistema e dell'utilizzatore finale.
- In generale, le potenziali risposte ai rischi per la sicurezza informatica dovrebbero applicare la seguente gerarchia basata sulla UNI EN ISO 12100:2010:
  - eliminare il rischio per la sicurezza informatica in fase di progettazione (evitare le vulnerabilità);
  - mitigare il rischio per la sicurezza mediante misure di riduzione del rischio (mitigazione) (limitare le vulnerabilità);
  - fornire informazioni sul rischio residuo per la sicurezza informatica e sulle misure che devono essere adottate dall'utilizzatore.
- Misure aggiuntive potrebbero essere adeguate funzioni di controllo legate alla sicurezza (SRP/CS) per mitigare le conseguenze di una minaccia, ad esempio monitoraggio sicuro dei valori limite.

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

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

Passi per affrontare la IT-security
UNI CEN ISO/TR 22100-4:2021 (§7)

- **Identificare**
  - Quali sono le minacce informatiche?
  - Cosa ha di prezioso l'utilizzatore della macchina?
  - Quali sono le vulnerabilità della macchina (ad esempio porte aperte, interfacce esterne)?
  - Quali sono le risorse che supportano le funzioni critiche?
- **Proteggere**
  - Sviluppare e attuare le contromisure appropriate per proteggere la macchina.
  - Le contromisure supportano la capacità di prevenire, limitare o contenere l'impatto di un potenziale attacco alla sicurezza informatica.

Passi per affrontare la IT-security
UNI CEN ISO/TR 22100-4:2021 (§7)

- **Individuare**
  - Sviluppare e attuare le misure appropriate per identificare tempestivamente il verificarsi di un attacco informatico.
  - La violazione di un sistema informatico può rimanere nascosta e, quindi, difficile da rilevare anche dopo un attacco riuscito.
- **Rispondere**
  - Sviluppare e attuare le attività appropriate per agire in merito ad un attacco informatico rilevato, ovvero arrestare e contenere l'impatto di un potenziale attacco informatico.
- **Recuperare**
  - Sviluppare e implementare le attività appropriate per ripristinare eventuali capacità o servizi che sono stati danneggiati a causa di un attacco informatico.

Minacce alla sicurezza informatica e motivazioni

UNI CEN ISO/TR 22100-4:2021 (tabella 2)

Minaccia alla sicurezza informatica	Manipolazione di macchine e impianti	Rilevanza per la sicurezza delle macchine
Accesso a dati/know-how del fabbricante della macchina o dell'utilizzatore della macchina (know-how di processo)	Nessuna	Nessuna
Creazione di un danno economico per l'utilizzatore della macchina	Durante l'uso	Improbabile ma possibile
Creazione di pericoli per macchine e/o persone (operatore, passanti)	Durante l'uso	Improbabile ma possibile
Creazione di danni alle infrastrutture e/o alle persone (operatore, passanti), ad esempio un atto terroristico	Durante l'uso	Probabile

Guida per i fabbricanti di macchine
UNI CEN ISO/TR 22100-4:2021 (§10.2)

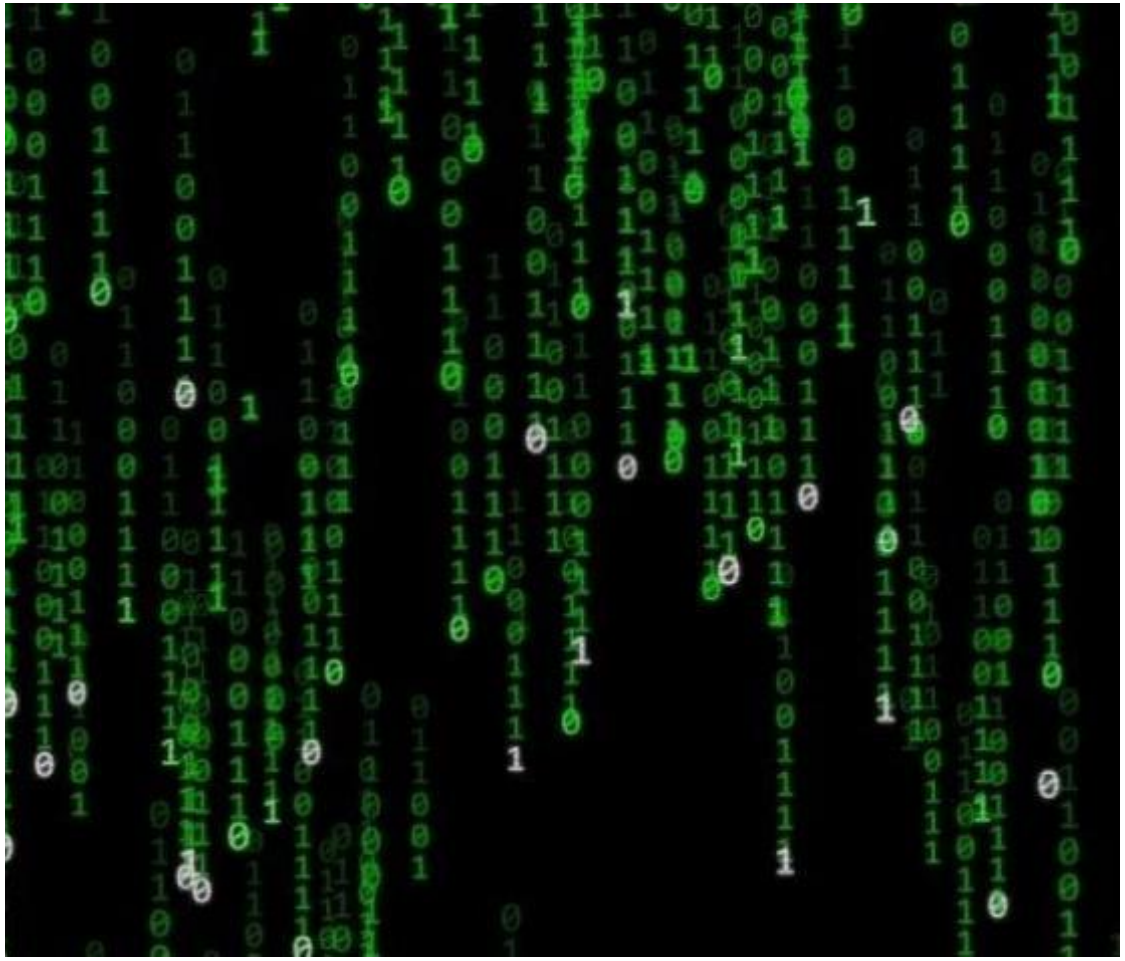
- Selezione di componenti appropriati (hardware / software)
  - I componenti / le parti della macchina relativi alla sicurezza (ad esempio sistemi di controllo, sensori, attuatori) che possono essere obiettivi di minacce informatiche dovrebbero avere funzionalità allo stato dell'arte, in grado di minimizzare la loro vulnerabilità rispetto a quelle possibili minacce.
  - Per esempio:
    - mezzi / misure di autenticazione per il controllo degli accessi (ad esempio lettori di carte, sistemi di password);
    - mezzi per l'aggiornamento del software;
    - mezzi per la comunicazione crittografata.

Guida per i fabbricanti di macchine
UNI CEN ISO/TR 22100-4:2021 (§10.3)

- Progettazione adeguata della macchina
  - In fase di progettazione, il fabbricante della macchina dovrebbe osservare principi / misure di base per ridurre al minimo la vulnerabilità delle parti relative alla sicurezza dell'intera macchina in relazione alle minacce informatiche.
  - Per esempio:
    - separare il più possibile il sistema informatico rilevante per la sicurezza dal sistema informatico globale della macchina;
    - dotare il sistema informatico della macchina di misure di riduzione dei rischi (ad esempio firewall, strumenti antivirus);
    - ridurre la complessità del sistema informatico della macchina (consentendo di affrontare meglio le possibili minacce informatiche);
    - realizzare una topologia del sistema informatico della macchina con livelli multipli e indipendenti (riducendo la vulnerabilità);
    - dotare la macchina di mezzi per rilevare componenti del sistema informatico essenziali per la sicurezza non funzionanti correttamente;
    - dotare la macchina di mezzi che la portino in uno stato sicuro nel caso in cui un componente del sistema informatico essenziale per la sicurezza non funzioni correttamente.

Sicurezza informatica
UNI EN ISO 20607:2019 (§4.11)

- La norma UNI EN ISO 20607:2019 fa riferimento al rapporto tecnico UNI CEN ISO/TR 22100-4:2021.
  - *Se possibile, il manuale di istruzioni deve contenere informazioni sulle vulnerabilità per la sicurezza IT. Vedere il punto 10.4 dell'**ISO/TR 22100-4:2018**.*



Sicurezza informatica nel manuale di istruzioni
UNI CEN ISO/TR 22100-4:2021 (§10.4)

- Il manuale di istruzioni deve contenere **indicazioni / raccomandazioni** adeguate su **come affrontare i problemi di sicurezza informatica** durante l'uso della macchina:
  - **Limitazione dell'accesso logico / fisico** ai sistemi informatici (con possibile influenza sulla sicurezza):
    - Utilizzare sistemi informatici interni con misure di riduzione del rischio (mitigazione) (ad esempio firewall, antivirus).
    - Mantenere le misure di riduzione del rischio (mitigazione) del sistema informatico in una modalità effettivamente sicura (implementare aggiornamenti dei fabbricanti di macchine / componenti).
    - Utilizzare i meccanismi di autenticazione e controllo degli accessi forniti (ad esempio lettori di schede) secondo le specifiche del fabbricante della macchina / dei componenti.
    - Limitare i privilegi dell'utente del sistema informatico solo a quelli richiesti per il ruolo di ogni persona.
    - Disabilitare tutte le porte / interfacce e i servizi esterni non utilizzati.
    - Adottare account utente individuali e gestirli adeguatamente (ad esempio aggiornamento delle password).

Sicurezza informatica nel manuale di istruzioni
UNI CEN ISO/TR 22100-4:2021 (§10.4)

- **Rilevamento e reazione ad incidenti** relativi alla sicurezza informatica (con possibile influenza sulla sicurezza):
  - Controllare regolarmente i mezzi forniti per rilevare componenti del sistema informatico guasti o servizi non disponibili secondo le specifiche del fabbricante della macchina / dei componenti.
  - Essere reattivo alle nuove vulnerabilità (risultanti da un attacco informatico (minaccia)).
- In caso di **manutenzione ed assistenza a distanza**:
  - Utilizzare i mezzi forniti per attivare e terminare una sessione di accesso remoto in base alle specifiche del fabbricante della macchina / dei componenti.
  - Utilizzare trasmissioni crittografate per avviare una manutenzione remota / servizio remoto in base a specifiche del fabbricante della macchina / dei componenti.
  - Sorvegliare qualsiasi sessione di accesso remoto (limitazione della durata dell'accesso remoto).

Nuovo progetto di norma ‘Protection against corruption’

prEN 50742

CENELEC

TC44X/Sec0362/INF
February 2024

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

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

Dear Members,

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

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

Nuovo progetto di norma ‘Protection against corruption’

prEN 50742

CLC/TC 44X

Date: 20YY-XX

prEN 50742:2024

Secretariat: BSI

Safety of Machinery— Electrotechnical aspect — Protection against corruption

??? — ???— DE???

!!! — !!! — FR!!!

QUADRA
Consulenza e Formazione

Grazie per l'attenzione

Ernesto Cappelletti

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