MEET IT

3CiME TECHNOLOGY ICT & INNOVATION

3CIME DAY

Sicurezza OT tra normative e *standard*: NIS2, ***C**yber **R**esilience **A**ct* e ISA/IEC 62443 per proteggere processi e prodotti

Argomenti di oggi

Differenze e sinergie tra IT e OT
La sicurezza dei servizi offerti e il supporto alla *compliance* dei clienti

NIS 2 applicata all'industria (Direttiva UE 2022/2555)
Misure tecniche, operative e organizzative adeguate e proporzionate per gestire i rischi

Regolamento Macchine (Regolamento UE 2023/1230)
Adeguata protezione da una alterazione accidentale o intenzionale

Cyber Resilience Act (Regolamento UE 2024/2847)
Requisiti Essenziali di CiberSicurezza

Standard ISA/IEC 62443 (livelli *Purdue*, zone e condotti)
2-1, 2–4, 3-2, 4-1, 4-2

Di processo **e** di prodotto (o servizio)

Gestione del rischio di sicurezza informatica

Gestione del rischio di sicurezza informatica sui prodotti e/o servizi offerti

Valutazione dei rischi, mitigazioni, rischi residui

Supporto ai clienti nella valutazione dei rischi, mitigazioni, rischi residui

Sicurezza della catena di approvvigionamento (e accessi remoti)

La sicurezza della catena di approvvigionamento dei clienti (e accessi remoti)

Piano di sicurezza degli *asset*, delle reti e delle comunicazioni

Supporto ai clienti nel piano di sicurezza degli *asset*, delle reti e delle comunicazioni

Monitoraggi (attivi e passivi), incidenti, notifiche, ripristino dei servizi

Proposta di servizi a supporto di monitoraggio, incidenti, notifiche, ripristino dei servizi

Il ciclo dell'eterno ritorno

Metodo iterativo per approssimazioni progressive

Giampietro Peghetti

ISA International Society of Automation
IEC International Electrotechnical Commission

Industrial CyberSecurity Expert

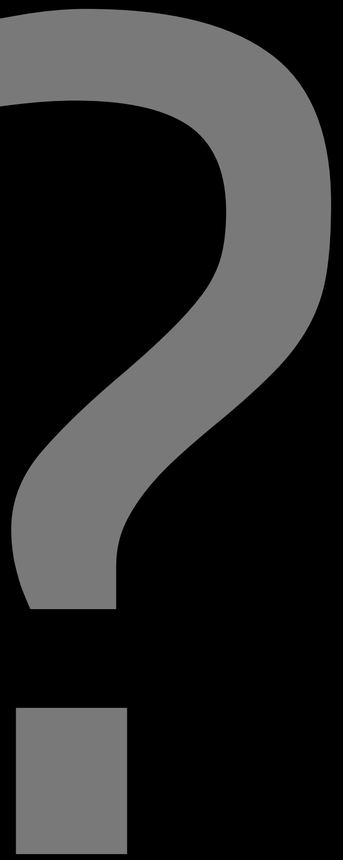
(ISC)² International Information System Security Certification Consortium

*CISSP **Certified** Information Systems Security Professional*

PMI Project Management Institute

*PMP® **P**roject **M**anagement Professional®*

Industrial CyberSecurity ~~Expert~~



Le
so
tutte!!!

L’unica cosa
che so
e di
non sapere
niente.

La finestra di Johari

AREA APERTA (IO APERTO)

Noto a sé / Noto agli altri

AREA CIECA (IO CIECO)

Ignoto a sé / Noto agli altri

Consulenza
Risk Assessment

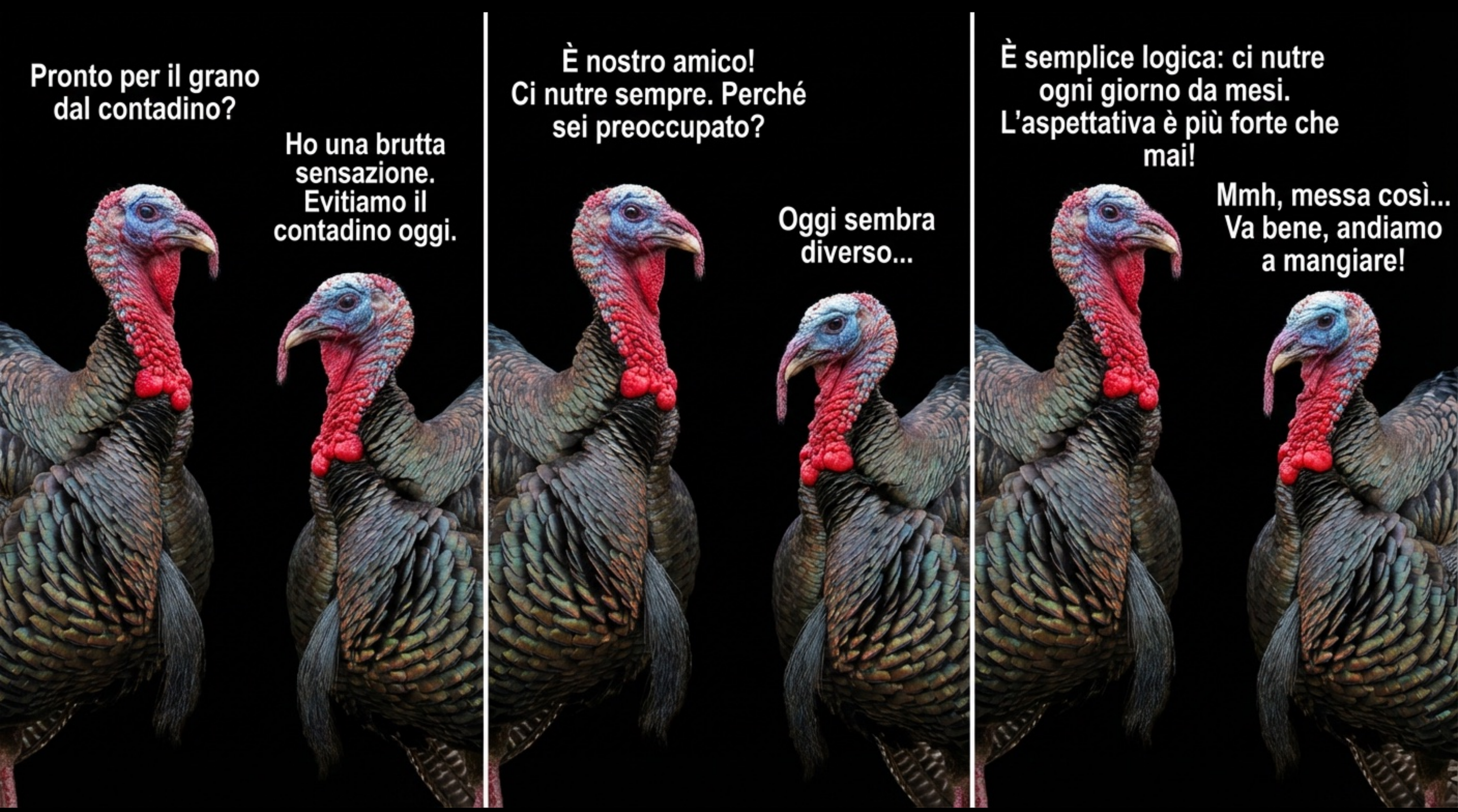
AREA NASCOSTA (IO NASCOSTO)

Noto a sé / Ignoto agli altri

AREA IGNOTA (IO IGNOTO)

Ignoto a sé / Ignoto agli altri

Rischio residuo
"Zero"


Pronto per il grano dal contadino?
Ho una brutta sensazione. Evitiamo il contadino oggi.
È nostro amico! Ci nutre sempre. Perché sei preoccupato?
Oggi sembra diverso...
È semplice logica: ci nutre ogni giorno da mesi. L'aspettativa è più forte che mai!
Mmh, messa così... Va bene, andiamo a mangiare!

Chi sono **oggi**
qui presenti
i più grandi (e forse i soli) **esperti**
di sicurezza informatica industriale?

Gestione, Rischio, Compliance (GRC)

Risorse umane (HR)

Marketing

Sales

Progettazione (R&D)

Ufficio acquisti

Produzione

Logistica e magazzino

Servizio clienti

Ingegneria e Manutenzione

Amministrazione e finanza

Sicurezza e Ambiente

Qualità

Diventare ***hacker*** di se stessi

Risorse umane (HR)

Marketing

Sales

Progettazione (R&D)

Ufficio acquisti

Produzione

Logistica e magazzino

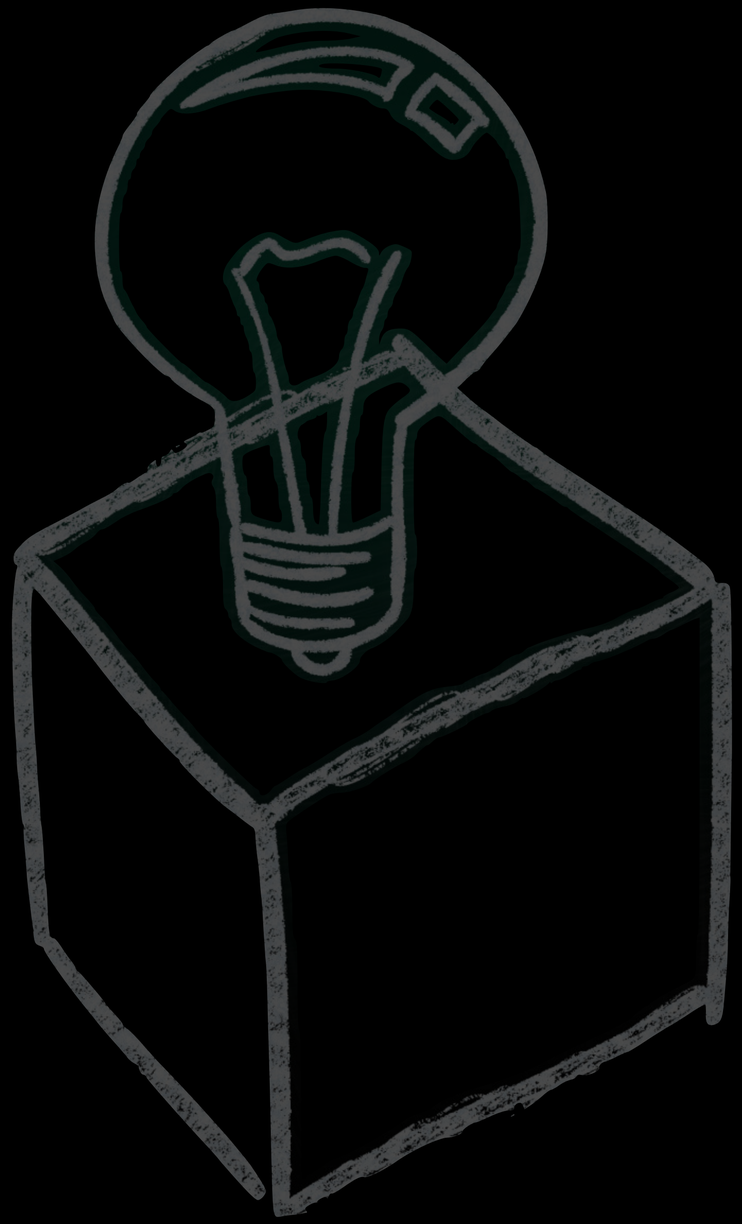
Servizio clienti

Ingegneria e Manutenzione

Amministrazione e finanza

Sicurezza e Ambiente

Qualità

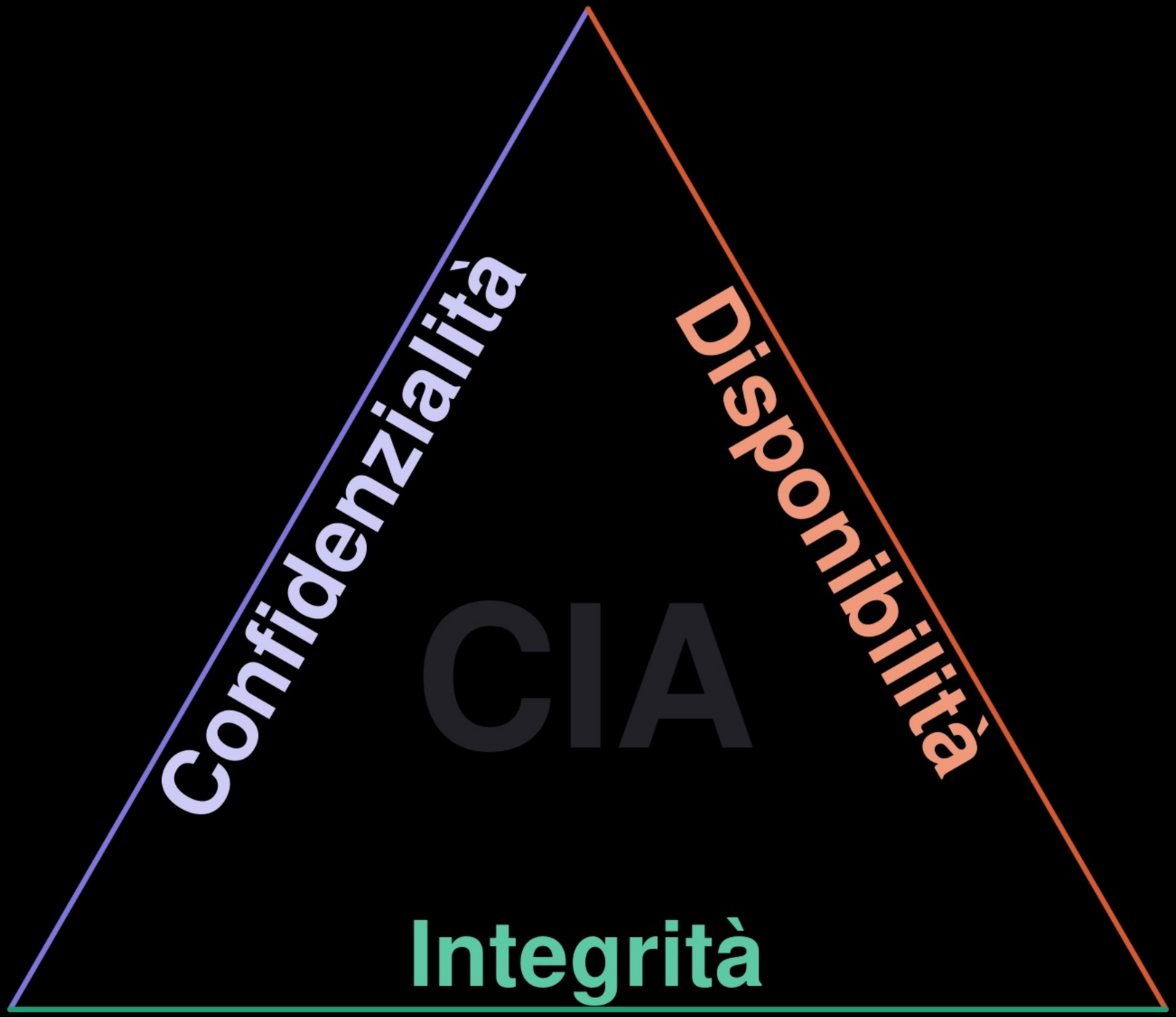


La sicurezza informatica
è passata alla difesa dei
dati

IT

OT

alla difesa di **dati**,
di **processi** e **prodotti**,
elementi tipici
del mondo industriale
(**sistemi fisici**)


Confidenzialità
Disponibilità
CIA
Integrità

N. RICHIAMO (KBA)
16265R

Mercedes-Benz

Difetto del fissaggio delle ruote

Dati principali

Marca	**Mercedes-Benz**
Riferimento KBA	**16265R**
Codice costruttore	**4090105**
Pubblicato	**18/05/2026**
Periodo di produzione	**17/11/2022 – 04/12/2025**
Veicoli interessati (Germania)	**2.712**
Veicoli interessati (mondo)	**2.712**
Sorveglianza KBA	**monitorato**
Incidenti noti	**nessuno**

Descrizione del difetto

Le viti delle ruote non sono state serrate alla coppia di serraggio prevista. Durante la marcia le viti e, di conseguenza, l'intero gruppo ruota potrebbero allentarsi.

Rimedio

Sui veicoli interessati il gruppo ruota viene controllato e, se necessario, ripristinato secondo le specifiche.

Modelli interessati (25)

Classe A	**Classe A AMG**	**Classe B**	**Classe C**	**Classe C AMG**
CLA	**CLA AMG**	**CLE**	**Classe E**	**Classe E AMG**
EQA	**EQB**	**EQE**	**EQE AMG**	**EQS**
Classe G	**GLA**	**GLA AMG**	**GLB**	**GLB AMG**
GLE	**GLE AMG**	**Classe S**	**SL**	**SL AMG**

Security

Safety

Un rischio ***cyber*** può influire sulla ***safety***?

Regolamento (UE) 2023/988

GPSR (General Product Safety Regulation)

*Art. 6: «1. a) Nel valutare se un prodotto è sicuro [**safe**],*
si prendono in considerazione in particolare gli aspetti seguenti: [...]

g) laddove lo imponga la natura del prodotto,
le adeguate caratteristiche di cibersicurezza *necessarie*
per proteggere il prodotto da ***influenze esterne****,*
compresi terzi malintenzionati,
*se tale influenza potrebbe avere un impatto sulla sicurezza [**safety**] del prodotto,*
compresa la possibile perdita di interconnessione».

Un rischio ***cyber*** può influire sulla ***safety***?

Regolamento (UE) 2023/1230

“Regolamento Macchine”

Allegato III, 1.1.9: «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 [...]

*non determini una situazione pericolosa [**hazardous situation**].*

I componenti hardware che trasmettono segnali o dati [...]

devono essere progettati in modo tale da essere

adeguatamente protetti da un’alterazione accidentale o intenzionale».

Process Hazard Analysis (**PHA**)
Hazard and Operability studies (**HAZOP**)

Un rischio ***cyber*** può influire sulla ***safety***?

Regolamento (UE) 2023/1230

“Regolamento Macchine”

Allegato III, 1.2.1: «I sistemi di comando
devono essere ***progettati e costruiti***
in modo tale che riescano a resistere […]
ad ***influssi esterni intenzionali o meno****,*
compresi ***tentativi deliberati ragionevolmente prevedibili*** *da parte di terzi*
*che conducono a una situazione pericolosa [****hazardous situations****]».*

Process Hazard Analysis (**PHA**)
Hazard and Operability studies (**HAZOP**)

Un rischio ***cyber*** può influire sulla ***safety***?

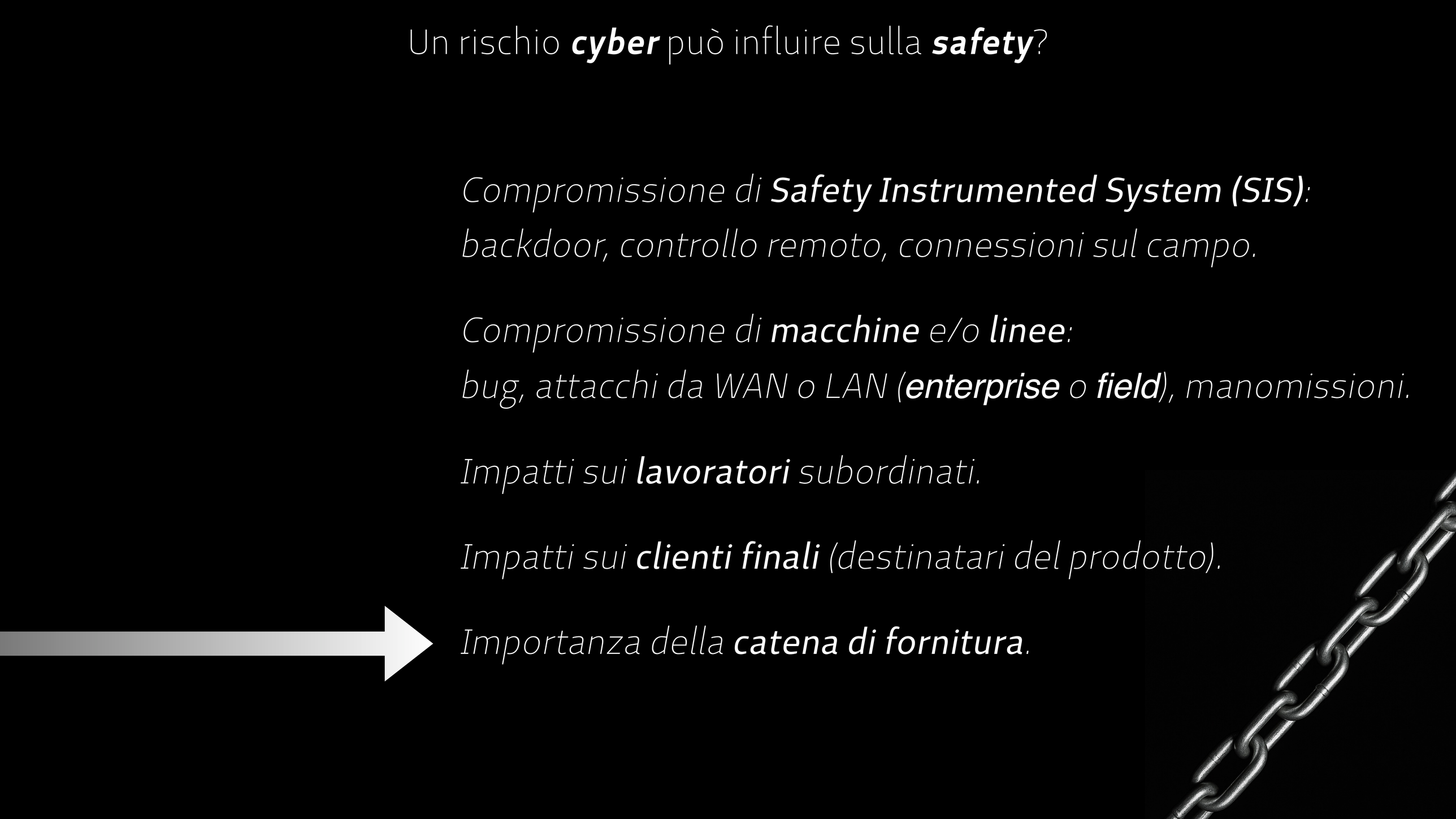
Compromissione di **Safety Instrumented System (SIS)**:
backdoor, controllo remoto, connessioni sul campo.

Compromissione di **macchine** *e/o* **linee**:
*bug, attacchi da WAN o LAN (***enterprise*** *o* ***field****), manomissioni.*

Impatti sui **lavoratori** *subordinati.*

Impatti sui **clienti finali** *(destinatari del prodotto).*

Importanza della **catena di fornitura**.



Le macchine (di produzione, o mie produzioni) possono essere attaccate da remoto?

- Sì, sempre.
- Sì, ma solo se sono connesse alla rete degli uffici.
- Potrebbe essere, anche ad insaputa di chi le usa.
- No, in nessun modo, perché le macchine sono isolate.

Le linee produttive (o le mie produzioni con software) possono essere attaccate da qualcuno in presenza?

- Sì, sempre, perché molte macchine delle linee hanno i sistemi di controllo tipicamente e a tutti gli operatori, o via cavo o via wireless.
- Sì, ma solo se sono presenti computer con tastiera e mouse ad uso degli operatori.
- Non ne sono sicuro: dovrei controllare se ci sono porte aperte.
- No, in nessun modo, perché i sistemi di controllo sono sempre inaccessibili agli operatori.

Il *software* (o il suo comportamento) può essere alterato?

- Sì, ma solo se il computer del programmatore è stato compromesso.
- Sì, ma solo dal programmatore o da chi ha il codice sorgente, e solo se ha accesso diretto al sistema di controllo (PLC o altro).
- No, a meno di situazioni impreviste, accidentali o meno.
- No, in nessun modo: i software delle macchine non prevedono aggiornamenti programmati in quanto sono stati validati in fase di consegna e sono risultati privi di bug.

Le componenti *hardware* (*chipset*, RAM, schede) possono essere alterate nel loro comportamento?

- Sì, potenzialmente in qualunque fase di lavorazione o utilizzo.
- Sì, ma solo da chi le ha prodotte.
- Sì, ma ci se ne accorgerebbe, per cui non ci sarebbe nessuna conseguenza di rilievo.
- No, in nessun modo: sono oggetti sicuri by design e by default.

Se qualcuno si fa male (in produzione o nell'utilizzo di un prodotto con software), è un problema?

- Sì, perché ci sono sempre conseguenze legali per il produttore.
- Sì, perché si ferma la produzione e/o ci sono danni almeno reputazionali per l'azienda.
- Forse sì, ma comunque non è una casistica che può portare ad una segnalazione obbligatoria alle autorità.
- Non è un problema vero: se si utilizza un oggetto fisico, è normale che ci si possa far male, e le cause di questo tipo sono solo temerarie.

Security

Safety

Production Safety

NIS 2
Industrial

Framework

D.Lgs. 82/2005	CAD
2014/910	Regolamento eIDAS
2015/758	Regolamento eCall
2015/2366	Direttiva PSD (Payment Services Directive) 2
2016/679	Regolamento GDPR
2016/1148	Direttiva NIS
2018/1972	Decisione EECC
2019/881	Regolamento CyberSecurity Act (ENISA)
2019/2144	Regolamento Automotive
L. 133/2019	Perimetro di sicurezza cibernetica nazionale
L. 109/2021	Agenzia per la Cybersicurezza Nazionale
2022/868	Regolamento Data Governance Act
2022/2554	Regolamento DORA
2022/2555	Direttiva NIS 2
2022/2557	Direttiva CER (Critical Entity Resilience)
2017/1584	Raccomandazione Incident response
2022/1925	Regolamento DMA (Digital Markets Act)
2022/2065	Regolamento DSA (Digital Services Act)
2023/1230	Regolamento Macchine
2023/2854	Regolamento Data Act
2024/1689	Regolamento AI (Artificial Intelligence Act)
2024/2690	Regolamento esecuzione NIS 2
2024/2847	Cyber Resilience Act
2025/38	Regolamento Cyber Solidarity Act

Digital Omnibus

NIS 2

Semplificazioni Italiane

Data	Norma	Descrizione
28/06/2024	Legge n. 90/2024	Legge Cyber Sicurezza
04/09/2024	D. Lgs. n. 138/2024	Recepimento Direttiva NIS 2 nell'ordinamento italiano
26/11/2024	Det. ACN n. 38565/2024	Piattaforma digitale NIS: termini e modalità di registrazione
09/12/2024	DPCM n. 221/2024	Criteri per l'applicazione della clausola di salvaguardia
10/04/2025	Det. ACN n. 136117/2025	Aggiornamento piattaforma NIS (sostituisce 38565/2024)
04/2025	Det. ACN n. 136118/2025	Notifica accordi volontari di condivisione informazioni
14/04/2025	Det. ACN n. 164179/2025	Misure di sicurezza di base e incidenti significativi (4 allegati)
09/2025	Linee Guida ACN	Supporto interpretativo agli allegati tecnici su misure e incidenti
22/07/2025	Det. ACN n. 283727/2025	Aggiornamento piattaforma NIS (sostituisce 136117/2025)
19/09/2025	Det. ACN n. 333017/2025	Sostituisce 283727/2025
24/12/2025	Det. ACN n. 379887/2025	Sostituisce 333017/2025
24/12/2025	Det. ACN n. 379907/2025	Sostituisce 164179/2025
31/12/2025	Linee Guida ACN	Gestione incidenti di sicurezza informatica

Framework

Regolamento (UE) 2016/679:
General Data Protection Regulation (**GDPR**) sulla Protezione dei dati personali.

Misure **tecniche** ed **organizzative** adeguate.

Direttiva (UE) 2016/1148:
Network Information Service (**NIS**) sulla sicurezza delle reti e dei sistemi informativi.

Misure tecniche ed organizzative adeguate e **proporzionate** alla gestione dei rischi.

Direttiva (UE) 2022/2555:
Network Information Service (**NIS 2**) sulla sicurezza delle reti e dei sistemi informativi.

Misure tecniche, **operative** e organizzative adeguate e proporzionate per gestire i rischi.

Direttiva (UE) 2022/2557:
Resilience of Critical Entities (**CER**) sulla strategia per la resilienza dei soggetti critici.

Misure tecniche, di sicurezza e organizzative adeguate e proporzionate per **garantire** la propria resilienza.

Regolamento (UE) 2023/123 (**Regolamento Macchine**):
sostituisce la Direttiva 2006/42/CE.

Adeguata protezione da una alterazione accidentale o intenzionale.

Checklist
di
conformità

Gestione
consapevole
del rischio


ALLARME
ANTINCENDIO
EVACUARE
IMMEDIATAMENTE
USCITA
EVACUARE
IMMEDIATAMENTE
ALLARME
ANTINCENDIO

Regolamento Macchine

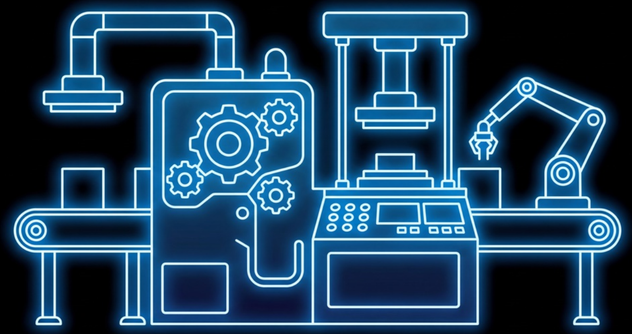
Filiera, processo, prodotto.

Fabbricanti, Importatori, Distributori e Mandatari.

Protezione dall’alterazione accidentale o intenzionale.

Garanzie. Prove. Tracciamento per cinque anni.

Aggiornamento.



Dal **20 gennaio 2027** sostituirà la Direttiva 2006/42/CE.

Interessa Fabbricanti, Importatori, Distributori e Mandatari.

Vi è una applicazione graduale:
13 luglio 2023: Art. 6, paragrafo 7, e Artt. 48 e 52.
14 ottobre 2023: Art. 50.
14 gennaio 2024: Artt. Da 26 a 42.
14 luglio 2024: Art. 6, paragrafi da 2 a 6, paragrafo 8 e paragrafo 11; Art. 47; Art. 53, paragrafo 3.
20 gennaio 2027: intero Regolamento.

2024

2025

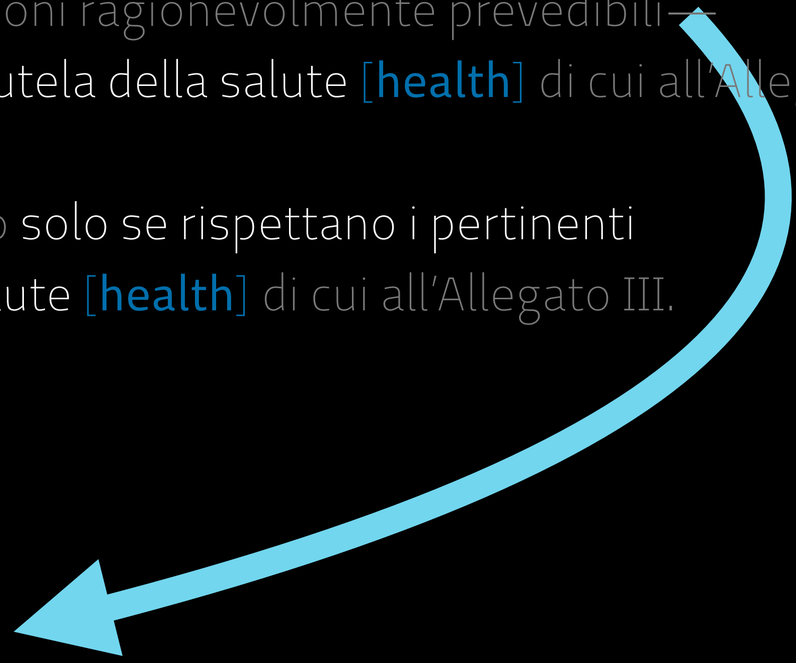
2026

2027

Articolo 8: **R**equisiti **E**ssenziali di **S**icurezza e di tutela della **S**alute

Le macchine o i prodotti correlati sono messi a disposizione sul mercato o messi in servizio soltanto se —quando debitamente installati, sottoposti a manutenzione e utilizzati conformemente al loro uso previsto o in condizioni ragionevolmente prevedibili— soddisfano i requisiti essenziali di sicurezza [safety] e di tutela della salute [health] di cui all'Allegato III.

Le quasi-macchine sono messe a disposizione sul mercato solo se rispettano i pertinenti requisiti essenziali di sicurezza [safety] e di tutela della salute [health] di cui all'Allegato III.



Ragionevolmente prevedibile

RESS

Autobus elettrici cinesi, allarme in Europa: “Si spengono da remoto”. Ecco come e i casi nel mirino

di Antonio Calitri

29 GENNAIO 2026 ALLE 17:30

2 MINUTI DI LETTURA

ROMA – Dopo Norvegia e Danimarca, l’allarme sul kill switch, la possibilità di spegnere da remoto gli autobus della Zhengzhou Yutong Group Co. si allarga al Regno Unito. Questo mese infatti il Dipartimento dei trasporti (DfT) e il National cyber security centre (Ncsc) hanno lanciato l’allarme sui circa 700 bus a marchio Yutong prodotti in Cina, in servizio sulle strade del Paese, per valutare se il governo debba imporre

ROMA – Dopo Norvegia e Danimarca, l'allarme sul kill switch, la possibilità di spegnere da remoto gli autobus della Zhengzhou Yutong Group Co. si allarga al Regno Unito. Questo mese infatti il Dipartimento dei trasporti (DfT) e il National cyber security centre (Ncsc) hanno lanciato l'allarme sui circa 700 bus a marchio Yutong prodotti in Cina, in servizio sulle strade del Paese, per valutare se il governo debba imporre restrizioni al produttore. Yutong è uno dei principali costrutto di mondiali di autobus ma ha incominciato la grande espansione fuori della Cina dopo aver aperto uno stabilimento dedicato all'elettrico nel 2012 e ora vanta una quota di mercato globale superiore al 10%. I suoi mezzi, dai 7 ai 18 metri tra autobus urbani, pullman a lunga percorrenza, autobus turistici, autobus pendolari, scuolabus e mobilità speciale coprono tutte le fasce di mercato e hanno prezzi convenienti. In Europa sono presenti in quasi tutti i mercati più importanti, dalla Spagna al Regno Unito, dalla Francia all'Italia e in particolare a Como, Palermo, Cremona e Bergamo.


OPEN CLOSE
SEEK
SEEK
RADIO MEDIA
PUSH ON
MP3 - WMA - JPEG
uconnect
A/C
20.5
22.5

TECNOLOGIA

Cybersecurity

Valasek e Miller hackerano una Jeep Cherokee

aggiornato il 22/07/2015 | 23 commenti

Chris Valasek e Charlie Miller colpiscono ancora. Questa volta, la "vittima" è una Jeep Cherokee del 2014, hackerata sfruttando una falla del sistema infotainment Uconnect. A differenza della Prius e dell'Escape, violate due anni fa con un laptop collegato alla porta della diagnostica, i due esperti di cybersecurity si sono introdotti nella Jeep a

Vulnerabilità nell'accessibilità remota. Come lo stesso Valasek ha spiegato a Quattroruote in un'intervista pubblicata sul numero di febbraio 2015 (**qui** le dieci cose da sapere sul tema), anche stavolta l'attacco è stato possibile sfruttando l'accessibilità remota della vettura: oltre alla connessione a Internet o alla rete cellulare, infatti, i canali potenzialmente utilizzabili dagli hacker includono wi-fi, Bluetooth, radio wireless, funzioni keyless, smartphone, app di bordo e i sistemi di monitoraggio della pressione delle gomme. Nel caso della Jeep, ai due esperti è bastato conoscere l'IP della vettura, per poi entrare grazie alla connessione Sprint usata dal veicolo: secondo quanto riferiscono, l'hacking è possibile su "tutti i veicoli Chrysler dotati di Uconnect venduti dalla fine del 2013, nel 2014 e all'inizio del 2015".

Articolo 10: Obblighi dei fabbricanti di **macchine** e di prodotti correlati

All'atto dell'immissione sul mercato o della messa in servizio di una macchina o di un prodotto correlato, i fabbricanti **garantiscono** che siano stati progettati e fabbricati conformemente ai requisiti essenziali di sicurezza e di tutela della salute di cui all'Allegato III.

Articolo 11: Obblighi dei fabbricanti di **quasi-macchine**

All'atto dell'immissione sul mercato di una quasi-macchina, i fabbricanti **garantiscono** che sia stata progettata e fabbricata conformemente ai pertinenti requisiti essenziali di sicurezza e di tutela della salute di cui all'Allegato III.

Progettati e fabbricati

Articolo 20: Presunzione di conformità dei prodotti rientranti nell'ambito di applicazione del presente regolamento

9. 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.

*

Regolamento (UE) 2019/881: ***Cyber Security Act***.
Regolamento (UE) 2024/482: applicazione ***Cyber Security Act***.
ENISA (Agenzia dell'Unione Europea per la Cybersecurity)
ACN (Agenzia per la Cybersicurezza Nazionale)
Certificazione della cibersicurezza dei prodotti, dei servizi e dei processi **TIC**.

Allegato III

Requisiti essenziali di sicurezza e di tutela della salute
relativi alla progettazione e alla costruzione di macchine o prodotti correlati

1.1. Considerazioni generali

1.1.9. Protezione dall’alterazione

1.2. Sistemi di controllo

1.2.1. Sicurezza ed affidabilità dei sistemi di comando

1.1.9 (nuovo): 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.

1.2.1 (ampliato): 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 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; [hazardous]

b) un'avaria nell'***hardware*** o nella logica del sistema di comando non crei situazioni pericolose; [hazardous]

c) errori della logica del sistema di comando non creino situazioni pericolose; [hazardous]

d) i limiti delle funzioni di sicurezza siano stabiliti come parte della valutazione del rischio effettuata dal fabbricante
e non siano consentite modifiche alle impostazioni o alle norme generate dalla macchina o dal prodotto correlato o dagli operatori,
neanche durante la fase di apprendimento della macchina o del prodotto correlato,
qualora tali modifiche possano determinare situazioni pericolose; [hazardous]

e) errori umani ragionevolmente prevedibili nelle manovre non creino situazioni pericolose;

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.

1.2.1 (ampliato): Sicurezza ed affidabilità dei sistemi di comando

I sistemi di controllo delle macchine o dei prodotti correlati
dotati di un comportamento o una logica integralmente o parzialmente **auto-evolutivi**
e che sono progettati per funzionare con livelli variabili di **autonomia**
devono essere progettati e costruiti in maniera tale da:

a) non essere la causa di azioni, da parte della macchina o del prodotto correlato,
che vanno **oltre** il suo compito e il suo spazio di movimento definiti;

b) consentire che siano registrati i dati relativi al **processo decisionale** in materia di sicurezza [safety]
per i sistemi di sicurezza basati su ***software*** che garantiscono la funzione di sicurezza, [safety]
compresi i componenti di sicurezza, [safety]
dopo che la macchina o il prodotto correlato sono stati immessi sul mercato o messi in servizio,
e che tali dati siano conservati per un anno dopo la loro raccolta,
esclusivamente per **dimostrare la conformità** della macchina o del prodotto correlato al presente allegato
a seguito di una richiesta motivata da parte di un'autorità nazionale competente;

c) consentire in qualsiasi momento la **correzione** della macchina o del prodotto correlato
al fine di preservarne la **sicurezza intrinseca**. [safety]

1.2.1 (ampliato): Sicurezza ed affidabilità dei sistemi di comando

Particolare attenzione deve essere prestata a quanto segue:

a) la macchina o il prodotto correlato non devono avviarsi in modo inatteso;

b) i parametri della macchina o del prodotto correlato non devono cambiare in modo incontrollato, laddove tale cambiamento possa portare a situazioni pericolose; [hazardous]

c) devono essere evitate le modifiche delle impostazioni o delle norme, generate dalla macchina o dal prodotto correlato o dagli operatori, anche durante la fase di apprendimento della macchina o del prodotto correlato, qualora tali modifiche possano determinare situazioni pericolose; [hazardous]

d) non deve essere impedito l'arresto della macchina o del prodotto correlato, se l'ordine di arresto è già stato dato;

e) nessun elemento mobile della macchina o del prodotto o pezzo correlato trattenuto dalla macchina o dal prodotto correlato deve cadere o essere espulso;

f) non deve essere impedito l'arresto manuale o automatico degli elementi mobili di qualsiasi tipo;

g) i dispositivi di protezione devono rimanere pienamente efficaci o dare un comando di arresto;

h) le parti del sistema di controllo legate alla sicurezza si devono applicare in modo coerente all'interezza di un insieme di macchine o di prodotti correlati o di semi-macchine o di una loro combinazione.

In caso di comando ***wireless***, un guasto della comunicazione o della connessione o una connessione difettosa non deve comportare una situazione pericolosa. [hazardous]

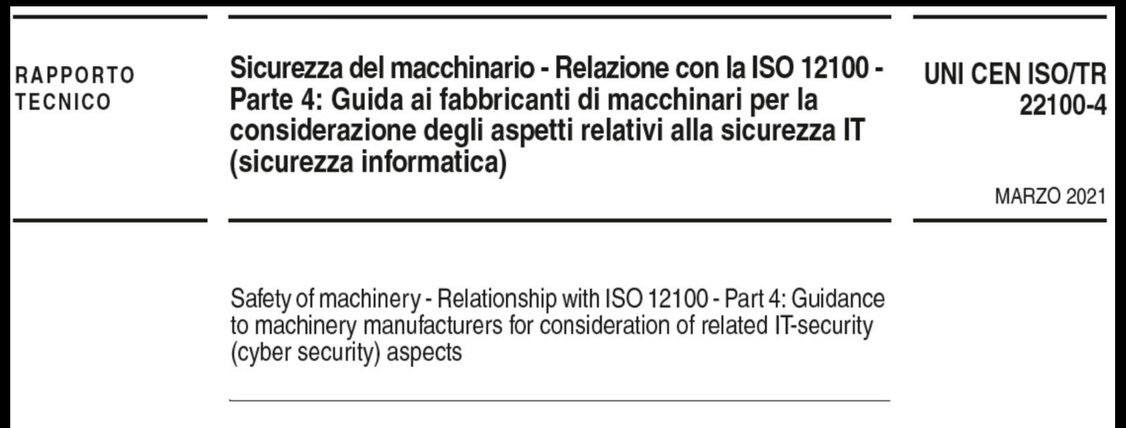
Safety

UNI CEN ISO/TR

22100-4:2021

UNI CEN ISO/TR 22100-4:2018 e 2021
Sicurezza del macchinario; Sicurezza informatica.

Questo *Technical Report* è il primo “ponte"
tra il mondo della sicurezza delle macchine (*safety*)
e quello della *industrial cyber security*.



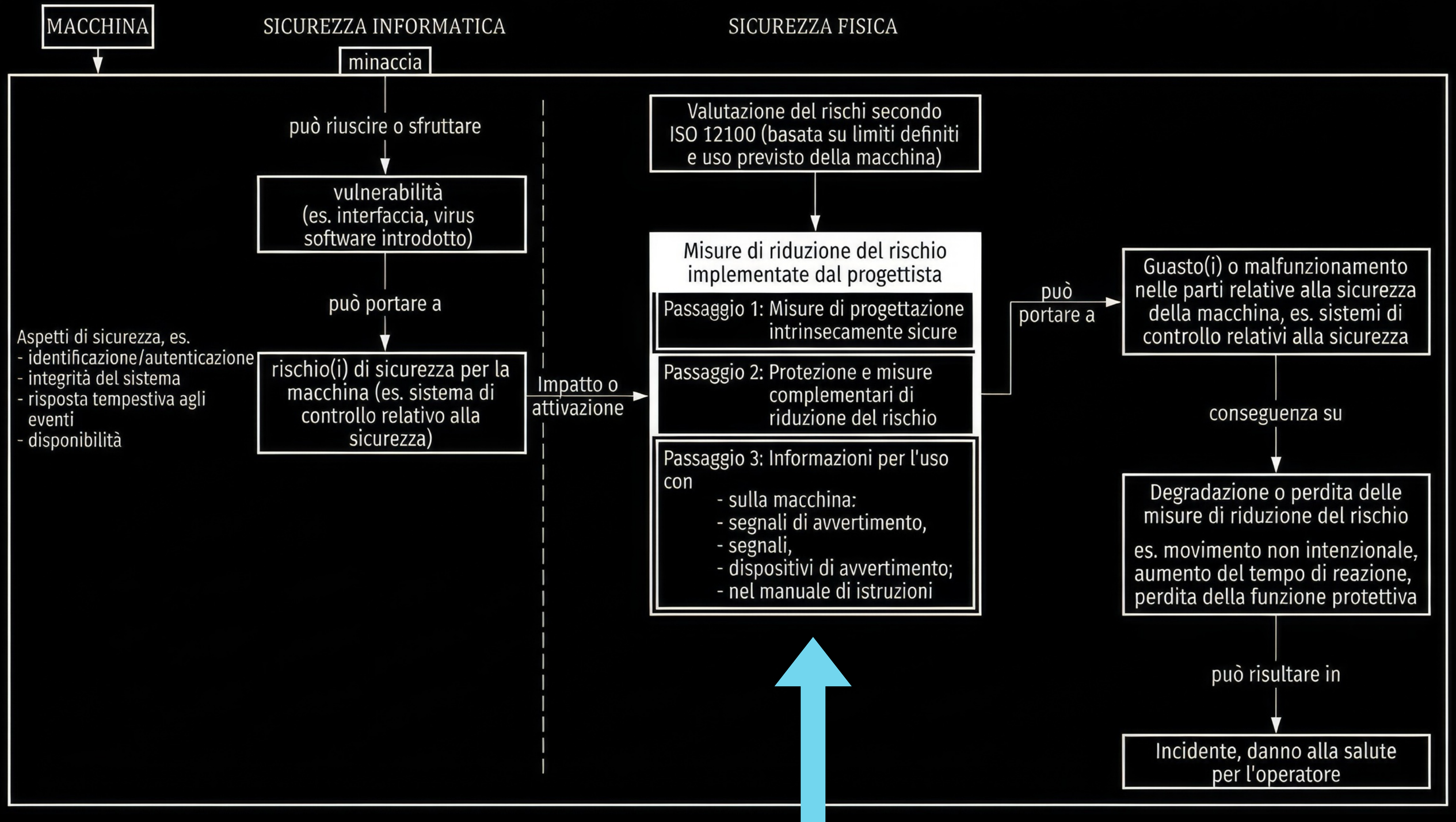
RAPPORTO TECNICO

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


MACCHINA
SICUREZZA INFORMATICA
SICUREZZA FISICA
minaccia
può riuscire o sfruttare
vulnerabilità
(es. interfaccia, virus
software introdotto)
può portare a
Aspetti di sicurezza, es.
- identificazione/autenticazione
- integrità del sistema
- risposta tempestiva agli
eventi
- disponibilità
rischio(i) di sicurezza per la
macchina (es. sistema di
controllo relativo alla
sicurezza)
Impatto o
attivazione
Valutazione del rischi secondo
ISO 12100 (basata su limiti definiti
e uso previsto della macchina)
Misure di riduzione del rischio
implementate dal progettista
Passaggio 1: Misure di progettazione
intrinsecamente sicure
Passaggio 2: Protezione e misure
complementari di
riduzione del rischio
Passaggio 3: Informazioni per l'uso
con
- sulla macchina:
- segnali di avvertimento,
- segnali,
- dispositivi di avvertimento;
- nel manuale di istruzioni
può
portare a
Guasto(i) o malfunzionamento
nelle parti relative alla sicurezza
della macchina, es. sistemi di
controllo relativi alla sicurezza
conseguenza su
Degradazione o perdita delle
misure di riduzione del rischio
es. movimento non intenzionale,
aumento del tempo di reazione,
perdita della funzione protettiva
può risultare in
Incidente, danno alla salute
per l'operatore

UNI CEN ISO/TR 22100-4:2018 e 2021
Sicurezza del macchinario; Sicurezza informatica.

Progettazione intrinsecamente sicura:
resilienza. SL-T, SL-C, SL-A

Protezioni e misure di protezione complementari:
contromisure.

Informazioni per l'uso sulla macchina:
raccomandazioni.

Tabella 3 — Esempi di misure di riduzione (mitigazione) del rischio per evitare/limitare le minacce alla sicurezza informatica che possono avere influenza sulla sicurezza dei macchinari

Area protettiva	Misura di riduzione (mitigazione) del rischio	Costruttore della macchina	Integratore	Utente finale
Restrizione dell'accesso logico/fisico al sistema IT (con possibile influenza sulla sicurezza)	Separazione fisica del sistema IT rilevante per la sicurezza dal sistema IT generale	x	x	x
	Fornitura di un sistema IT con misure di riduzione (mitigazione) del rischio (es. firewall, strumenti antivirus)	x	x	x
	Conservazione delle misure di riduzione (mitigazione) del rischio del sistema IT in una modalità sicura attuale (es. aggiornamento degli strumenti antivirus)			x
	Fornitura di mezzi che consentano un aggiornamento del software	x	x	
	Fornitura di meccanismi di autenticazione e controllo degli accessi separati (es. lettori di schede, serrature fisiche)	x	x	
	Fornitura di una topologia di rete	x	x	

UNI CEN ISO/TR 22100-4:2018 e 2021
Sinergie.

La sicurezza informatica industriale

di una macchina

è una responsabilità condivisa

(fabbricante, *system integrator*, cliente finale):

nessun soggetto della filiera può gestirla da solo

né delegarla interamente ad altri.

Safety

CEI CLC/IEC/TS

63074:2024

CEI CLC/IEC/TS 63074:2024
Sicurezza del macchinario; Sistemi di Controllo Safety

Questa Specifica Tecnica
rappresenta il collegamento più diretto e approfondito
tra *safety* funzionale delle macchine e *cyber security*.

Cita direttamente
gli *standard* ISA/IEC 62443.

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

Safety

prEN

50742:202*

prEN 50742:202*

Nuova norma!

Il documento tratta i requisiti

del Regolamento (UE) 2023/1230,

Allegato III, punto 1.1.9,

e i requisiti correlati di cui

all'Allegato III, punto 1.2.1, lettere a) ed f).

prEN 50742:202*

Eliminare le vulnerabilità.

Mitigare le vulnerabilità.

Informare: le informazioni per l'uso
devono fornire tutte le indicazioni necessarie
affinché l'utilizzatore possa adottare contromisure.

prEN 50742:202*

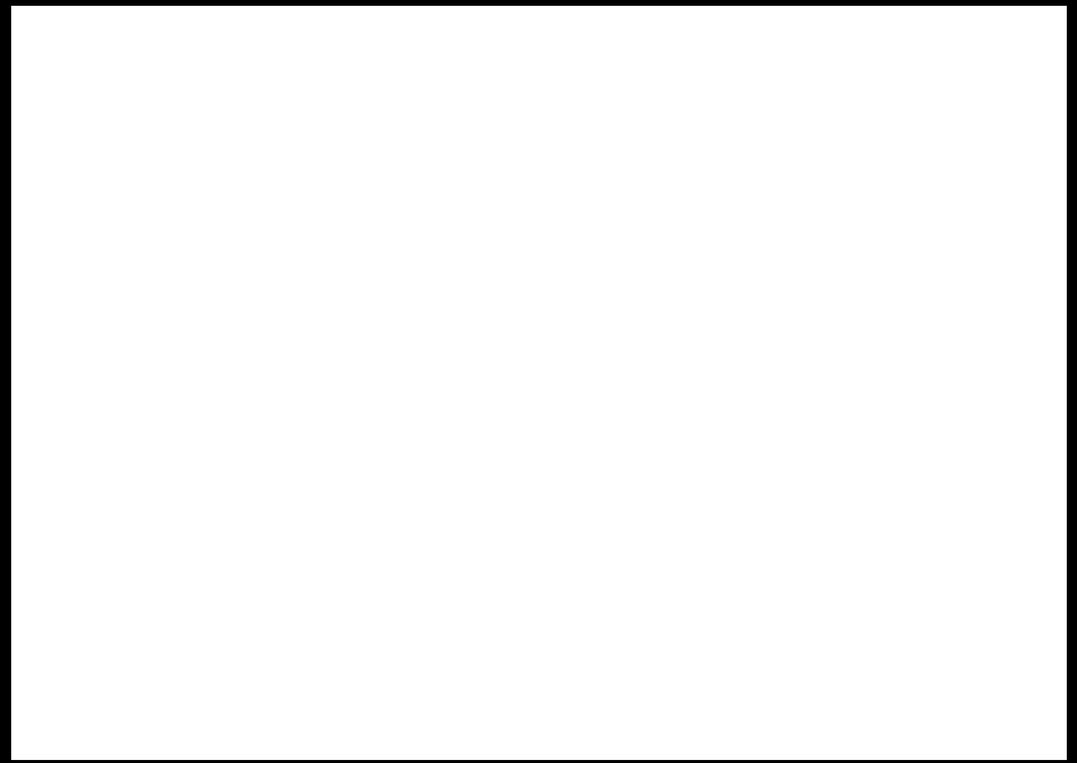
Prevede due approcci tra loro alternativi.

Il primo è interno alla norma.

Il secondo si riferisce direttamente agli *standard*:

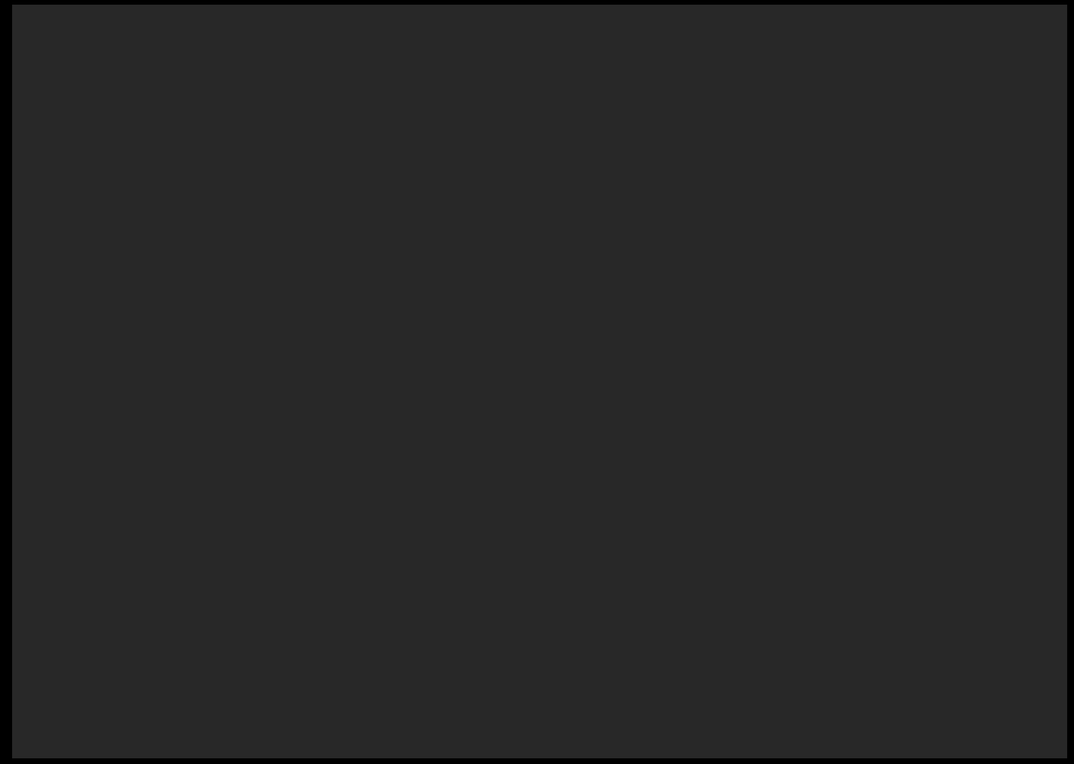
- ISA/IEC 62443-3-3 per i sistemi informatici delle macchine;
- ISA/IEC 62443-4-2 per le componenti utilizzati.

CRA



Art. 2:

Prodotti con elementi digitali
con una connessione dati
logica o fisica diretta o indiretta
a un dispositivo o a una rete.



Art. 3:

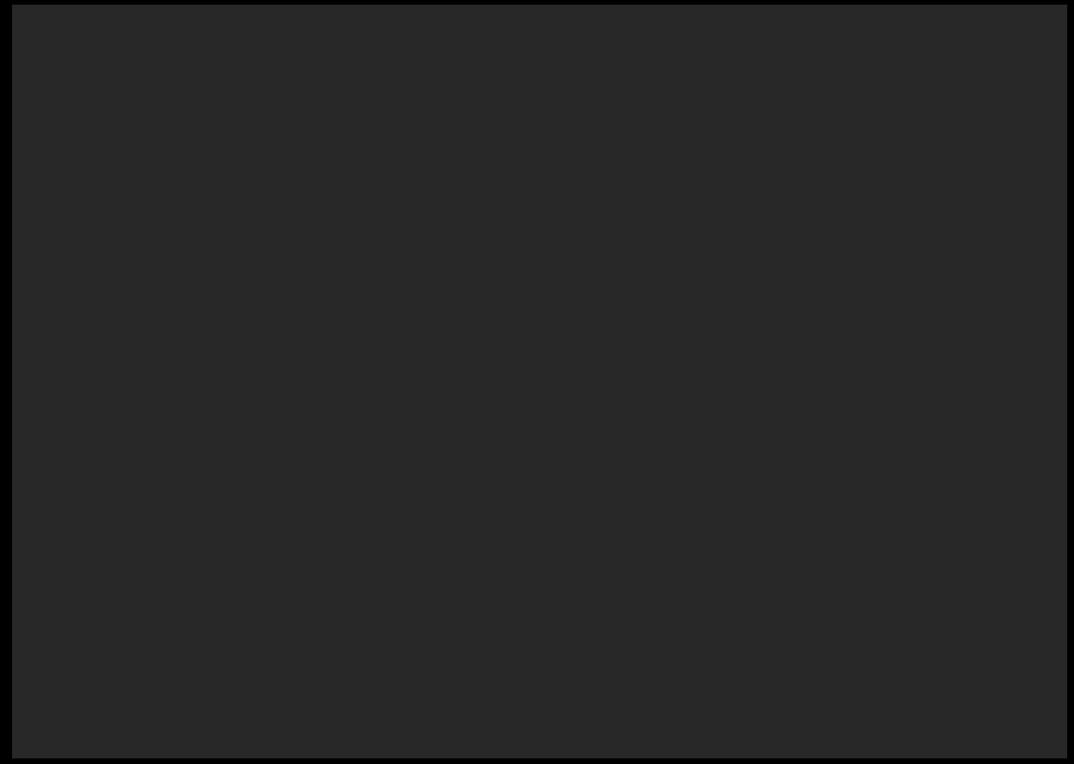
«prodotto con elementi digitali»:

qualsiasi prodotto

software o *hardware*

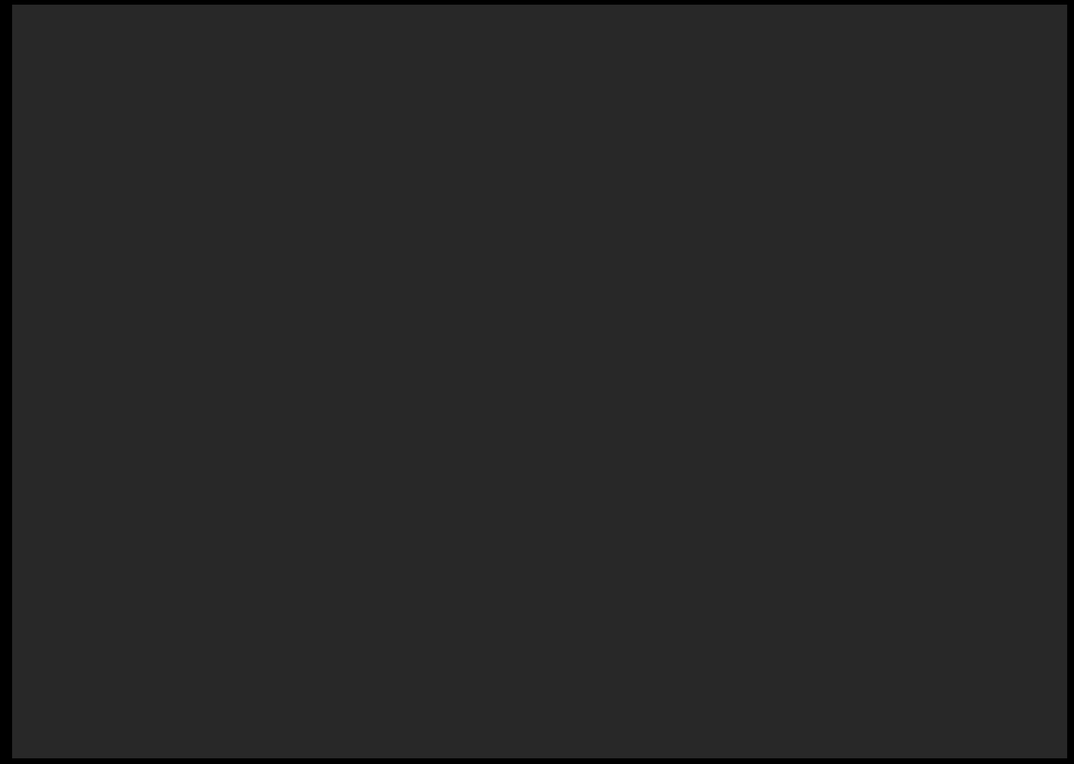
e le relative soluzioni

di elaborazione dati da remoto.



Art. 3:

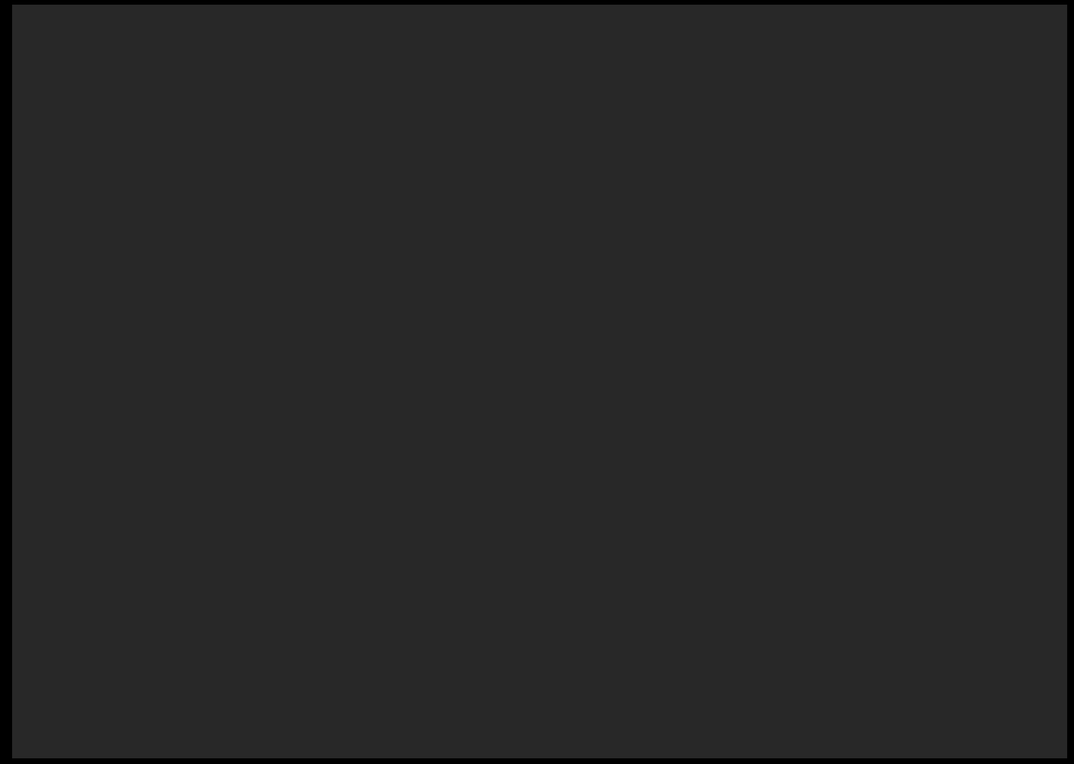
«uso ragionevolmente prevedibile»:
un uso che
non corrisponde necessariamente
alla finalità prevista dal fabbricante,
ma che è probabile possa derivare
da un comportamento umano
o da operazioni o interazioni tecniche
ragionevolmente prevedibili.



Art. 3:

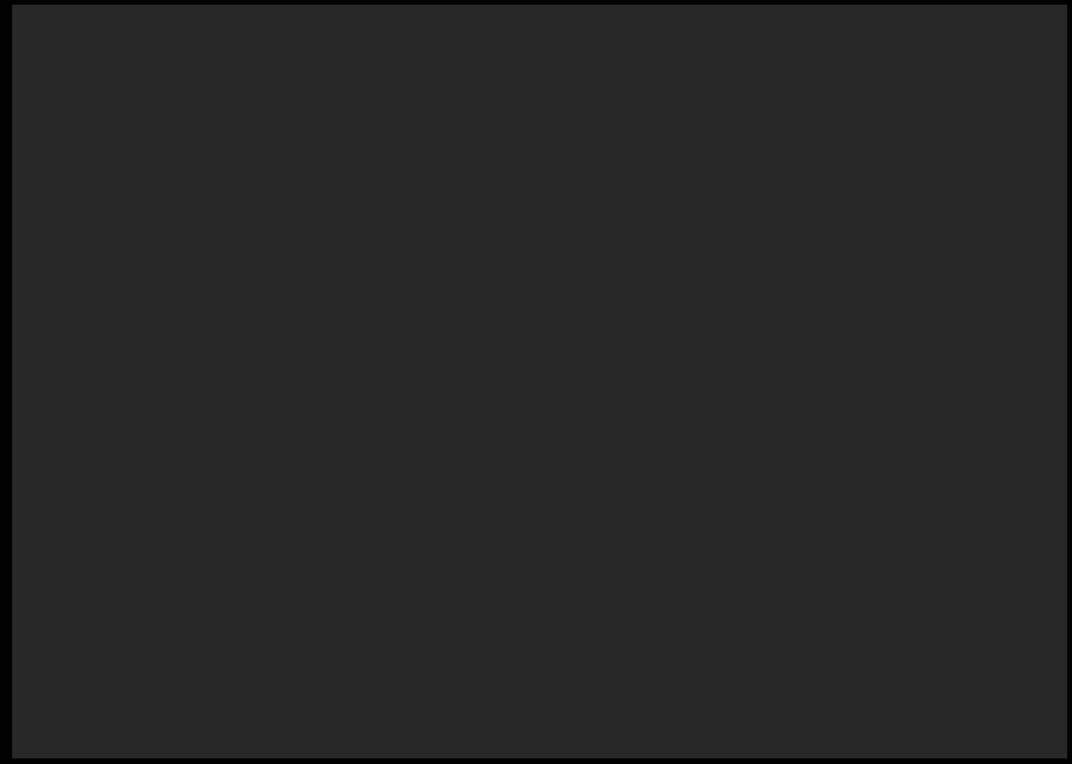
«uso improprio ragionevolmente prevedibile»:

l'uso di un prodotto
con elementi digitali
in un modo non conforme
alla sua finalità prevista,
ma che può derivare
da un comportamento umano
o da un'interazione con altri sistemi
ragionevolmente prevedibili.



Art. 3:

«marcatura CE»: una marcatura
mediante cui un fabbricante
indica che un prodotto
con elementi digitali
e i processi
messi in atto dal fabbricante
sono conformi
ai requisiti essenziali di cibersicurezza
di cui all'allegato I.



Standard

62443

62443

International Society of Automation
Setting the Standard for Automation™

General

1.1 Terminology, concepts, and models (Technical Specification)
1.2 Master glossary of terms and abbreviations (Technical Report)
1.3 System security conformance metrics
1.4 IACS security lifecycle and use-cases

Policies & Procedures

2.1 Establishing an **IACS security program** (International Standard)
2.2 IACS security program ratings
2.3 Patch management in the IACS environment (Technical Report)
2.4 Security program requirements for **IACS service providers** (International Standard)
2.5 Implementation guidance for IACS asset owners (Technical Report)

Systems

3.1 Security technologies for IACS (Technical Report)
3.2 **Security risk assessment** for system design (International Standard)
3.3 **System security requirements and security levels** (International Standard)

Component

4.1 Product security **development** lifecycle requirements (International Standard)
4.2 Technical security requirements for IACS **components** (International Standard)

2-1

Security program requirements for IACS asset owners

Requisiti per un sistema di gestione della sicurezza IACS (CSMS)

- Destinata all'asset owner: definisce il programma di sicurezza aziendale per gli IACS
- Politiche, organizzazione, ruoli e responsabilità per la cybersecurity OT
- Analisi e valutazione del rischio come fondamento del CSMS
- Selezione delle contromisure, formazione e consapevolezza del personale
- Miglioramento continuo: audit, riesame e mantenimento nel tempo

● Requisiti di processo (ruolo specifico)

CSMS · RISK

2-4

Security program requirements for IACS ***service providers***

Requisiti del programma di sicurezza per i *service provider*

- Destinata ai fornitori di servizi di integrazione e manutenzione
- Definisce le capability di sicurezza che il fornitore deve dimostrare
- Copre integrazione, messa in servizio e manutenzione dell'impianto
- Requisiti organizzati in profili applicabili al servizio erogato
- Base contrattuale: l'asset owner può esigere conformità verificabile

● Requisiti di processo (ruolo specifico)

3-2

*Security **risk assessment** for system design*

Valutazione del rischio e progettazione del sistema

- Definizione del System under Consideration (SuC): perimetro dell'analisi
- Valutazione iniziale del rischio (high level) sull'intero SuC
- Partizionamento in Zone e Conduit (ZCR) in base a criticità e funzioni
- Valutazione dettagliata del rischio per ogni zona e conduit
- Assegnazione dei Security Level Target (SL-T) e requisiti di progetto

● Processo di risk assessment e design

SuC · ZCR · PHA

3-3

System security requirements and security levels

Requisiti di sicurezza di sistema e *Security Level*

- 7 Requisiti Fondamentali (FR): IAC, UC, SI, DC, RDF, TRE, RA
- Requisiti di sistema (SR) derivati dai FR, con Requirement Enhancement
- 4 Security Level (SL1–SL4) in funzione della capacità dell'attaccante
- Mappa SR ↔ SL: quali requisiti servono per ogni livello di sicurezza
- Verifica di progetto: SL-C raggiunto dal sistema vs SL-T richiesto

4-1

Secure product development lifecycle requirements

Ciclo di vita di sviluppo sicuro del prodotto (SDL)

- Destinata ai product supplier: sicurezza integrata nello sviluppo
- 8 pratiche: SM, SR, SD, SI, SVV, DM, SUM, SG
- Security by design: requisiti, threat model e difesa in profondità
- Testing di verifica e validazione, gestione dei difetti di sicurezza
- Gestione di patch e aggiornamenti, linee guida di hardening per l'utente

● Requisiti di processo (ruolo specifico)

4-2

*Technical security requirements for IACS **components***

Requisiti tecnici di sicurezza per i componenti IACS

- Requisiti di componente (CR) derivati dagli SR della 3-3
- 4 tipologie: applicazioni software, dispositivi embedded, host, apparati di rete
- Capability Security Level (SL-C) dichiarato per ciascun componente
- Consente di selezionare componenti coerenti con l'SL-T della zona
- Base per la certificazione di prodotto (es. ISASecure, IECEE)

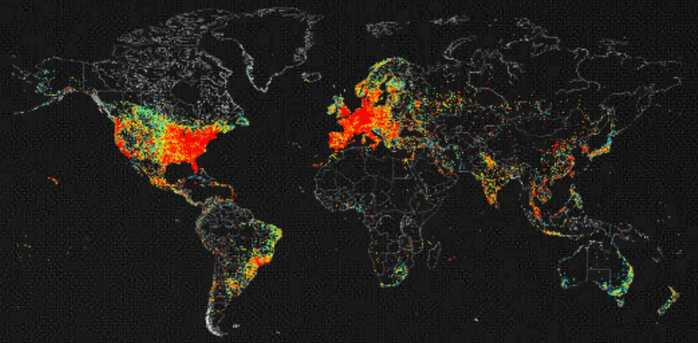
Shodan | Maps | Images | Monitor | Developer | More...

SHODAN | Explore | Pricing | Search | Login

Search Engine for the Internet of Everything

Shodan is the world's first search engine for Internet-connected devices. Discover how Internet intelligence can help you make better decisions.

SIGN UP NOW



// EXPLORE THE PLATFORM

Beyond the Web

Websites are just one part of the Internet. Use Shodan to discover everything from power plants, mobile phones, refrigerators and Minecraft servers.

Monitor Network Exposure

Keep track of all your devices that are directly accessible from the Internet. Shodan provides a comprehensive view of all exposed services to help you stay secure.

Internet Intelligence

Learn more about who is using various products and how they're changing over time. Shodan gives you a data-driven view of the technology that powers the Internet.

More than 3 million registered users across the world are using Shodan, including:

89% of the Fortune 100 | **5 of the Top 6 Cloud Providers** | **1,000+ Universities**