

Innovazione **T**ecnologica, **D**igitale, **A**I

**Quale impatto sulla Safety?**



Dipartimento Ingegneria Industriale



## Dalla Direttiva Macchine al Regolamento Macchine: quali impatti su tecnologie emergenti e AI

**Dott. Ing. Luciano Di Donato**

**Dirigente INAIL – Direttore del laboratorio IV Sicurezza degli  
impianti di trasformazione e produzione**

**Alma Mater Studiorum Università di Bologna 10 Aprile 2026**

Dipartimento innovazioni tecnologiche e sicurezza degli impianti prodotti e insediamenti antropici

## Presentazione del Laboratorio IV

Attività di ricerca del laboratorio IV INAIL



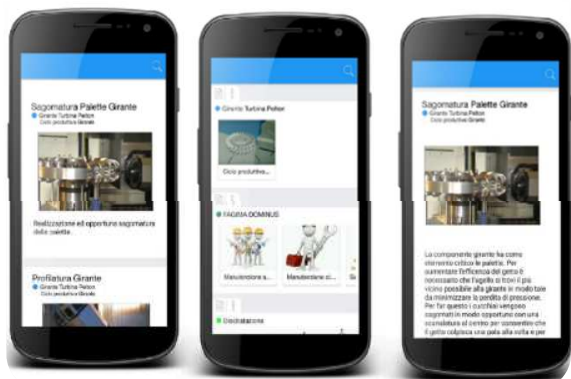
## Dalla direttiva al regolamento

- Motivi del cambiamento;
- Cyber security and cyber safety;
- Case study (robotica);
- La formazione.

## La Certificazione

- Ipotesi di certificazione (DC) di una macchina secondo il regolamento;
- La certificazione degli algoritmi.

# Laboratorio IV – Sicurezza degli impianti di Trasformazione e Produzione



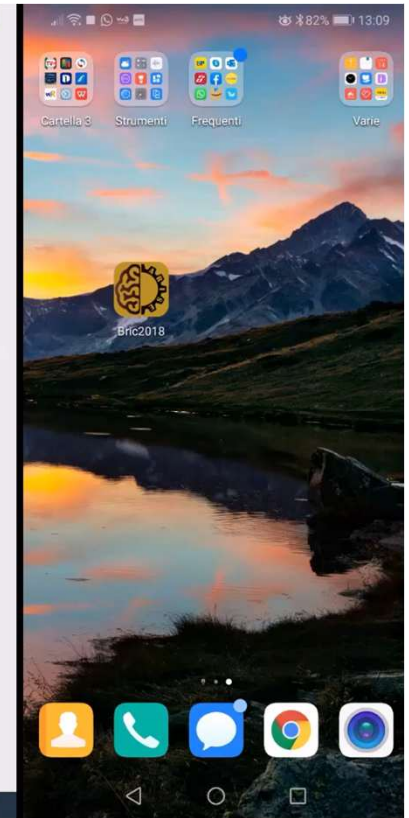
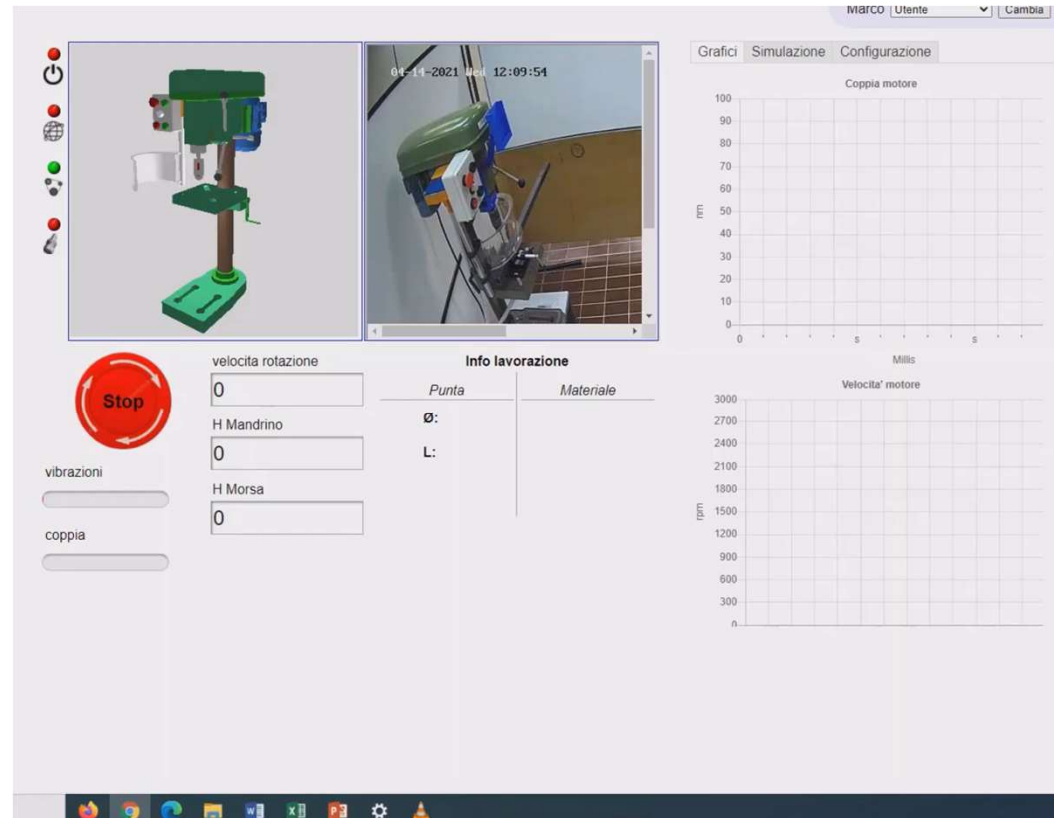
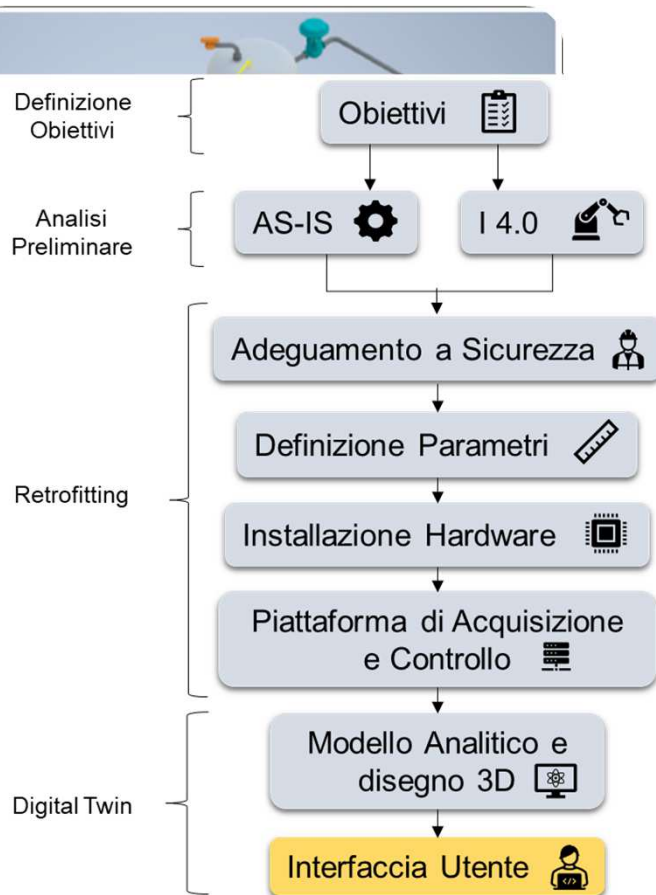
**Esoscheletro aptico**



INAIL

Dipartimento innovazioni tecnologiche e sicurezza degli impianti prodotti e insediamenti antropici

# Laboratorio IV – Sicurezza degli impianti di Trasformazione e Produzione





## Laboratorio IV – Sicurezza degli impianti di Trasformazione e Produzione



INAIL

Dipartimento innovazioni tecnologiche e sicurezza degli impianti prodotti e insediamenti antropici

## Laboratorio IV – Sicurezza degli impianti di Trasformazione e Produzione

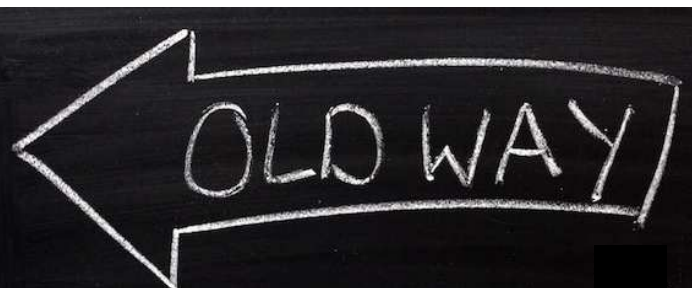


**START4.0**

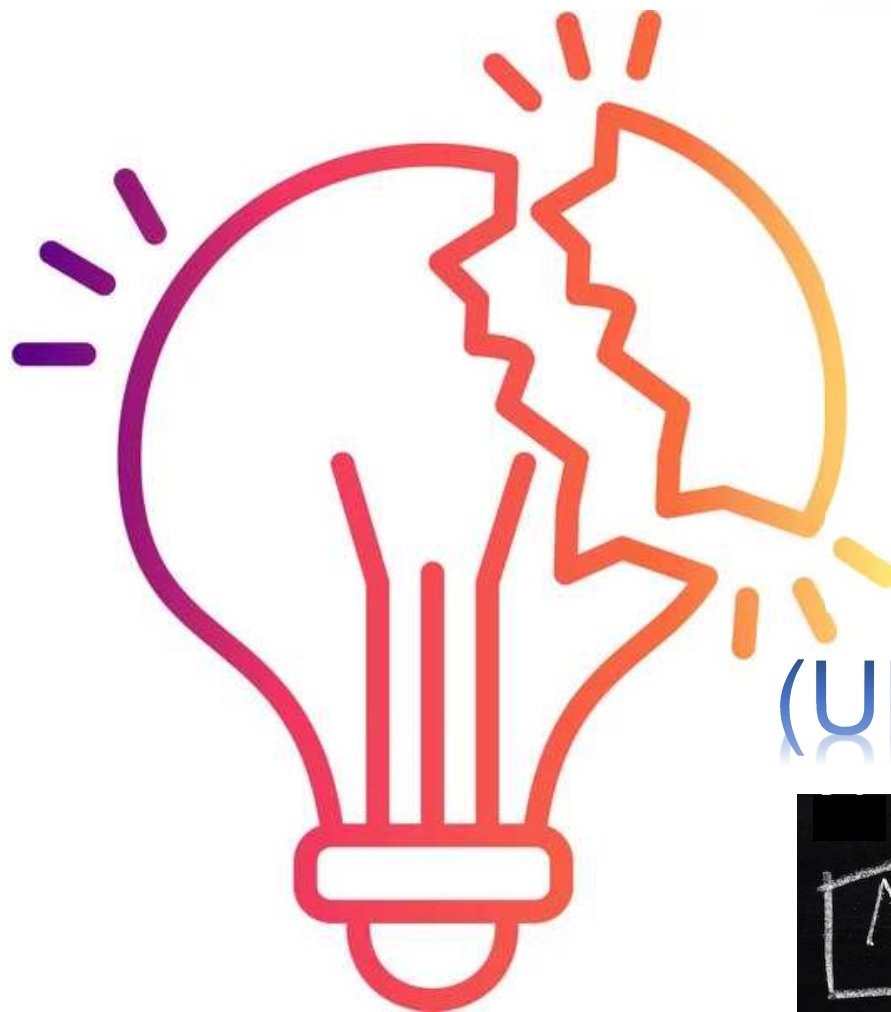
Applicazione di Virtual Reality e Geofencing per aumentare la sicurezza in cantiere



## Dalla Direttiva al Regolamento



2006/42/CE



(UE) 2023/1230





Regolamento (UE) 2023/1230



## Regolamento (UE) 2023/1230 relativo alle macchine

La direttiva macchine CE e 2006/42/CE sono atti legislativi dell'Unione europea che prevedono un recepimento da parte degli Stati membri



Anche il regolamento macchine UE 2023/1230 è un atto legislativo dell'Unione europea ma è direttamente applicabile in ciascuno degli Stati membri .

### Vantaggi

- Attuazione con una maggiore uniformità
- Nessuna difficoltà nel recepimento
- Maggior stato di diritto

La conversione della direttiva in regolamento permette di evitare:

- i ritardi nel recepimento
- differenze di interpretazione tra gli Stati membri.





## I principali motivi del cambiamento



## Regolamento (UE) 2023/1230 relativo alle macchine

Questo cambiamento normativo riflette l'evoluzione tecnologica del settore industriale, caratterizzato da:



Una crescente integrazione di sistemi digitali e componenti software nelle macchine.



Un diffuso impiego di intelligenza artificiale (AI) per funzioni di controllo, supervisione e sicurezza.



Un aumento dei rischi collegati alla cybersecurity e Cybersafety e all'alterazione dei sistemi di comando (volontaria o accidentale).

sicurezza degli impianti prodotti e insediamenti antropici



## Algoritmi



# Regolamento (UE) 2023/1230 relativo alle macchine

## Requisiti essenziali di sicurezza legati agli algoritmi:

### Protezione dalle alterazioni (RES 1.1.9)

Il software deve impedire interferenze che possano creare situazioni pericolose, inclusi:



Intrusioni digitali,



Manomissioni della logica di controllo,



Modifiche accidentali o intenzionali dovute ad aggiornamenti o apprendimento dell'AI.



## Algoritmi



# Regolamento (UE) 2023/1230 relativo alle macchine

## Requisiti essenziali di sicurezza legati agli algoritmi:

### **Sicurezza e affidabilità dei sistemi di comando (RES 1.2.1)**

Gli algoritmi devono garantire:



comportamento prevedibile,



tolleranza ai guasti, gestione sicura dell'errore,



fallback in caso di anomalie dell'AI.

Queste prescrizioni si sovrappongono a quanto previsto dall'AI Act in termini di accuratezza, robustezza e supervisione umana

sicurezza degli impianti prodotti e insediamenti antropici



## I principali motivi del cambiamento



## Regolamento (UE) 2023/1230 relativo alle macchine

Cybersecurity/Cybersafety come requisito di sicurezza Il regolamento introduce misure obbligatorie per:



Una protezione dei dati.



Una integrità del software.



Una gestione delle vulnerabilità e una continuità operativa in caso di attacchi informatici.

Le macchine connesse rientrano così nel perimetro del Cyber Resilience Act e del Reg. (UE) 2019/881.

sicurezza degli impianti prodotti e insediamenti antropici





# Regolamento (UE) 2023/1230 relativo alle macchine

## Alcune Definizioni Art. 3

### «macchina»

insieme di cui alle lettere da a) ad e) **al quale manca soltanto il caricamento del software destinato all'applicazione specifica prevista dal fabbricante;**

### «componente di sicurezza»:

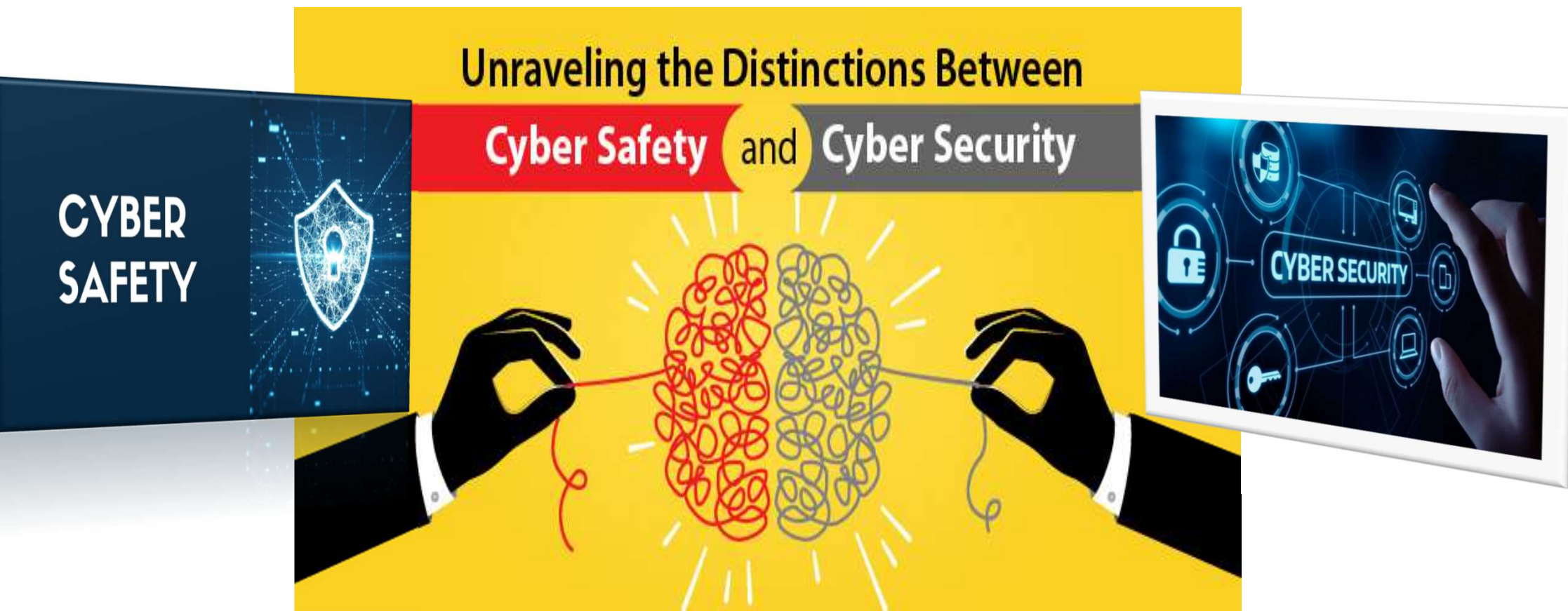
**un componente fisico o digitale, compreso un software**, di un prodotto rientrante nell'ambito di applicazione del presente regolamento, **che è progettato o destinato ad espletare una funzione di sicurezza** e che è immesso sul mercato separatamente, **il cui guasto o malfunzionamento mette a repentaglio la sicurezza delle persone**

Ambito di applicazione



sicurezza degli impianti prodotti e insediamenti antropici

# Cyber security and Cyber safety





## Aspetti di cyber security



# Regolamento (UE) 2023/1230 relativo alle macchine

## Cenni sulla Cyber Security

### Considerando 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 **ciber-sicurezza**.

sicurezza degli impianti prodotti e insediamenti antropici



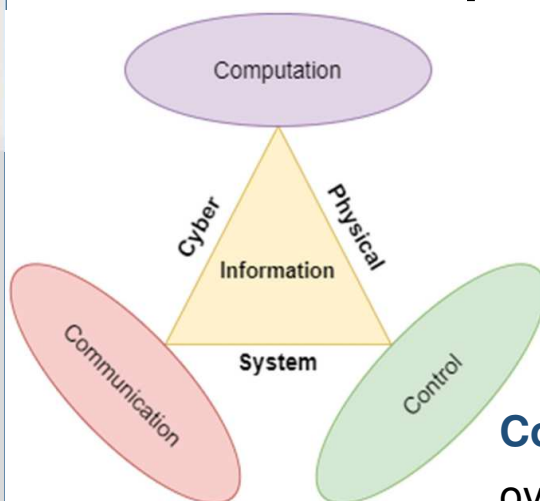
## Aspetti di cyber security



# Regolamento (UE) 2023/1230 relativo alle macchine

## Cenni sulla Cyber Security

### Una macchina può essere un sistema cyber-fisico



#### Physical

C'è un'interfaccia tra l'uomo e la macchina

#### Smart

poiché fa uso di tecnologie informatiche (machine learning, neural networks).

#### Connesso

ovvero non è un sistema "isolato" come lo era in passato. È connessa con il gestionale, oppure è accessibile dal remoto.



**Interagisce** continuamente con l'ambiente circostante. Dispone di sensori per "**sentire**" l'ambiente esterno e di attuatori per "**agire**" sull'ambiente esterno e perciò può svolgere compiti di controllo.

sicurezza degli impianti prodotti e insediamenti antropici





## Aspetti di cyber security

# Regolamento (UE) 2023/1230 relativo alle macchine

## Cenni sulla Cyber Security

### Una macchina può essere un sistema cyber-fisico

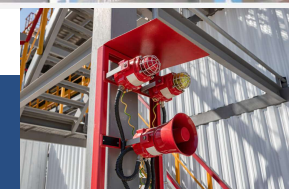
In un sistema IT, il requisito più importante è quello della confidenzialità: si vogliono evitare i data leakage (la perdita di dati).

Nel caso delle macchine e dei sistemi cyber-fisici in genere, il requisito di integrità è quello più importante perché una violazione dell'integrità di un sistema informatico può avere un impatto negativo sulla safety:

- qualcosa si può danneggiare o non funzionare ;
- **può esserci una ricaduta legata ad un infortunio .**



REQUISITI	DEFINIZIONE	MINACCIA
Confidenzialità	Garanzia contro l'accesso non autorizzato alle informazioni riservate	Furto di informazioni
Integrità	Assicurarsi che le informazioni siano affidabili e precise	Modifica delle informazioni (e funzionalità)
Disponibilità	Assicurazione che le informazioni e i servizi siano disponibili quando necessario	Impossibile accedere al servizio



**Cyber Safety**



## Aspetti di cyber security



Regolamento (UE) 2023/1230 relativo alle macchine

## Allegato III RESS art. 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**



sicurezza degli impianti prodotti e insediamenti antropici



## Aspetti di cyber security



# Regolamento (UE) 2023/1230 relativo alle macchine

## Allegato III RESS art. 1.1.9.



### Protezione dall'alterazione

#### 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.**

sicurezza degli impianti prodotti e insediamenti antropici



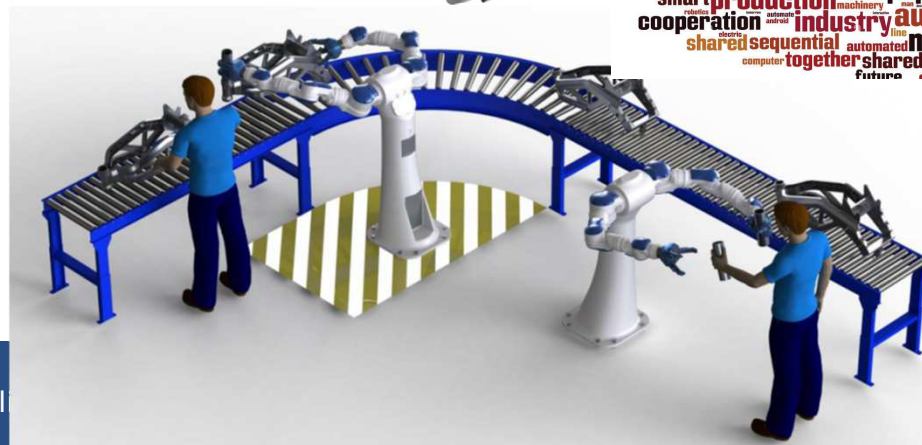
# Case Study



robot  
robotics  
work system  
project  
years  
engineering  
arduino  
video  
time  
control  
human  
software  
problem  
mean  
problem  
control  
cost  
people  
program  
motors  
nice  
idea  
drones  
controller  
cost  
design  
hand  
speed  
little  
make  
course  
makes  
ai  
experience  
move  
awesome  
real  
definitely  
help  
bit  
mechanical  
currently  
camera  
eye  
humanoid  
table  
start  
years  
start  
build  
computer  
looking  
source  
competition  
stuff  
world  
guys  
team  
thought  
based  
draw  
base  
arm  
hard  
cool  
issue  
design  
hardware  
pretty  
machine  
look  
sensors  
probably  
working  
servos  
question  
motors  
nice  
idea  
drones  
controller  
cost  
design  
hand  
speed  
little  
make  
course  
makes  
ai  
experience  
move  
awesome  
real  
definitely  
help  
bit  
mechanical  
currently  
camera  
eye  
humanoid  
table  
start  
years  
start  
build  
computer  
looking  
source  
competition  
stuff  
world  
guys  
team  
thought

CASE STUDIES

robot  
collaborative  
robot  
technology  
interaction  
collaboration  
robotic  
production  
equipment  
hand  
industrial  
digital  
cooperation  
shared  
sequential  
computer  
together  
shared  
space  
future  
engineering  
artificial  
real-time  
cobot  
system  
automation  
manufacturing  
space  
tool  
flexibility  
productivity  
manufacture  
safe  
behavior  
factory  
responsive  
human-robot  
automatic  
coexistence  
service  
robot  
electronic  
behavior  
safe  
artificial







## Standard applicabili



# UNI EN ISO 10218-2:2025

Robot e attrezzature per robot - Requisiti di sicurezza per robot industriali - Parte 2: Sistemi ed integrazione di robot

## 5.2.16 Cybersecurity

**Deve essere condotta una valutazione delle minacce alla sicurezza informatica.**



devono essere **previste misure di sicurezza informatica** per impedire l'accesso non autorizzato al/ai sistema/i di controllo, **al suo hardware, software, ai dati di configurazione e al/ai programma/i applicativo/i.**



- **protezione autenticata della configurazione di sicurezza;**
- **possibilità di modificare le configurazioni predefinite (ad esempio nomi utente, password utente, indirizzi IP e autenticazione di sicurezza).**

sicurezza degli impianti prodotti e insediamenti antropici



## Standard applicabili



# UNI EN ISO 10218-2:2025

Robot e attrezzature per robot - Requisiti di sicurezza per robot industriali - Parte 2: Sistemi ed integrazione di robot

## 7.5.23 Sicurezza informatica

**Devono essere fornite informazioni su tutte le funzionalità e metodologie di sicurezza informatica implementate per consentire all'utente di introdurre misure quali firewall, creazione di un piano di ripristino e implementazione di un approccio basato sul ciclo di vita continuo.**



- **revisione della valutazione del rischio per la sicurezza alla luce di nuove minacce e vulnerabilità e,**
- **implementazione delle patch software richieste**

sicurezza degli impianti prodotti e insediamenti antropici



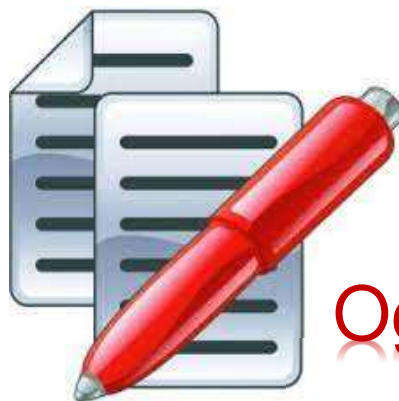
## PDR UNI Cyber Safety



## Prassi di Riferimento Cyber Safety

### Linee di indirizzo per la protezione dall'alterazione dei sistemi informatici delle macchine

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.



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.

**Oggi In inchiesta pubblica**

In tale contesto, le minacce informatiche che interessano nell'ambito della presente trattazione sono quelle che possono generare rischi di lesioni o danno alle persone.

sicurezza degli impianti prodotti e insediamenti antropici



## Prassi di Riferimento Cyber Safety

**Linee di indirizzo per la protezione dall'alterazione dei sistemi informatici delle macchine**



### **SOGGETTI COINVOLTI**

**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.

**PDR UNI Cybe**



IACS	sistemi di controllo industriale, compresi sistemi di controllo distribuito (DCS), controllori logici programmabili (PLC), unità terminali remote (RTU)
IACS	sistemi informativi associati quali: controllo avanzato o multivariabile, ottimizzatori online (ad esempio CAM/CAE), monitor di apparecchiature specifiche, interfacce grafiche.
IACS	interfacce interne, umane, di rete o interfacce di macchina associate utilizzate per fornire controllo, sicurezza e funzionalità operativa di produzione per processi continui

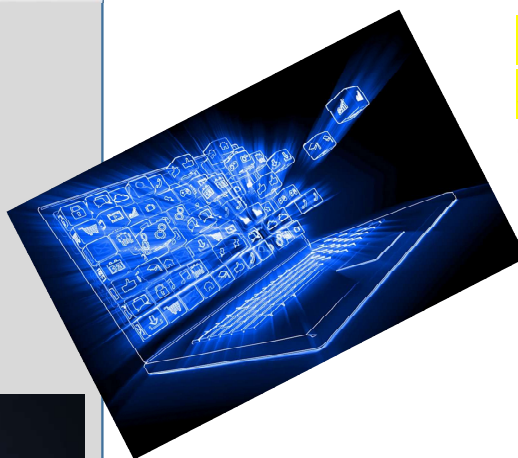
con una o più risorse delle IACS rilevanti per la sicurezza dei prodotti.

sicurezza degli impianti prodotti e insediamenti antropici





## Aspetti di cyber security



# Regolamento (UE) 2023/1230 relativo alle macchine

## Allegato III RESS art. 1.1.9.

### Protezione dall'alterazione

**Software e dati critici** per il rispetto da parte della macchina o del prodotto correlato **dei pertinenti requisiti essenziali di sicurezza e di tutela della salute** devono essere individuati come tali e **devono essere adeguatamente protetti da un'alterazione accidentale o intenzionale.**

La macchina o il prodotto correlato **devono 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.**



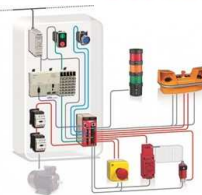
# Prassi di Riferimento Cyber Safety

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



Vulnerabilità

Sicurezza informatica

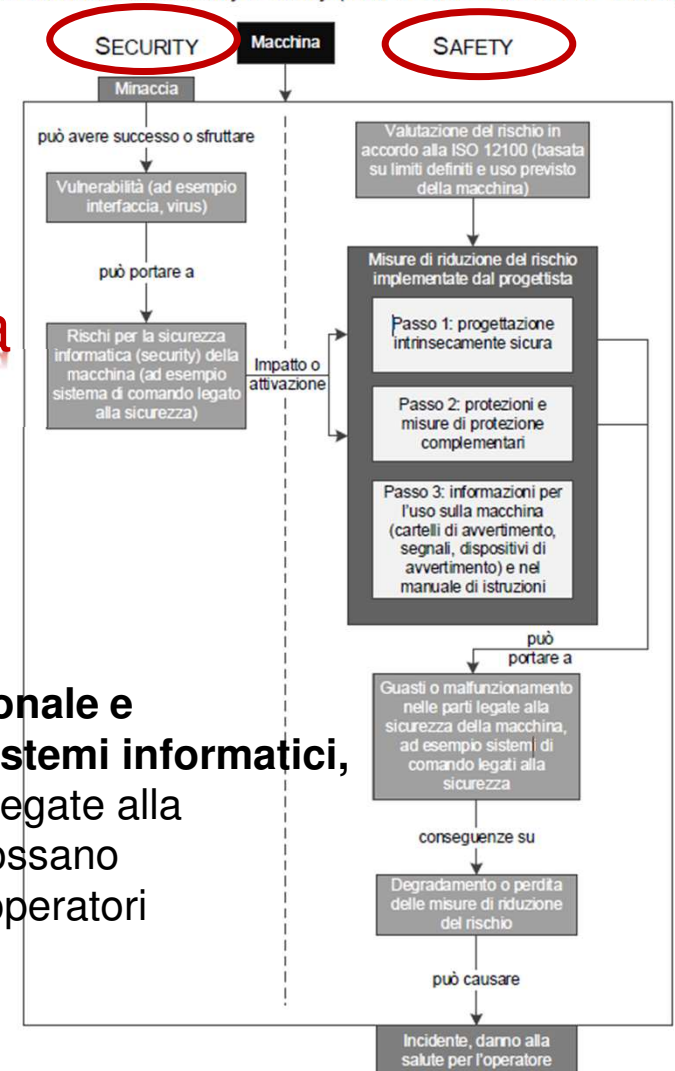


Sistema di comando legato alla sicurezza

PDR UNI Cyber Safety



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



sicurezza degli impianti prodotti e insediam

## La Formazione



**La sicurezza non è teoria: è tornare a casa.**



# Machinery Safety Specialist

## COMPITI E ATTIVITÀ SPECIFICHE DELLA FIGURA PROFESSIONALE

### PRASSI DI RIFERIMENTO

UNI/PdR 151:2023

**Profilo professionale dello specialista in sicurezza delle macchine**  
**Requisiti di conoscenza, abilità, autonomia e responsabilità**

*Machinery safety specialist professional knowledge, skills, and requirements*

La prassi di riferimento definisce i requisiti professionali dello specialista in sicurezza delle macchine, ossia la conoscenza dei requisiti di sicurezza previsti dalla legislazione europea e da altra legislazione europea di prodotto eventualmente applicabile, e dalle disposizioni di legge pertinenti, nelle attività di progettazione, sviluppo, produzione, manutenzione e documentazione di prodotti.

# NEWS

il mantenimento, l'aggiornamento e l'evoluzione delle competenze necessarie all'attività professionale dello specialista in sicurezza delle macchine non sono subordinati a uno specifico percorso formativo.

Il professionista è comunque tenuto a seguire percorsi autonomi o guidati di aggiornamento professionale continuo.

tti e insediamenti antropici





# Machinery Safety Specialist

## VALUTAZIONE DEI RISCHI

### PRASSI DI RIFERIMENTO

UNI/PdR 151:2023

#### Profilo professionale dello specialista in sicurezza delle macchine - Requisiti di conoscenza, abilità, autonomia e responsabilità

*Machinery safety specialist professional profile - Knowledge, skills, autonomy and responsibility requirements*

La prassi di riferimento definisce i requisiti relativi all'attività professionale dello specialista in sicurezza delle macchine, ossia di un esperto nell'applicazione dei requisiti di sicurezza previsti dalla legislazione europea relativa alle macchine nonché da altra legislazione europea di prodotto eventualmente applicabile ai prodotti, dalle norme e dalle disposizioni di legge pertinenti, nelle attività di progettazione, fabbricazione, valutazione di conformità e documentazione di prodotti.

# NEWS

per ciascuna fase di vita del prodotto,  
individuazione:

- delle persone coinvolte;
- dei limiti del prodotto;
- **dell'uso scorretto ragionevolmente prevedibile;**
- dei pericoli presenti e dell'estensione della zona pericolosa ad essi correlata;
- delle situazioni per cui le persone sono esposte ai pericoli identificati;
- del rischio correlato ad ogni pericolo identificato, in termini di gravità del danno e probabilità di accadimento;

tti e insediamenti antropici

# Requisiti essenziali di sicurezza e tutela della salute

## ALLEGATO III parte A

### i) Definizioni

INAIL

#### INTERAZIONE UOMO-MACCHINA

L'USO SCORRETTO PUÒ ESSERE RAGIONEVOLMENTE PREVEDIBILE

**PREMESSA** - La valutazione del rischio dell'interazione uomo-macchina, specie in presenza di macchine autonome e semiautonome, è resa complessa dalla variabilità delle possibilità di interazione.

è aggirare la difficoltà di un problema da un altro punto di vista cognitivo.

ontare il problema i costrutti strutturali antecedenti o successivi.

Intervento significa produrre la probabilità di strain e il task e, conseguentemente, prevedere lo scorretto invece che stimare la possibilità e intervenire a valle per gestire il rischio. In tal senso, mettere a fuoco i costrutti cognitivi diversi dallo stato di comfort ovvero di massima performance è un'opportunità per aumentare il livello di sicurezza.

#### L'IMPIANTO NORMATIVO

Allo stato attuale, l'impianto legislativo e normativo è finalizzato a tutelare la sicurezza e la salute dei lavoratori, prescrivendo il rispetto di requisiti di progetto al fine di prevenire infortuni ai danni dei lavoratori che operano con macchine. La direttiva macchine 2006/42/CE, come anche il Regolamento UE 2023/1230, prescrive, in particolare, che il prodotto immesso sul mercato o comunque messo in servizio nel territorio europeo rispetti dei requisiti minimi attraverso una valutazione dei rischi che il fabbricante deve realizzare. Questa valutazione prevede la definizione a monte dei limiti d'uso della macchina, il che comprende l'uso previsto e l'uso scorretto ragionevolmente prevedibile. L'individuazione di quest'ultimo è chiaramente legata alla soggettività insita negli aggettivi "prevedibile" e "ragionevole". Il confine tra ciò che è ragionevole e ciò che non lo è, peraltro, è in continua evoluzione come anche il conseguente stato dell'arte. Ad ogni modo la progettazione della macchina da parte del fabbricante deve, quindi, tener in considerazione l'uso scorretto ragionevolmente prevedibile da parte dell'utilizzatore finale, adottando accorgimenti progettuali e, dove necessario, anche specifici mezzi tecnici per gestire i rischi connessi. La norma UNI EN ISO 12100 fornisce un elenco esemplificativo di comportamento involontario dell'operatore o uso scorretto ragionevolmente prevedibile della macchina (Fig. 1).

Il Rapporto Tecnico UNI ISO/TR 14121-2, guida pratica all'applicazione dei principi della sopra citata norma, suggerisce, per garantire che siano identificati tutti gli usi - inclusi quelli scorretti ragionevolmente prevedibili -

## Uso scorretto ragionevolmente prevedibile La trasformazione digitale e il cambiamento nell'interazione uomo-macchina

Figura 2

Costrutti cognitivi comportamentali di cui alla norma UNI EN ISO 12100-1 Punto 5.5.1 lettera c

#### Mind Wandering

- Perdita di controllo della macchina da parte dell'operatore
- Comportamento derivante da mancanza di concentrazione o non curanza
- Reazione istintiva di una persona in caso di malfunzionamento, incidente o guasto durante l'uso della macchina

#### Effort Withdrawal

- Scelta comportamentale derivante dall'adozione della «linea di minor resistenza» nell'esecuzione di un compito
- Comportamento derivante da mancanza di concentrazione o non curanza

#### Perseveranza

- Reazione istintiva di una persona in caso di malfunzionamento, incidente o guasto durante l'uso della macchina
- Comportamento risultante da pressioni per tenere la macchina in esercizio in tutte le circostanze

#### Cecità e Sordità inattentiva

- Perdita di controllo della macchina da parte dell'operatore
- Comportamento derivante da mancanza di concentrazione o non curanza



# Machinery safety specialist

**Conoscenze, abilità, autonomia e responsabilità associate all'attività professionale**

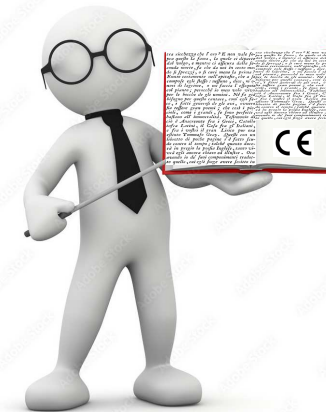


**Specialista livello base**

IL DEFEATING DI UN DISPOSITIVO DI INTERBLOCCO ASSOCIATO AI RIPARI

INAIL Norma EN ISO 14119:2013. Caso studio

2016



**Specialista livello avanzato**

tti e insediamenti antropici



Compito	Riga <sup>a)</sup>	Conoscenze	Abilità	Livello
Valutazione della conformità degli equipaggiamenti elettrico, pneumatico, oleoidraulico	4	Legislazione europea relativa alle macchine [9] UNI EN ISO 4413 UNI EN ISO 4414 CEI EN 60204-1	Valutare se i dispositivi elettrici, pneumatici e oleodinamici del prodotto sono conformi al progetto e sono compatibili in funzione dell'installazione sul prodotto.	Base e avanzato (punto 4.4.1)
	5		Definire gli interblocchi funzionali e le caratteristiche dei dispositivi elettrici, pneumatici e oleodinamici del prodotto necessari ad attuare la sua funzionalità.  Determinare se i dispositivi elettrici, pneumatici e oleodinamici del prodotto sono stati combinati e installati in modo da permettere la funzionalità in sicurezza prevista per il prodotto.	Avanzato (punto 4.4.2)
Valutazione delle funzioni di sicurezza	6	Legislazione europea relativa alle macchine [9] UNI EN ISO 12100	Identificare le funzioni necessarie a implementare la riduzione del rischio mediante funzioni di sicurezza.	Base e avanzato (punto 4.5.1)
	7	UNI EN ISO 13849-1 UNI EN ISO 13849-2 CEI EN IEC 62061	Definire il livello di prestazione delle funzioni di sicurezza necessario a ridurre adeguatamente il rischio.  Valutare la conformità delle funzioni di sicurezza realizzate al livello di prestazione richiesto.  Identificare se gli elementi del software necessari ad implementare le funzioni di sicurezza sono stati scelti e implementati correttamente sull'appropriata piattaforma hardware.  Determinare l'appropriata validazione delle funzioni di sicurezza realizzate.	Avanzato (punto 4.5.2)

## Certificazione di una macchina e certificazione degli algoritmi



# Certificazione

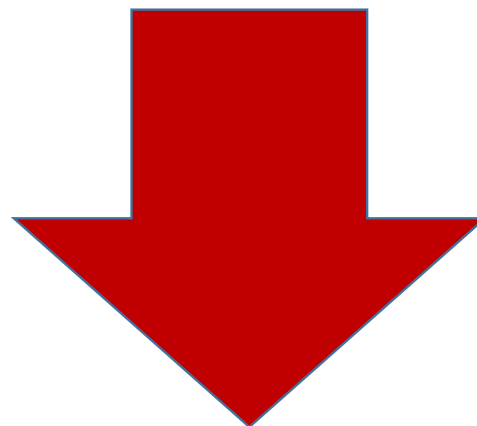




## Regolamento (UE) 2023/1230 relativo alle macchine

### Operatore economico

Il testo legale della 2006/42/CE non usa la parola importatore questo è uno dei motivi per cui la Direttiva non è allineata al NLF (New Legislative Framework)



L'importatore **non va nominato**. Infatti l'azione di muovere un prodotto dall'esterno di UE verso la UE



Importatore

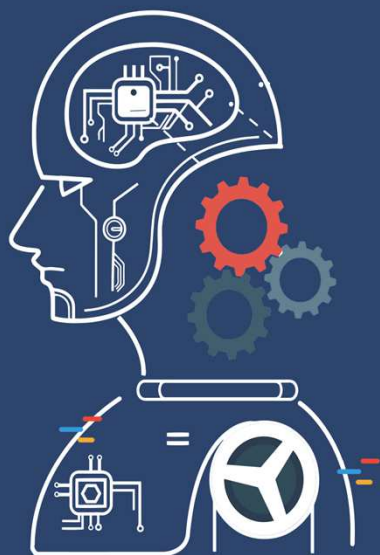
**Identifica  
l'importatore**

### L'operatore economico





## Criteri di confronto per la certificazione



## Regolamento (UE) 2023/1230 relativo alle macchine

### Certificazione degli algoritmi tra Regolamento Machine e AI ACT :

#### Sistema IA ad alto rischio



Lo scopo del presente regolamento (AI act) è migliorare il funzionamento del mercato interno e promuovere la diffusione di un'intelligenza artificiale (IA) antropocentrica e affidabile, garantendo nel contempo un livello elevato di protezione della salute, della sicurezza.... Omississ...

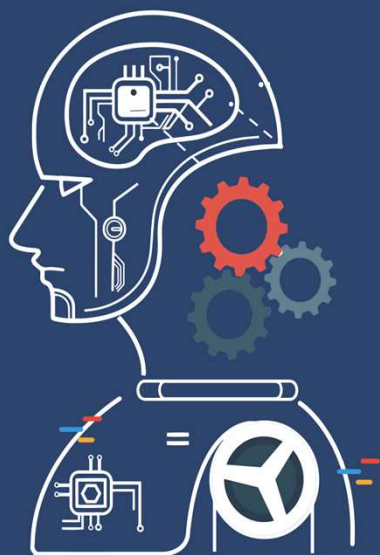


Un sistema di IA è considerato ad alto rischio se sono soddisfatte entrambe le condizioni seguenti:

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 (GU L 157 del 9.6.2006, pag. 24) [abrogata dal regolamento sui prodotti macchina];



## Criteri di confronto per la certificazione



## Conclusioni

**Il Regolamento Macchine (UE) 2023/1230** introduce, un approccio pienamente integrato tra sicurezza meccanica e sicurezza algoritmica, riconoscendo che nelle macchine moderne la componente software è determinante per il funzionamento sicuro.

### I principali effetti per i fabbricanti e datori di lavoro sono:

- ✓ **N**ecessità di certificare anche gli algoritmi, non solo la macchina;
- ✓ **O**bligo di coinvolgere organismi notificati per sistemi intelligenti ad alto rischio;
- ✓ **A**dozione di misure di cybersecurity equivalenti ai requisiti meccanici tradizionali;
- ✓ **R**endicontazione dettagliata della logica e del comportamento dell'AI;
- ✓ **G**estione rigorosa degli aggiornamenti software per evitare modifiche sostanziali non conformi.
- ✓ **A**ssicurarsi la presenza di personale con la qualifica di Machine Specialist (anche per il datore di Lavoro)

sicurezza degli impianti prodotti e insediamenti antropici

# Smart INAIL

Grazie per l'attenzione

[I.didonato@inail.it](mailto:I.didonato@inail.it)



