SEMINARIO TECNICO · 27 MAGGIO 2026

Sicurezza delle Macchine

Dalla robotica collaborativa agli umanoidi

AI e cybersecurity nel Regolamento (UE) 2023/1230

Ing. Fabrizio Catinari

Commissione Tematica Meccanica Industriale

Ordine degli Ingegneri della Provincia di Roma

INDICE

Di cosa parleremo

1. Robotica collaborativa: i RESS che la disciplinano
2. Robot umanoidi: stato dell'arte e inquadramento
3. AI nel Regolamento: All. I, All. II e RESS auto-evolutivi
4. Cybersecurity: RESS 1.1.9 e 1.2.1
5. Scenari di rischio applicativi
6. Appendici tecniche (ISO/TS 15066, prEN 50742)
7. Riepilogo e domande

Dove ci posizioniamo nel Regolamento 2023/1230

Quattro punti del Regolamento contengono tutto ciò che ci serve oggi:

Art. 3	**Definizioni** componente di sicurezza (p. 3), modifica sostanziale (p. 16), ciclo di vita (p. 34), codice sorgente (p. 35)
All. I parte A	**Categorie ad alto rischio (Art. 25 par. 2)** punti 5 e 6 — sistemi AI a comportamento autoevolutivo come componenti / integrati
All. II	**Elenco indicativo componenti di sicurezza** punto 18 — software che garantisce funzioni di sicurezza; punto 19 — componenti AI autoevolutivi
All. III	**Requisiti essenziali di sicurezza** 1.1.6 ergonomia · 1.1.9 protezione dall'alterazione · 1.2.1 sistemi di comando · 1.3.7 elementi mobili · 1.5.14 imprigionamento

SEZIONE 1

1 Robotica collaborativa: i RESS che la disciplinano

Cambio di paradigma rispetto al robot industriale

Robot industriale

EN ISO 10218-1/-2

- Sicurezza per allontanamento
- Recinzioni, scanner, interlock
- Velocità e coppie elevate
- Contatto da impedire

Cobot (Collaborative Robot) → Collaborative Application

ISO/TS 15066:2016 → EN ISO 10218:2025 (Pubblicata ma in attesa di citazione GUUE)

- Sicurezza per convivenza controllata
- Spazio di lavoro condiviso
- Sensoristica + limitazione forza/velocità
- *4 modalità: SRMS, HG, SSM, PFL*
- Tensioni psichiche (RESS 1.1.6 ergonomia/stress, 1.3.7 elementi mobili)

Le 4 modalità collaborative

01 **Safety-rated monitored stop (SRMS)**

Il robot è fermo quando l'operatore è presente nello spazio di lavoro condiviso; gli azionamenti rimangono in monitored stop

02 **Hand guiding (HG)**

L'operatore guida fisicamente il robot (ad esempio per l'insegnamento di un percorso) applicando una forza diretta sulle sue parti, trasformandola in un comando di movimento

03 **Speed and separation monitoring (SSM)**

Il robot riduce la propria velocità in proporzione alla distanza dell'operatore, garantendo che si fermi del tutto prima che possa avvenire qualsiasi contatto accidentale.

04 **Power and force limiting (PFL)**

Il robot è progettato e configurato (tramite limiti fisici e controllo della coppia) per tollerare e limitare l'energia di un eventuale contatto (volontario o involontario) con l'essere umano, prevenendo lesioni

Elementi mobili: il passo sui cobot

ALLEGATO III, PUNTO 1.3.7 — RISCHI DOVUTI A ELEMENTI MOBILI (ESTRATTO)

«La prevenzione di rischi derivanti da contatto che determinano situazioni di pericolo e le tensioni psichiche che possono essere causate dall'interazione con la macchina deve essere adeguata in relazione a: a) coesistenza uomo-macchina in uno spazio condiviso in assenza di collaborazione diretta; b) interazione uomo-macchina.»

LETTURA NORMATIVA

Per la prima volta il legislatore distingue due regimi: coesistenza in spazio condiviso (no contatto diretto) e collaborazione vera e propria. Entrambe vanno valutate per rischi fisici e psichici.

Implica: la valutazione del rischio del cobot deve includere parametri biomeccanici (ISO/TS 15066) E carico cognitivo / stress psichico.

Ergonomia: lettera f) — l'interfaccia uomo-macchina

ALLEGATO III, PUNTO 1.1.6 LETTERA (F) — ERGONOMIA

«adeguare l'interfaccia tra uomo e macchina alle caratteristiche prevedibili degli operatori, anche rispetto a una macchina o a un prodotto correlato dotati di un comportamento o una logica integralmente o parzialmente auto-evolutivi e che sono progettati per funzionare con livelli variabili di autonomia»

Cosa significa per cobot e umanoidi

- Il RESS 1.1.6 lett. f) include esplicitamente le macchine "auto-evolutive con livelli variabili di autonomia".
- L'HMI di un cobot/umanoide deve essere adeguata alle caratteristiche PREVEDIBILI degli operatori — quindi mediata da human factors.
- Non è solo questione di ergonomia fisica: è ergonomia cognitiva e di interazione.

Rischio di restare imprigionati nella macchina

ALLEGATO III, PUNTO 1.5.14 — RISCHIO DI RESTARE IMPRIGIONATI IN UNA MACCHINA

«Le macchine o i prodotti correlati devono essere progettati, costruiti o dotati di mezzi che consentano di evitare che una persona resti chiusa all'interno o, se ciò non fosse possibile, devono essere dotati di mezzi per chiedere aiuto.»

Rilevanza per applicazioni collaborative

- Applicabile a tutti i contesti dove l'operatore può rimanere intrappolato nella zona di lavoro della macchina.
- Particolarmente critico per celle robotizzate, AGV/AMR che operano in corridoi stretti, e applicazioni con umanoidi mobili in ambienti chiusi.
- Soluzioni tipiche: pulsanti di chiamata aiuto all'interno della cella, sensori di presenza, sblocco emergenza dei ripari, comunicazione bidirezionale.

1.6 · ALL. III RESS 1.2.1 (D)

Sicurezza ed affidabilità dei sistemi di comando: Limiti delle funzioni di sicurezza

ALLEGATO III, PUNTO 1.2.1 — LETTERA (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»

APPLICAZIONE PRATICA AI COBOT

- I limiti di forza/velocità (PFL) e di separazione (SSM) sono parte integrante della valutazione del rischio.
- Non modificabili da operatori in produzione, neanche durante l'apprendimento o la riprogrammazione.
- Architetturalmente: i parametri di sicurezza a livello *safety* non scrivibile da codice applicativo.

Modifica sostanziale: definizione completa

ART. 3 PUNTO 16 — DEFINIZIONE INTEGRALE

«una modifica di una macchina o di un prodotto correlato, mediante mezzi fisici o digitali dopo che tale macchina o prodotto correlato è stato immesso sul mercato o messo in servizio, che non è prevista né pianificata dal fabbricante, e che incide sulla sicurezza della macchina o del prodotto correlato creando un nuovo pericolo o aumentando un rischio esistente, che richiede: a) l'aggiunta di ripari o di dispositivi di protezione alla macchina o al prodotto correlato, operazione che necessita la modifica del sistema di controllo della sicurezza esistente, o b) l'adozione di misure di protezione supplementari per garantire la stabilità o la resistenza meccanica di tale macchina o prodotto correlato»

Attenzione alla soglia

Non basta che la modifica incida sulla sicurezza: deve anche richiedere (a) nuovi ripari/dispositivi con modifica del sistema di controllo, o (b) misure per stabilità/resistenza meccanica. Soglia restrittiva.

1.8 · PUNTO CRITICO

"Cobot-capable" ≠ applicazione collaborativa sicura

La modalità collaborativa è caratteristica del SISTEMA INTEGRATO, non del solo robot.

Robot + end-effector + pezzo + layout + task = applicazione da valutare nel suo insieme.

Implicazioni sotto il Regolamento (UE) 2023/1230

- Valutazione del rischio a livello di sistema (All. III parte B punto 1) — interazioni tra componenti incluse.
- Un cambio significativo di end-effector/task può configurare modifica sostanziale Art. 3 punto 16.
- Chi effettua la modifica sostanziale è considerato fabbricante (Art. 18) e applica Art. 25 par. 2-4.

SEZIONE 2

2 Robot umanoidi: stato dell'arte e inquadramento

Cos'è un robot umanoide industriale

Robot antropomorfo bipede, dotato di manipolazione bimanuale, mobilità autonoma in ambiente non strutturato, pilotato da modelli foundation di visione-linguaggio-azione (VLA) o policy neurali.

Tre caratteristiche tecniche che lo distinguono dal cobot:

Mobilità

Equilibrio dinamico bipede; locomozione in spazi aperti non strutturati.

Apprendimento

Modello probabilistico (policy neurale) che migliora con i dati di esercizio.

Interazione

Comprensione del linguaggio naturale; gesture, comandi vocali, anche soggetti non addestrati.

Perchè umanoide industriale?

La domanda legittima che si fa qualunque ingegnere impiantista quando vede un umanoide è: perché un bipede instabile e debole quando ho lo SCARA che gira da quarant'anni?

La sfida tra due filosofie produttive e infrastrutturali opposte

Automazione “Tradizionale”

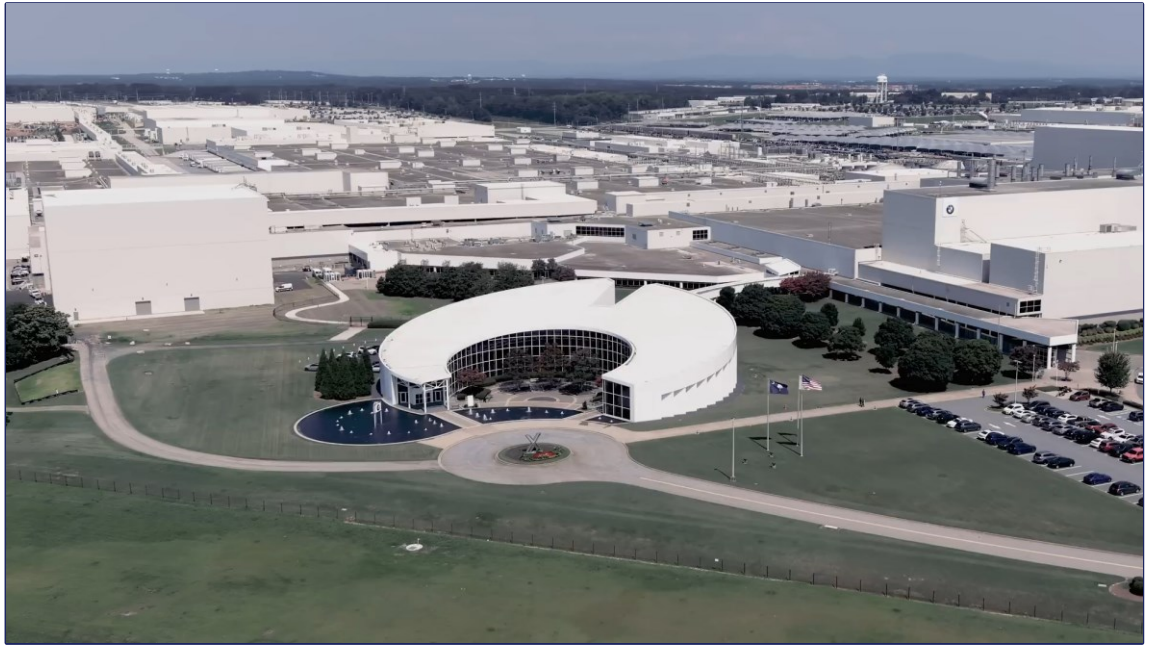
L'automazione tradizionale richiede ambienti Greenfield: progetti la linea attorno al robot, pavimenti perfetti, gabbie in acciaio, dime al millimetro. Capex enorme, layout congelato per dieci anni

Form Factor “Umano”

L'umanoide è progettato per il Brownfield: integrazione in stabilimenti esistenti pensati per esseri umani alti 170 cm. Usa le stesse scale, le stesse porte, gli stessi utensili. Non sostituisce lo SCARA, lo affianca dove non può andare e azzera il CapEx infrastrutturale di carpenteria, recinzione e sicurezza fisica.

È una filosofia diversa, non un competitor diretto

Figure 02 — Figure AI



CARATTERISTICHE

Produttore
Figure AI (USA)

Altezza
~ 1,68 m

Peso
~ 70 kg

Modello AI
VLA (visione-linguaggio-azione)

Pilot industriale
BMW Spartanburg

Link al video

Unitree H1 / G1 — Unitree Robotics

CARATTERISTICHE

Produttore
Unitree Robotics (CN)

Altezza
H1: ~ 1,80 m · G1: ~ 1,32 m

Peso
H1: ~ 47 kg · G1: ~ 35 kg

Velocità max
H1: > 3 m/s (record bipede)

Mercato
Ricerca + industriale general-purpose

Link al video

Dove cade un umanoide industriale nel Reg. 1230

Art. 3 punto 1	**È una "macchina" ai sensi del Regolamento** Insieme con sistema di azionamento, parti collegate (di cui almeno una mobile), per applicazione determinata. L'umanoide rientra a pieno titolo.
All. I parte A punto 6	**Probabilmente ad alto rischio** Se le funzioni di sicurezza (riconoscimento ostacoli, evitamento collisioni) sono affidate al modello AI auto-evolutivo: organismo notificato obbligatorio (Art. 25 par. 2).
All. III RESS 1.1.6 lett. f) e g)	**Interfaccia uomo-macchina avanzata** Interfaccia adeguata, comunicazione di azioni pianificate, risposta gestuale/verbale alle persone — requisiti pensati esattamente per gli umanoidi.

Comunicazione e gestualità degli umanoidi

ALLEGATO III, PUNTO 1.1.6 LETTERA (G) — ERGONOMIA

«se del caso, adeguare una macchina o un prodotto correlato dotati di un comportamento o una logica integralmente o parzialmente auto-evolutivi e che sono progettati per funzionare con livelli variabili di autonomia affinché rispondano alle persone adeguatamente e appropriatamente (ad esempio verbalmente attraverso parole e non verbalmente attraverso gesti, espressioni facciali o movimento del corpo) e comunichino le loro azioni pianificate (ad esempio cosa faranno e perché) agli operatori in maniera comprensibile»

OSSERVAZIONE

È la prima volta che una norma europea di prodotto industriale prescrive a una macchina di comunicare verbalmente, gestualmente e di anticipare le sue azioni. Disposizione pensata per umanoidi e cobot AI-driven.

Sistemi auto-evolutivi: tre obblighi specifici

Per i sistemi di controllo con comportamento o logica auto-evolutivi:

ALLEGATO III, PUNTO 1.2.1 — LETTERA (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»

ALLEGATO III, PUNTO 1.2.1 — LETTERA (B)

«consentire che siano registrati i dati relativi al processo decisionale in materia di sicurezza per i sistemi di sicurezza basati su software che garantiscono la funzione di sicurezza […] dopo che la macchina o il prodotto correlato sono stati immessi sul mercato […] conservati per un anno dopo la loro raccolta»

ALLEGATO III, PUNTO 1.2.1 — LETTERA (C)

«consentire in qualsiasi momento la correzione della macchina o del prodotto correlato al fine di preservarne la sicurezza intrinseca»

Punti normativi ancora da risolvere

01 Valutazione rischio in ambiente non strutturato

ISO 12100 presuppone pericoli identificabili; con umanoidi in spazi aperti l'inventario tende all'indeterminato.

02 Soglie biomeccaniche di ISO/TS 15066

Pensate per bracci fissi; un umanoide di 60-80 kg che cade trasferisce energia cinetica molto superiore.

03 Norme armonizzate ancora assenti

Per la categoria umanoidi non c'è ancora una norma di tipo C. prEN 50742 in elaborazione per la parte cyber.

04 Catena di responsabilità modelli foundation

Il fabbricante della macchina spesso NON sviluppa il modello AI. Tema di accountability ancora aperto.

SEZIONE 3

3 AI nel Regolamento: All. I, All. II e RESS auto-evolutivi

Il software è componente di sicurezza

ART. 3 PUNTO 3 — 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 ma che non è indispensabile per il funzionamento di tale prodotto, o per il quale componenti normali possono essere sostituiti per il funzionamento di tale prodotto»

CONSIDERANDO 19 — LA RATIO

«L'evoluzione del settore delle macchine ha determinato il ricorso crescente a mezzi digitali e i software svolgono un ruolo sempre più importante […]. Inoltre, la definizione di componenti di sicurezza dovrebbe riguardare non soltanto i dispositivi fisici ma anche quelli digitali. Al fine di tenere conto del crescente ricorso ad esso come componente di sicurezza, il software che svolge una funzione di sicurezza ed è immesso in maniera indipendente sul mercato dovrebbe essere considerato un componente di sicurezza.»

Punti 18 e 19: distinzione fondamentale

Nell'elenco indicativo di componenti di sicurezza il legislatore distingue due categorie:

ALLEGATO II PUNTO 18 — SOFTWARE (GENERALE)

«Software che garantisce funzioni di sicurezza.»

ALLEGATO II PUNTO 19 — SOFTWARE AI AUTO-EVOLUTIVO

«Componenti di sicurezza dotati di un comportamento integralmente o parzialmente autoevolutivo che utilizzano approcci di apprendimento automatico che garantiscono funzioni di sicurezza.»

LA DIFFERENZA È SOSTANZIALE

- Solo il punto 19 (AI auto-evolutivo) è automaticamente in All. I parte A (alto rischio).
- Il punto 18 generico NON comporta in sé l'obbligo di notified body.
- Considerando 55: la valutazione di terzi del software safety vale solo per i sistemi AI auto-evolutivi.

AI nelle categorie ad alto rischio

Soggette ad Art. 25 par. 2 — una procedura a scelta tra esame UE del tipo (modulo B+C), garanzia qualità totale (modulo H) o verifica di un unico prodotto (modulo G); in tutti e tre i casi con organismo notificato

ALL. I PARTE A · PUNTO 5

«Componenti di sicurezza dotati di un comportamento integralmente o parzialmente autoevolutivo che utilizzano approcci di apprendimento automatico che garantiscono funzioni di sicurezza.»

ALL. I PARTE A · PUNTO 6

«Macchine che integrano sistemi con un comportamento integralmente o parzialmente autoevolutivo che utilizzano approcci di apprendimento automatico che garantiscono funzioni di sicurezza che non sono state immesse in modo indipendente sul mercato, solo per quanto riguarda tali sistemi.»

Nota: il punto 6 si applica solo ai sistemi NON già immessi separatamente sul mercato (e dunque non già certificati).

Considerando 54: perché l'AI auto-evolutiva è in All. I

CONSIDERANDO 54

«i sistemi con comportamento evolutivo che garantiscono funzioni di sicurezza dovrebbero essere inclusi nell'allegato I a causa delle loro caratteristiche quali la dipendenza dai dati, l'opacità, l'autonomia e la connettività, che potrebbero aumentare considerevolmente la probabilità e la gravità del danno e compromettere gravemente la sicurezza della macchina o del prodotto correlato»

01	02	03	04
Dipendenza dai dati	**Opacità**	**Autonomia**	**Connettività**

Art. 3 p.16 + Art. 18: l'update del modello

Il caso pratico

Un aggiornamento OTA del modello AI di una macchina già immessa sul mercato. Il modello, dopo l'update, esplora nuove azioni che richiedono ripari aggiuntivi o nuove protezioni meccaniche per essere sicure.

CONSEGUENZE NORMATIVE

- L'update rientra in modifica sostanziale ex Art. 3 punto 16 (mezzi digitali) SE soddisfa anche la condizione (a) o (b).
- Chi effettua la modifica diventa fabbricante ex Art. 18, salvo l'utilizzatore non professionale per uso proprio.
- Va applicata la procedura di valutazione della conformità ex Art. 25 par. 2-4 — riapposizione della marcatura CE.
- Da All. III parte B punto 1: la valutazione del rischio originale doveva già coprire l'evoluzione prevista del comportamento.

SEZIONE 4

4 Cybersecurity: RESS 1.1.9 e 1.2.1

Per la prima volta: l'attore ostile

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 cibersicurezza.»

IL SALTO NORMATIVO

Dalla 2006/42/CE alla 2023/1230: dal solo "non malizioso" anche al "malizioso".

- *Confine espresso: misure "proporzionate" e "limitate alla protezione della sicurezza" del prodotto (non cybersecurity in senso lato).*
- *Tutto ciò che è cybersecurity NON di prodotto resta ad altri atti UE (Cybersecurity Act, CRA, NIS2).*

Protezione dall'alterazione

ALLEGATO III, PUNTO 1.1.9 — APERTURA

«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.»

ALLEGATO III, PUNTO 1.1.9 — SOFTWARE E DATI CRITICI

«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.»

ALLEGATO III, PUNTO 1.1.9 — EVIDENZE DI INTERVENTO

«La macchina o il prodotto correlato devono raccogliere prove di un intervento legittimo o illegittimo sul software o di una modifica del software installato […] o della sua configurazione.»

I sistemi di comando contro l'attacco

ALLEGATO III, PUNTO 1.2.1 — LETTERA (A)

«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»

LETTURA NORMATIVA

La formula «tentativi deliberati ragionevolmente prevedibili da parte di terzi» fa entrare il threat modeling nella safety di prodotto.

- *Soglia: ragionevolmente prevedibili — non tutti gli attacchi possibili, ma quelli verosimili nel contesto d'uso.*
- *Conseguenza pratica: l'analisi delle minacce affianca l'analisi dei pericoli ISO 12100 nel dossier tecnico.*

Tracciabilità del software safety: 5 anni

ALLEGATO III, PUNTO 1.2.1 — LETTERA (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»

Obblighi operativi

- Log strutturato di ogni intervento sul software safety post-immissione (chi, quando, cosa).
- Versionamento e retention obbligatoria 5 anni dal caricamento — anche per gli aggiornamenti OTA.
- Accesso "motivato" delle autorità nazionali competenti: il dato deve essere recuperabile.

Presunzione di conformità via Reg. (UE) 2019/881

ART. 20 PAR. 9 — SINTESI NORMATIVA

«Le macchine e i prodotti correlati certificati nell'ambito di un sistema di certificazione della cibersicurezza adottato ai sensi del Reg. (UE) 2019/881 — i cui riferimenti siano stati pubblicati nella GUUE — sono considerati conformi ai RESS 1.1.9 e 1.2.1, per la protezione contro la corruzione e per la sicurezza e affidabilità dei sistemi di controllo, nei limiti delle previsioni certificate.»

LA SCORCIATOIA OPERATIVA

Una macchina certificata sotto schema EUCC (o futuri schemi del Cybersecurity Act) gode di presunzione di conformità ai RESS cyber del Regolamento 1230. Si evita la duplicazione di certificazioni sullo stesso rischio.

SEZIONE 5

5 Scenari di rischio applicativi

5.1 · SCENARIO

Manipolazione remota di un cobot

Situazione

Cobot connesso via OPC UA. Phishing su rete IT → propagazione a OT → modifica dei parametri PFL → impatto sull'operatore.

RESS applicabili

- All. III RESS 1.1.9 (protezione alterazione)
- All. III RESS 1.2.1 (a) (resistenza ad attacchi)
- All. III RESS 1.2.1 (d) (limiti safety non modificabili)
- All. III RESS 1.2.1 (f) (log 5 anni)

Misure di compliance

- Autenticazione forte degli accessi ai parametri safety
- Integrità delle ricette/parametri firmata
- Segregazione di rete IT/OT con DPI
- Parametri PFL in livello safety non scrivibile da applicativo
- Log accessi conservati ≥ 5 anni
- Possibile presunzione di conformità via certificazione cyber Reg. 2019/881 (Art. 20 par. 9)

Oltre il prodotto: la catena della cybersicurezza

Il Considerando 25 lo anticipa: il Reg. 1230 «non preclude l'applicazione […] di altri atti giuridici dell'Unione che affrontano specificamente aspetti di cibersicurezza». La sicurezza reale di una macchina connessa vive sulla cerniera IT/OT — e su quella cerniera convergono tre atti UE distinti, in capo a soggetti distinti.

Reg. 2023/1230 - Macchina	Reg. 2024/2847 — CRA —Componenti digitali	Dir. 2022/2555 — NIS2 — Utilizzatore
RESS 1.1.9 (protezione dall'alterazione), 1.2.1 lett. (a) (resistenza ad attacchi) e (f) tracciabilità 5 anni). Cybersecurity di prodotto, perimetro della macchina.	Cybersecurity by design del software e dei componenti digitali immessi separatamente (controllori, gateway, moduli AI). SBOM, gestione vulnerabilità, notifica incidenti.	Misure organizzative e tecniche: segmentazione IT/OT, gestione accessi, risposta incidenti, formazione. Soggetto essenziale o importante secondo dimensione e criticità. Si somma agli obblighi del D.Lgs. 81/2008 come datore di lavoro.

LETTURA NORMATIVA

La cybersecurity di una macchina collaborativa non è un obbligo unico ma una catena. Se uno degli anelli salta, la conformità formale del prodotto non basta a tenere in piedi la safety reale.

5.3 · SCENARIO

Umanoide industriale con riconoscimento biometrico

Un umanoide industriale riconosce gli operatori autorizzati alla cella tramite face matching per personalizzare l'interazione (RESS 1.1.6 lett. f e g).

Triplo binario normativo

Reg. 2023/1230	AI Act 2024/1689	GDPR 2016/679
Componente di sicurezza (All. II p. 19). Categoria All. I parte A p. 5 o 6: notified body. RESS 1.1.6 e 1.2.1.	Biometria — All. III categoria 1. Possibili profili di Art. 5 in determinati spazi pubblici.	Trattamento di dato biometrico (Art. 9). Base giuridica, DPIA (Art. 35), informativa.

SEZIONE 6

6 Appendici tecniche: ISO/TS 15066 e prEN 50742

Limiti biomeccanici quasi-statici per contatto cobot-uomo

Soglie di pressione e forza massime ammesse per contatto in modalità PFL (estratto Tabella A.2 / A.3).

Regione corporea	Pressione quasi-statica [N/cm²]	Forza quasi-statica [N]
Cranio / fronte	130	130
Viso	110	65
Collo (lato)	140	150
Spalla, articolazioni	160	210
Torace	140	140
Addome	110	110
Braccio, gomito	190	150
Mano, dito	260	140
Coscia	250	220

NOTE OPERATIVE

Pressione max:
applicata su area di contatto piccola (dito, spigolo)

Forza max:
applicata su area più ampia (piano)

Quasi-statico = contatto con corpo bloccato (clamping); transitorio = contatto libero (recoil possibile). I limiti raddoppiano per contatto transitorio.

Per umanoidi (60-80 kg): l'energia cinetica trasferita in una caduta supera ampiamente queste soglie. Limiti da rivedere?

Norma armonizzata cyber in elaborazione

Titolo

Safety of machinery — Protection of machinery against corruption (CENELEC TC 44X)

Norma armonizzata in elaborazione per supportare la dimostrazione di conformità ai RESS 1.1.9 (protezione dall'alterazione) e ai requisiti associati di 1.2.1 lettere (a) e (f) (resistenza ad attacchi)

Stato e impatto

Stato attuale

Documento prEN in elaborazione presso CENELEC TC 44X. Citazione formale ancora non disponibile nella GUUE.

Cosa fornirà

Procedure e requisiti tecnici per dimostrare la conformità al RESS 1.1.9 (protezione dall'alterazione) e al RESS 1.2.1 (a) e (f)

Ruolo nel sistema

Una volta pubblicata e citata nella GUUE darà presunzione di conformità (Art. 20). Nel frattempo: vale il principio di Art. 17 (norma di stato dell'arte).

SEZIONE 7

7 Riepilogo e domande

Cosa portare a casa:

1. **Il software è componente di sicurezza (Art. 3 p. 3)**

   La definizione di componente di sicurezza include esplicitamente il software.

2. **Solo l'AI auto-evolutiva = alto rischio (All. I parte A 5-6)**

   Considerando 55: la valutazione di terzi vale solo per i sistemi AI auto-evolutivi, non per ogni software.

3. **RESS 1.1.6 lett. f e g sono pensati per umanoidi**

   Interfaccia adeguata, gesti, comunicazione delle azioni pianificate.

4. **Cybersecurity nei RESS 1.1.9 e 1.2.1 lett. (a)**

   Per la prima volta una norma di prodotto cita l'attore ostile.

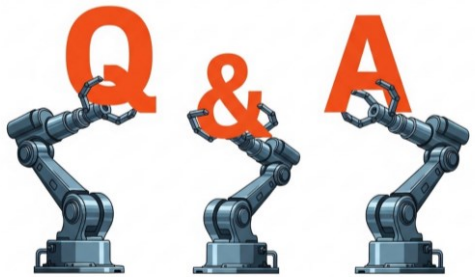
5. **Modifica sostanziale anche digitale, con soglia (Art. 3 p. 16)**

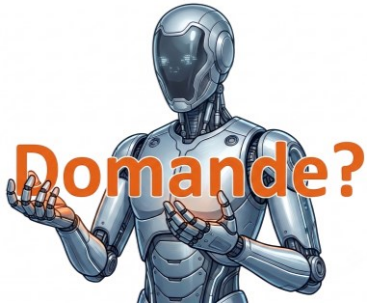
   Non basta che incida sulla sicurezza: deve richiedere ripari/protezioni aggiuntivi o misure di stabilità.

Articoli e allegati richiamati

Art. 3 p. 3	Componente di sicurezza (include software)
Art. 3 p. 16	Modifica sostanziale (con condizioni a/b)
Art. 18	Chi modifica diventa fabbricante
Art. 20 par. 9	Presunzione conformità via Reg. 2019/881
Art. 25 par. 2	Procedura conformità per All. I parte A
All. I parte A p. 5	Componenti AI auto-evolutivi (alto rischio)
All. I parte A p. 6	Macchine che integrano AI auto-evolutiva
All. II punto 18	Software che garantisce funzioni di sicurezza
All. II punto 19	Componenti AI auto-evolutivi
All. III 1.1.6 (f/g)	Ergonomia per macchine auto-evolutive
All. III 1.1.9	Protezione dall'alterazione
All. III 1.2.1 (a-f)	Sicurezza sistemi di comando
All. III 1.3.7	Elementi mobili: coesistenza e interazione
All. III 1.5.14	Rischio di restare imprigionati

Grazie per l'attenzione





"Il Regolamento (UE) 2023/1230 ha già scritto, nei suoi RESS, il quadro per cobot e umanoidi. Il nostro compito di ingegneri è tradurlo in progetti"

Ing. **Fabrizio Catinari**

Ingegneria e Innovazione

+39 335 7898179

fabrizio@ingcatinari.com

www.ingcatinari.com