

Automation TECHNOLOGY

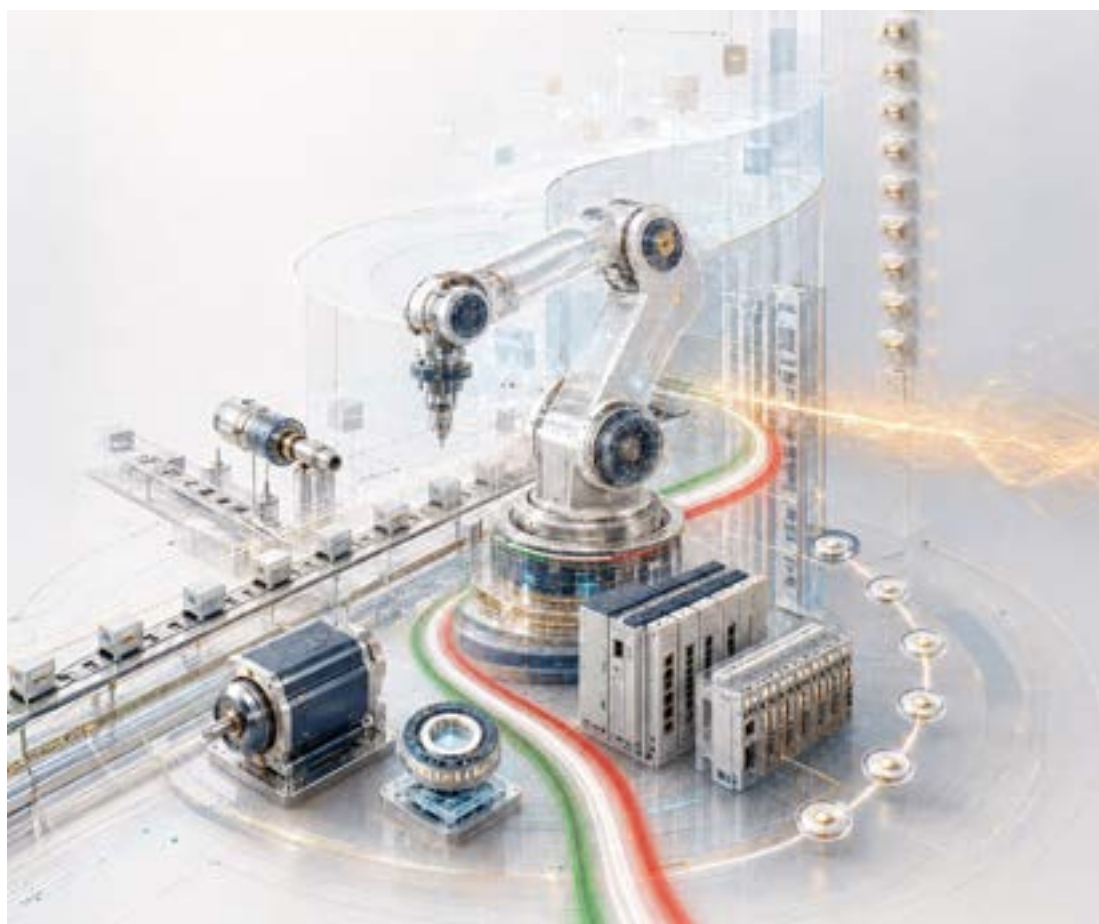
Industrial Technologies | Plant & Asset Management | Digital Transformation

#EVENTI
DAL MADE IN
ITALY AL «MADE
BY ITALY»

#MERCATI
LA TOP 20 DELL'AUTOMAZIONE ITALIANA

#OPERATIONS
DAL GUASTO ALLA SOLUZIONE CON IL METODO 8D

#SECURITY
AGENTI AI: IL RISCHIO ENTRA NELLE RETI OT



NANO & QUBO

Strumenti di misura multifunzione per applicazioni
in BT e MT



Inquadra
il QR Code
e visita il sito

EFRER
LOOK BEYOND. MEASURE BETTER!



persone



partnership



soluzioni



Siamo un **team italiano** in continua evoluzione, al fianco di chi ogni giorno affronta le sfide di un mercato dinamico nel settore elettrotecnico.

Crediamo in una collaborazione autentica, fatta di ascolto e fiducia, dove competenze e passione si trasformano in soluzioni concrete.

Human CollaborAction:
l'energia delle persone,
la forza delle soluzioni.

DKC
NEXT TO YOU

www.dkceurope.com



IN COPERTINA
La Top 20
dell'automazione
Made in Italy

7 **EDITORIALE / EDITORIAL**
LA CONFORMITÀ CHE CREA MERCATO /
COMPLIANCE THAT CREATES MARKETS
Armando Martin

8 **FIERE & EVENTI / TRADE FAIRS & EVENTS**
DAL MADE IN ITALY AL «MADE BY ITALY»:
L'AUTOMAZIONE ITALIANA CERCA IL VALORE
OLTRE IL COMPONENTE
A cura della Redazione

14 **TREND & SCENARI / TRENDS & SCENARIOS**
LA TOP 20 DELL'AUTOMAZIONE MADE IN ITALY
A cura di Armando Martin

22 **SICUREZZA & PROTEZIONE / SAFETY & SECURITY**
CRA, DALL'11 SETTEMBRE LA CYBER-RESILIENZA
DIVENTA OPERATIVA
A cura della Redazione

28 **AUTOMAZIONE E CONTROLLO /
AUTOMATION AND CONTROL**
COME L'INTELLIGENZA ARTIFICIALE TRASFORMA
LE IT OPERATIONS, ANCHE NEI DATA CENTER
DELLE PMI
A cura di Damiano Cosma De Angelis



Automation TECHNOLOGY

Anno X - N.38 - Settembre / Ottobre 2026
www.automationtechnology.editorialedelfino.it



34 **STRUMENTAZIONE / INSTRUMENTATION**
DISCHI DI ROTTURA: FUNZIONAMENTO,
NORMATIVE E CONFRONTO CON LE VALVOLE
DI SICUREZZA - SECONDA PARTE
A cura di Alessandro Brunelli

40 **SOFTWARE & PIATTAFORME**
DAL MICROPROCESSORE AL TENSORE:
L'ARCHITETTURA DEI CHIP NELL'ERA DELL'AI
A cura di Massimo Nannini

44 **OPERATIONS & APPLICATIONS**
DAL GUASTO ALLA SOLUZIONE
CON IL METODO 8D
A cura di Laura Profeta

50 **SICUREZZA & PROTEZIONE / SAFETY & SECURITY**
CYBERSECURITY INDUSTRIALE: QUATTRO FALSI
MITI DA SUPERARE
A cura di Exor International

54 **SOFTWARE & PIATTAFORME**
APPLICATION OF AUTOMATION STUDIO®
FOR INTEGRATED MULTI-DOMAIN MODELLING
IN MECHATRONIC SYSTEMS
A cura di Filippo Mazzocato, Luigi Mazza

64 **CONSULENZA D'IMPRESA /
BUSINESS CONSULTANCY**
PRIMA I PROCESSI, POI IL SOFTWARE
A cura di Fedele Maniglio

68 **SICUREZZA & PROTEZIONE / SAFETY & SECURITY**
AGENTI AI E SICUREZZA OT: LA LEZIONE
DEL CASO OPENAI-HUGGING FACE
A cura di Simone Facchinetti

72 **PROMOREDAZIONE**
SOFTING INDUSTRIAL AUTOMATION: COME
TRASFORMARE I DATI DI FABBRICA IN VALORE
A cura della Redazione

75 **NEWS**
I³NEWS - Industry • Innovation • Insights
A cura della Redazione

80 **SAVE THE DATE 2026**
EVENTI E FIERE DEL SETTORE / EVENTS&EXHIBITIONS

AUTOMATION TECHNOLOGY

Rivista internazionale di tecnologie industriali, automazione di processo, gestione di impresa, trasformazione digitale
International magazine of industrial technologies, process automation, enterprise management, digital transformation

Anno X N.38 - Pubblicazione Settembre / Ottobre 2026

Year X N.38 - Publication September / October 2026

Periodico trimestrale pubblicato da Editoriale Delfino

Quarterly magazine published by Editoriale Delfino

Editoriale Delfino pubblica anche volumi e le seguenti riviste:

CL II Cartolibraio, EDM Power Electronics Design, Elettrofazione, Power Technology,

Editoriale Delfino also publishes volumes and the following magazines: CL II Cartolibraio, EDM Power Electronics Design, Elettrofazione, Power Technology.

Direzione, Redazione, Segreteria di Redazione, Ufficio Pubblicità Management, Editorial office, Editorial office, Advertising office

Via Aurelio Saffi 9 – 20123 Milano

Tel. +39 02-9578.4238

editorialedelfino.it

automationtechnology.editorialedelfino/

email generale: info@editorialedelfino.it

PEC: editorialedelfino@pec.editorialedelfino.it

REDAZIONE E CONTATTI/EDITORIAL STAFF AND CONTACTS

Direttore Responsabile/Responsible Director

Andrea Ferriani

Direttore Editoriale/Editorial Director

Armando Martin

Comitato Scientifico/Scientific Committee

Solomon Almadi, Ugo Baggi, Alessandro Brunelli, Josè Covelli, Francisco Diaz Andreu, Giuliano Monizza, Massimo Nannini, Alberto Sibono, Enzo Maria Tieghi

Hanno collaborato a questo numero/Have collaborated on this issue

Alessandro Brunelli, Cosma Damiano De Angelis, Simone Facchinetti, Armando Martin, Filippo Mazzocato, Massimo Nannini, Fedele Maniglio, Luigi Mazza, Laura Profeta

AI Disclaimer

Alcuni contenuti e immagini sono stati elaborati o revisionati con il supporto di strumenti di intelligenza artificiale. Tutti i materiali sono sottoposti al controllo editoriale umano; la responsabilità della pubblicazione resta in capo alla redazione e agli autori.

Some content and images have been created or revised with the support of artificial intelligence tools. All materials undergo human editorial review; responsibility for publication remains with the editorial team and the authors.

Pubblicità/Advertising

info@editorialedelfino.it

Email redazione/Editorial Email

atred@editorialedelfino.it

Ufficio Traffico/Traffic Office

florian.mara78@gmail.com

ABBONAMENTI/SUBSCRIPTIONS

Ufficio abbonamenti/Subscription Office

abbonamenti@editorialedelfino.it

Condizioni di abbonamento/Subscription conditions

Cartaceo Annuale / Yearly Paper: € 46,00

Pdf Annuale / Yearly Pdf: € 28,00

Copia Amazon / Amazon Copy: € 9,99

L'abbonamento si attiva mediante:

- Versamento sul conto corrente postale 61080917
- Bonifico bancario su IBAN: IT 76 W 07601 01600 000 061 080 917
- Carta di credito esclusivamente tramite sito internet editorialedelfino.it

The subscription is activated by means of:

- Transfer to postal current account 61080917
- Bank transfer to IBAN: IT 76 W 07601 01600 000 061 080 917
- Credit card exclusively via website www.editorialedelfino.it

Singola copia/Single copy

Costo singola copia € 11,00, € 15,00 (arretrata)

Gli importi sopra riportati sono da intendersi già al netto di eventuali costi bancari, postali e altri oneri.

Single copy cost € 11,00, € 15,00 (backlog)

The above amounts are net of any bank, postal and other charges.



I.V.A. assolta dall'Editore ai sensi dell'articolo 74 lettera C del D.P.R. 633/72. Le richieste di eventuali fascicoli arretrati non pervenuti, dovranno essere comunicate all'indirizzo abbonamenti@editorialedelfino.it, entro e non oltre due mesi dalla data di non ricezione degli stessi.

V.A.T. paid by the Publisher pursuant to Article 74 letter C of Presidential Decree 633/72. Requests for any backlog files not received should be sent to the following address abbonamenti@editorialedelfino.it at the latest two months after the date of non-receipt.

Associazioni Partner



Fiere & Eventi di cui AT è media partner



GESTIONE DATI E STAMPA

È vietata la riproduzione anche parziale degli articoli, fotografie, tabelle, disegni e immagini senza la preventiva autorizzazione della casa editrice. Manoscritti con relative immagini non si restituiscono anche se non pubblicati. La Direzione della testata non è responsabile dei testi redazionali, delle opinioni espresse da autori e collaboratori, né dei messaggi pubblicitari che sono pubblicati in conformità alle richieste dell'inserzionista.

Editoriale Delfino garantisce che i dati custoditi nel proprio archivio elettronico non saranno ceduti ad altri e saranno utilizzati per l'invio della rivista, delle newsletter e delle DEM. Tali dati verranno gratuitamente rettificati o cancellati su richiesta dell'interessato. Poste Italiane S.p.A. Spedizione in abbonamento postale D.L. 353/2003 (Conv. in L. 27 febbraio 2004 n. 46) art. 1, comma 1, LO/MI Milano. La pubblicità non supera il 45% della superficie totale della rivista.

Iscrizione ROC 11421 del 17 settembre 2005.

Impaginazione: Mara Florian - Vertemate con Minoprio (CO)

Stampa: Mediagrat SpA - Noventa Padovana (PD)

Prodotto interamente realizzato in Italia

Editoriale Delfino: da sempre sostenitrice del Made in Italy

DATA MANAGEMENT AND PRINTING

Reproduction, even partial, of articles, photographs, tables, drawings and images is forbidden without the prior authorisation of the publishing house. Manuscripts with related images are not returned even if not published. The management of the magazine is not responsible for editorial texts, opinions expressed by authors and collaborators, nor for advertising messages that are published in accordance with the requests of the advertiser.

Editoriale Delfino guarantees that the data stored in its electronic archive will not be transferred to others and will be used to send the magazine, the newsletters and the DEM. These data will be corrected or deleted free of charge at the request of the interested party. Poste Italiane S.p.A. Shipment by postal pass D.L. 353/2003 (Conv. in L. 27 febbraio 2004 n. 46) art. 1, paragraph 1, LO/MI Milan. Advertising does not exceed 45% of the total area of the magazine.

Layout: Mara Florian - Vertemate con Minoprio (CO)

Press: Mediagrat SpA - Noventa Padovana (PD)

Product entirely made in Italy

Editoriale Delfino: always a supporter of Made in Italy



linkedin.com/company/automationtechnology

automationtechnology.editorialedelfino.it/



Advantech	79	IXON	78
ANIE Automazione	8, 9, 14-20	Lafert Group	15, 16, 18, 20
Asem	15, 16, 19, 20	Lovato Electric	16, 18
Bausano	79	M.ake Global	8, 11, 67
BI-MU	74, 77, 80	Metal Work	16, 17
Bonfiglioli	8-10, 14-19, 56-59	MOMODESIGN Centro Stile	78
Camozzi Group	16, 17	Motovario	16, 19
Carlo Gavazzi Controls	16, 20	NVIDIA	41, 42, 79
Comau	8, 10, 15-17, 20	OpenAI	68-71
Corvina	8, 10, 16, 19, 50-53	PatSnap	77
Datalogic	15-17	Pneumax	8, 10, 16, 18
DKC	I COP	Pizzato Elettrica	16, 19, 20
Duplomatic MS	16, 18, 20	ReeR	14, 16, 19, 20
ETA	16, 20	SAVE Verona	76, 80
Eurotech	15, 16, 19	Save the Date 2026	80
Exor International	8, 15, 16, 19, 20, 50-53	Seco	15-18
Finder	16, 18	Siemens	17, 73, 77
Gefran	16, 18, 79	Softing Industrial Automation	72-74
Hannover Messe	80	SPS Italia	8-12, 80
Hugging Face	68-71	Veronafiore	76
IEMA	78	World Robot Conference	76
IIoT World	77		



**Selezionato tra le 50 migliori
opere di divulgazione
scientifica 2025**



Autore: Armando Martin **Titolo:** Automation Megatrend **Sottotitolo:** Come le tendenze più innovative dell'Automazione stanno trasformando le attività industriali e plasmando il nostro futuro **Prefazione:** a cura di Jacopo Di Blasio **Postfazione:** a cura di Mario Gargantini **Formato:** 17 x 24 cm. **Casa Editrice:** Editoriale Delfino **ISBN:** 979-12-5520-104-5 **Numero di pagine:** 352 **Edizione:** I edizione 2025
<https://editorialedelfino.it/prodotto/automation-megatrend/>

THE SPACE < EARTH INDUSTRY CONVERGENCE HUB

Where exploration ends, integration begins

The solutions you're looking for might have
been developed in a world you don't know . . . yet

RIMINI EXPO CENTRE • RIMINI, ITALY
23—25 SEP 2026

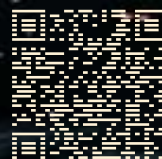
ORGANIZED BY
**ITALIAN
EXHIBITION
GROUP**
Providing the future

IN COLLABORATION WITH



Ministero degli Affari Esteri
e della Cooperazione Internazionale

ITA
ITALIAN TRADE AGENCY



DRIVING
THE ENERGY
TRANSITION

27

KEY

THE
ENERGY
TRANSITION
EXPO

10 — 12
MARCH
2027

RIMINI
EXPO
CENTRE
Italy

Registrati ora,
scarica
il biglietto



key-expo.com
#climatefriends

Organized by
**ITALIAN
EXHIBITION
GROUP**
Providing the future

In collaboration with



Ministero degli Affari Esteri
e della Cooperazione Internazionale

ITA
ITALIAN TRADE AGENCY

OpportunItaly
Opportunities for your business in Italy

Simultaneously with



**ITALIA
SOLARE**
Il fotovoltaico è di tutti



**Forum
Tech**



LA CONFORMITÀ CHE CREA MERCATO



a cura di Armando Martin

Per molte PMI la nuova stagione normativa appare come una grandinata di adempimenti: AI Act, CRA (Cyber Resilience Act), NIS2, sostenibilità, Ecodesign e futuro Passaporto digitale di prodotto. Procedure, competenze e verifiche sui fornitori assorbono risorse scarse. Ma parlare soltanto di burocrazia significa perdere il punto industriale, nella misura in cui queste norme stanno ridisegnando i requisiti di accesso al mercato.

Dal 2 agosto 2026 sono applicabili nuove disposizioni dell'AI Act, comprese quelle sulla trasparenza, mentre l'obbligo di alfabetizzazione sull'AI vale già dal febbraio 2025. Anche una PMI che usa sistemi generativi per marketing, assistenza clienti o selezione del personale deve sapere quali strumenti impiega, con quali dati e sotto quale controllo umano. Per un costruttore di macchine che introduce AI nella manutenzione predittiva, la domanda non può più essere soltanto «funziona?», ma anche «quali rischi genera e come li governiamo?».

Sul fronte cyber la scadenza più vicina è l'11 settembre 2026. Il CRA impone ai fabbricanti di prodotti con elementi digitali di segnalare vulnerabilità attivamente sfruttate e incidenti gravi, con un primo avviso entro 24 ore e la notifica entro 72. Per chi produce PLC, gateway, HMI o dispositivi IoT significa organizzare vulnerability management, aggiornamenti e responsabilità nella supply chain. Gli obblighi principali scatteranno nel dicembre 2027, ma architetture e cicli di sviluppo non si correggono in poche settimane. Anche le norme green seguono la stessa logica. Le semplificazioni europee hanno alleggerito l'impatto diretto della CSRD (Corporate Sustainability Reporting Directive) sulle PMI, senza eliminare le richieste di clienti, banche e capofiliere su emissioni, materiali e tracciabilità. L'Ecodesign for Sustainable Products Regulation porterà progressivamente requisiti di durabilità, riparabilità e Passaporto digitale di prodotto. Il dato ambientale, come la distinta base cyber-sicura, diventa parte del prodotto. L'onere esiste e va riconosciuto. Servono standard, strumenti accessibili e incentivi, altrimenti la conformità favorirà soprattutto le grandi imprese. Ma per le PMI che si muovono per tempo può diventare un vantaggio partire da meno incidenti, prodotti migliori, filiere trasparenti e più credibilità sui mercati internazionali. La conformità non dovrebbe essere l'ultima firma prima della vendita, ma una funzione della progettazione. È così che il costo regolatorio può trasformarsi in investimento industriale.

COMPLIANCE THAT CREATES MARKETS

For many SMEs, the new regulatory landscape looks like a hailstorm of compliance requirements: the AI Act, the CRA (Cyber Resilience Act), NIS2, sustainability rules, Ecodesign and the forthcoming Digital Product Passport. Procedures, specialist expertise and supplier audits consume already scarce resources. Yet focusing solely on bureaucracy misses the industrial significance of these measures, as they are reshaping the requirements for market access.

New provisions of the AI Act have applied since 2 August 2026, including transparency requirements, while the obligation to ensure adequate AI literacy has already been in force since February 2025. Even an SME using generative systems for marketing, customer service or recruitment must know which tools it is using, what data they process and what human oversight is in place. For a machine builder introducing AI into predictive maintenance, the question can no longer be simply, "Does it work?", but must also include, "What risks does it create, and how do we manage them?" On the cybersecurity front, the nearest deadline is 11 September 2026. The CRA requires manufacturers of products with digital elements to report actively exploited vulnerabilities and severe incidents, issuing an early warning within 24 hours and a notification within 72 hours. For manufacturers of PLCs, gateways, HMIs or IoT devices, this means establishing vulnerability-management processes, update procedures and clear responsibilities across the supply chain. The main obligations will apply from December 2027, but architectures and development cycles cannot be corrected in just a few weeks.

Green regulations follow the same logic. European simplification measures have reduced the direct impact of the CSRD (Corporate Sustainability Reporting Directive) on SMEs, without eliminating requests from customers, banks and lead companies for information on emissions, materials and traceability. The Ecodesign for Sustainable Products Regulation will progressively introduce requirements concerning durability, reparability and the Digital Product Passport. Environmental data, like a cybersecurity bill of materials, is becoming an integral part of the product itself.

The burden is real and must be acknowledged. Standards, accessible tools and incentives are needed; otherwise, compliance will mainly benefit larger companies. For SMEs that act early, however, it can become a competitive advantage, delivering fewer incidents, better products, more transparent supply chains and greater credibility in international markets. Compliance should not be the final signature before a sale, but an integral part of the design process. This is how the cost of regulation can be transformed into industrial investment.



DAL MADE IN ITALY AL «MADE BY ITALY»: L'AUTOMAZIONE ITALIANA CERCA IL VALORE OLTRE IL COMPONENTE



a cura della Redazione

Alla tavola rotonda organizzata da Editoriale Delfino durante SPS Italia 2026, imprese, tecnologi e consulenti si sono confrontati sul passaggio dall'eccellenza di prodotto alla capacità di progettare sistemi intelligenti, piattaforme e nuovi modelli industriali. Dati di mercato, servitizzazione, efficienza energetica, AI, regole europee e ruolo delle PMI compongono un quadro nel quale hardware e software non si escludono: il vero vantaggio nasce dalle decisioni che la loro integrazione rende possibili.

Il Made in Italy industriale sa progettare motori, robot, valvole, macchine e linee competitive sui mercati più esigenti. La domanda, oggi, è un'altra: **chi governerà l'intelligenza del sistema nel quale quei componenti lavorano?** È da questo interrogativo che ha preso le mosse la tavola rotonda "Dal Made in Italy al «Made by Italy»", promossa da Editoriale Delfino il 26 maggio nell'Arena Next di SPS Italia 2026, a Fiere di Parma. Moderato da Armando Martin, direttore editoriale di *Automation Tech-*

nology, il confronto ha riunito Marco Vecchio, segretario ANIE Automazione, per il market outlook; Fabrizio Di Stasio, Solution Marketing Manager di Bonfiglioli; Francesco Renelli, Head of Strategy & Intelligence di Comau; Stefano Isella, Chief Sales Officer di Exor International/Corvina; Domenico Di Monte, Corporate Brand Manager di Pneumax; Cosma Damiano De Angelis, esperto di AI e Big Data; Simone Facchinetti, avvocato d'impresa; e Fedele Maniglio, consulente strategico M.ake Global. Sul tavolo non c'era un semplice ag-



giornamento tecnologico, ma la posizione che l'industria italiana intende occupare nella catena del valore digitale.

Un settore resiliente, ma in trasformazione

Il quadro introduttivo di Marco Vecchio ha dato profondità economica al dibattito. Dopo l'espansione eccezionale del triennio 2021-2023 e il successivo destocking, il 2025 ha mostrato una stabilizzazione migliore delle attese. La ripresa, tuttavia, non è omogenea: software, intelligenza artificiale, cybersecurity e sistemi digitali appaiono più dinamici dell'automazione tradizionale. La manifattura meccanica ed elettrotecnica rimane un pilastro dell'export e dell'occupazione italiana, ma il suo baricentro competitivo si sta spostando.

Il mercato, in altre parole, può tornare a crescere senza che il valore rimanga necessariamente dove si trovava. Il moderatore lo ha sintetizzato così: **“La crescita arriva da dove mettiamo più testa, non da dove mettiamo più ferro”**. È il passaggio decisivo: l'hardware resta indispensabile, ma dati, algoritmi, interoperabilità e servizi possono catturare una quota crescente del margine e della relazione con il cliente.

«La crescita dell'automazione è trainata sempre più da software, AI, cybersecurity e sistemi digitali: il valore si sta spostando oltre il prodotto fisico». **Marco Vecchio, Anie Automazione.**

Dal prodotto alla capacità operativa

Il primo fronte ha riguardato ciò che le aziende venderanno tra cinque anni: ancora prodotti fisici o, sempre di più, capacità operativa, performance garantita e risultati misurabili?

Per Fabrizio Di Stasio, Bonfiglioli, il componente non scompare, ma deve diventare parte di un'architettura leggibile e interoperabile. Un azionamento o un riduttore continueranno a essere giudicati per prestazioni e affidabilità; accanto ai dati di targa, però, conteranno uptime, consumo reale, diagnostica e capacità di dialogare con il sistema.

La qualità fisica diventa la base di una promessa più ampia. La sua sottolineatura è stata netta: **non basta aumentare l'efficienza nominale; occorre evitare che una tecnologia eccellente venga impiegata male o sovradimensionata.**



La tavola rotonda “Dal Made in Italy al Made by Italy”, organizzata da Automation Technology a SPS Italia 2026, ha riunito imprese ed esperti per discutere il futuro dell'automazione italiana.

«L'efficienza nominale non basta: anche la tecnologia migliore perde valore se viene sovradimensionata o utilizzata lontano dalle condizioni ottimali». **Fabrizio Di Stasio, Bonfiglioli.**

Francesco Renelli ha portato la prospettiva di Comau. Nella robotica il software genera una parte crescente della differenziazione e l'AI entra nel mondo fisico attraverso robot e cobot. La definizione di **"Physical AI"** descrive bene questa convergenza: l'intelligenza artificiale non rimane confinata a un'applicazione, ma percepisce, interpreta e agisce nel processo produttivo. Il valore del robot, quindi, non coincide più soltanto con cinematica, payload e precisione; comprende la capacità di adattarsi al contesto, apprendere dai dati e integrarsi con il flusso operativo.

«Con la Physical AI, robot e cobot diventano la manifestazione concreta di un'intelligenza capace di percepire, interpretare e agire nel processo produttivo». **Francesco Renelli, Comau.**

Stefano Isella ha collegato questa evoluzione alla servitizzazione. Rendere disponibile il dato tramite edge e IoT non è il traguardo: è la condizione per costruire manutenzione predittiva, assistenza remota, continuità operativa e ricavi ricorrenti. Qui la barriera è anche commerciale. **"La rete vendita deve cambiare mindset"**, ha osservato in sostanza Isella: passare dal proporre il "ferro" al vendere il valore di una fabbrica che non si ferma richiede competenze, metriche e incentivi differenti.

«La rete commerciale deve cambiare mentalità: non vendere soltanto il "ferro", ma il valore di una fabbrica connessa che non si ferma». **Stefano Isella, Corvina.**

Il "Made by Italy" non nega il Made in Italy, ma lo estende: dall'eccellenza del singolo prodotto alla responsabilità sul risultato del sistema. Chi controlla piattaforma, modello di ottimizzazione e relazione digitale con l'utilizzatore presidia anche le decisioni; chi resta soltanto fornitore di un componente rischia di diventare un commodity supplier di fascia alta.

La tavola rotonda "Dal Made in Italy al Made by Italy", organizzata da Automation Technology a SPS Italia

2026, ha riunito imprese ed esperti per discutere il futuro dell'automazione italiana.

Efficienza energetica: il limite è nel sistema

La transizione energetica ha reso concreto il ragionamento. Le tecnologie efficienti esistono, gli obiettivi sono definiti e gli strumenti di sostegno non mancano; eppure l'adozione procede più lentamente del necessario. Per Di Stasio il problema si manifesta spesso nel dimensionamento e nell'uso: motori ad alta efficienza possono lavorare lontano dal punto ottimale, vanificando parte del vantaggio. L'efficienza reale non coincide con quella del catalogo.

La risposta passa dalla disponibilità di dati e dalla capacità di orchestrare carichi, ricette e tempi di produzione.

Un proof of concept richiamato nel confronto mostra che pianificare i batch considerando footprint energetico, costo dell'energia e condizioni operative permette di ottimizzare il consumo per unità prodotta, non soltanto quello di una singola apparecchiatura.

Domenico Di Monte, Pneumax, ha spostato il fuoco dal componente all'architettura: **"Non esiste una macchina intelligente senza componenti intelligenti"**. Sensori, attuatori e isole di valvole devono produrre informazioni utili e standardizzate; solo così il livello superiore può decidere. È però vero anche il contrario: componenti intelligenti, lasciati isolati, non rendono intelligente la fabbrica. Servono interoperabilità, semantica comune e una visione di ciclo di vita.

«Non esiste una macchina intelligente senza componenti intelligenti, ma è l'integrazione di sistema a trasformare i dati in efficienza reale». **Domenico Di Monte, Pneumax.**

Da qui il richiamo all'Asset Administration Shell e al Digital Product Passport. Non sono semplici etichette digitali, ma possibili infrastrutture per rendere disponibili dati tecnici, ambientali, manutentivi e di tracciabilità lungo la filiera.

L'efficienza diventa sistemica quando il dato accompagna il prodotto e può essere interpretato da soggetti e piattaforme differenti. In questa prospettiva Transizione 5.0 può essere utile se spinge le imprese a misurare e riprogettare il processo, anziché limitarsi a sostituire asset.

AI industriale: meno integrazione o integrazione più evoluta?

L'arrivo dell'AI solleva una domanda scomoda per il settore: se strumenti più accessibili consentono all'end user di analizzare dati, generare codice e configurare applicazioni, il system integrator perde centralità? Le risposte di Renelli e Cosma Damiano De Angelis hanno indicato una direzione opposta. L'AI può abbassare alcune barriere, ma aumenta il bisogno di chi comprende il processo, seleziona i dati, valida i risultati e collega ambienti eterogenei.

Il system integrator si trasforma così da programmatore specializzato a **"allenatore di dati"** e orchestratore. Deve saper far convivere PLC installati da anni, sensori, edge computing, cloud, modelli di machine learning e vincoli di sicurezza. La competenza verticale sul processo diventa ancora più importante, perché un algoritmo statisticamente efficace può essere industrialmente inutile se non rispetta tempi, qualità, safety e responsabilità operative.

De Angelis ha illustrato il caso di un impianto di frantumazione nel quale un digital twin, alimentato da dati supervisionati, consente di anticipare derive qualitative che le analisi di laboratorio rileverebbero ore dopo. La previsione ravvicinata permette di correggere il processo prima che si accumulino scarti. Il significato competitivo è chiaro: **non basta produrre lo strumento che genera il dato; occorre saper trasformare quel dato in una decisione tempestiva.**

«Non basta produrre lo strumento che genera il dato: il vantaggio competitivo nasce dalla capacità di trasformarlo in una decisione tempestiva». **Cosma Damiano De Angelis, esperto di AI e Big Data.**

Per i fornitori tradizionali la minaccia non è l'AI in sé, ma la possibilità che altri occupino lo spazio fra misura e decisione. Per gli integratori l'opportunità consiste nel combinare conoscenza dell'impianto, qualità del dato e governance del modello. Nelle PMI questo ruolo è ancora più rilevante, perché le competenze non sono sempre presenti all'interno.

Europa: le regole possono diventare infrastruttura competitiva

Il quarto tema ha messo a confronto i modelli globali. Gli Stati Uniti dispongono di capitale, hyperscaler e

piattaforme; la Cina combina scala, velocità di esecuzione e integrazione delle filiere. L'Europa possiede un patrimonio manifatturiero e normativo, ma fatica a tradurlo in un progetto industriale unitario.

Per Di Monte la risposta non può essere l'imitazione. Le filiere europee e italiane possono valorizzare affidabilità, flessibilità, qualità del processo e gestione responsabile del dato. Per funzionare, però, il modello richiede standard condivisi e connessioni digitali fra imprese: la resilienza non nasce dalla somma di molte eccellenze isolate.

Simone Facchinetti ha affrontato la questione dal diritto d'impresa. AI Act, Cyber Resilience Act e disciplina del dato vengono spesso percepiti soltanto come costi. Possono invece diventare una garanzia contrattuale e reputazionale, soprattutto nei mercati ad alta criticità. **La compliance è competitiva quando rende dimostrabili sicurezza, responsabilità e controllo lungo l'intera catena del valore.**

«La compliance diventa competitiva quando consente di dimostrare sicurezza, responsabilità e controllo lungo l'intera catena del valore.» **Simone Facchinetti, avvocato d'impresa.**

Se la complessità regolatoria viene scaricata sulle PMI senza strumenti e competenze, il vantaggio si trasforma in burocrazia. La sfida europea è stabilire regole credibili e renderne possibile l'applicazione industriale: Digital Product Passport, cybersecurity by design e governance dell'AI devono entrare nell'architettura del prodotto, non essere aggiunti alla fine.

PMI: fragilità strutturale, vantaggio adattivo

L'ultima parte del confronto ha riportato il discorso sulla struttura produttiva italiana. Le PMI sono spesso sottocapitalizzate, poco managerializzate e dipendenti da poche figure chiave. Fedele Maniglio ha descritto senza indulgenza il limite dei modelli *"capo-centrici"*, nei quali informazione e decisione rimangono concentrate al vertice. Un'organizzazione simile fatica ad assorbire tecnologie che richiedono dati condivisi, responsabilità distribuite e apprendimento continuo.

«L'AI può ridurre lo svantaggio di scala delle PMI, ma senza una revisione dei processi rischia di accelerare anche inefficienze e disorganizzazione». **Fedele Maniglio, M.ake Global.**

Proprio l'AI, tuttavia, può ridurre lo svantaggio di scala. Strumenti per customer care, controllo di gestione, analisi commerciale, documentazione e supporto tecnico consentono anche a una piccola impresa di costruire capacità un tempo accessibili soltanto alle grandi organizzazioni. Per Maniglio l'opportunità è "democratica", ma non automatica: senza revisione dei processi, l'AI accelera anche inefficienze e confusione. Isella ha sottolineato una crescente apertura delle PMI verso IoT e cybersecurity. Il CRA contribuisce a rendere evidente che connettività e sicurezza non sono opzioni separate: chi immette sul mercato prodotti con elementi digitali deve governarne vulnerabilità, aggiornamenti e ciclo di vita. Questo può premiare le aziende che trasformano tempestivamente l'adempimento in caratteristica del prodotto e in argomento commerciale.

La dimensione ridotta offre velocità, prossimità al cliente e personalizzazione: gli ingredienti della "creatività adattiva" italiana. Per trasformarli in vantaggio sistemico servono reti, competenze condivise e standard. **La PMI non deve diventare una multinazionale in miniatura: deve poter accedere a infrastrutture e conoscenze di livello industriale conservando la propria agilità.**

Il valore è nelle decisioni, ma il prodotto resta la prova

La domanda finale chiedeva di scegliere dove risieda il valore strategico: nel prodotto fisico, nel software o nelle decisioni abilitate dal software. Il confronto ha mostrato che una separazione netta sarebbe artificiale. Senza un prodotto affidabile non c'è dato credibile né azione sicura; senza software il prodotto rimane isolato; senza decisioni migliori, hardware e software non generano un risultato economico.

La gerarchia, però, cambia. Il prodotto è la prova concreta della competenza industriale; il software connette, interpreta e rende scalabile quella competenza; la decisione converte tutto questo in uptime, qualità, energia risparmiata e servizio al cliente. È qui che si concentra il valore più difficile da sostituire.

Il "Made by Italy" non è dunque uno slogan alternativo al Made in Italy. È la proposta di portare l'ingegno italiano dal componente all'architettura, dalla personalizzazione alla piattaforma, dalla vendita alla responsabilità sul risultato. Come ha ricordato Martin nella chiusura, il pericolo maggiore non è che l'Italia non riesca nella

transizione, ma **"che ce la faccia in ordine sparso"**: alcune grandi imprese capaci di scalare, molte PMI eccellenti ma scollegate e, fra loro, uno spazio di integrazione occupato da piattaforme straniere.

La tavola rotonda non ha consegnato una ricetta unica. Ha però indicato quattro condizioni: dati interoperabili, competenze che uniscano processo e digitale, compliance incorporata nella progettazione e collaborazione di filiera. L'automazione italiana continuerà a essere giudicata per ciò che sa costruire. Sempre più spesso, tuttavia, sarà scelta per **ciò che permette al cliente di decidere e ottenere.**

Video integrale della tavola rotonda: <https://youtu.be/gl2D5mqf5eQ>

Keywords: automazione industriale; Made by Italy; SPS Italia 2026; intelligenza artificiale; Physical AI; servitizzazione; efficienza energetica; system integration; Cyber Resilience Act; PMI manifatturiere.



SOLIDS

16 - 17 FEBBRAIO 2028

PARMA

FIERA PER LE TECNOLOGIE DEI GRANULI,
DELLE POLVERI E DEI SOLIDI SFUSI

Dalla movimentazione al controllo di processo: il mondo dei materiali sfusi incontra automazione e digitalizzazione

Esponi tra i professionisti che stanno trasformando gli impianti industriali del **bulk handling** attraverso **IIoT**, **sensoristica intelligente**, **manutenzione predittiva** e **automazione avanzata**



PERCHÉ ESPORRE?

PRESENTA TECNOLOGIE 4.0 IN AZIONE

Mostra dal vivo soluzioni per automazione, IIoT, sensoristica, AI, controllo di processo e manutenzione predittiva: verso l'industria 5.0

RAFFORZA IL TUO POSIZIONAMENTO NEL MERCATO

Posizionati come partner tecnologico strategico per l'evoluzione dell'industria manifatturiera e di processo

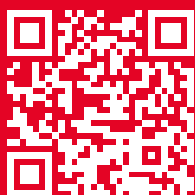


GENERA CONTATTI QUALIFICATI

Incontra responsabili produzione, manutenzione, automazione e progettazione provenienti dai principali settori dell'industria di processo

INTERCETTA PROGETTI DI RETROFIT E SMART FACTORY

Dialoga con aziende che stanno investendo in efficienza, digitalizzazione e upgrade degli impianti industriali



DIVENTA ESPOSITORE

16 e 17 febbraio 2028
Fiere di Parma

Incontra responsabili di stabilimento, progettisti, OEM, system integrator e professionisti dell'industria di processo che visitano SOLIDS Parma per trovare **soluzioni innovative per automazione, movimentazione, dosaggio e trasformazione di polveri, granuli e materiali sfusi.**

LA TOP 20 DELL'AUTOMAZIONE MADE IN ITALY



a cura di Armando Martin

L'ultima edizione dell'Osservatorio ANIE sull'industria italiana dell'Automazione è l'occasione per incrociare lo stato di salute del settore con la consistenza delle aziende del Made in Italy, fino a redigerne una classifica. Le prime venti a matrice italiana, da Bonfiglioli a Reer, compongono una mappa di leadership, specializzazioni e assetti proprietari, con un quarto delle posizioni ormai a controllo estero: un nucleo da oltre 5 miliardi di euro di ricavi aggregati che, allargato a OEM e settori adiacenti, supera i 20 e rappresenta un ecosistema concentrato nel manifatturiero padano, strategico per la competitività nazionale.

SOMMARIO

- Il quadro di sistema
- Perimetro e criteri
- La classifica e le schede

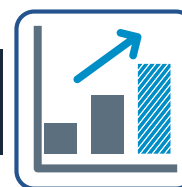
Il quadro di sistema

L'ultimo Osservatorio ANIE fotografa un settore dell'automazione italiana che ha ormai assorbito le anomalie generate dal biennio post-pandemico.

Il 2025 si è chiuso con una crescita del fatturato interno del 3%, a fronte di vendite estere in calo del 3,5%. Il dato aggregato nasconde però dinamiche molto differenziate tra tecnologie e mercati, mentre il sentiment delle imprese resta improntato alla prudenza.

In questo contesto, la classifica delle venti principali aziende italiane dell'Automazione rappresenta una mappa della capacità competitiva nazionale di fronte a quattro grandi trasformazioni: digitalizzazione, cybersecurity, intelligenza artificiale e polarizzazione tecnologica.

I dati ANIE evidenziano infatti una crescita sostenuta del wireless industriale (+36,6%), del networking industriale (+13,7%) e dei sistemi SCADA (+8%), mentre arretrano azionamenti (-3,2%), HMI (-2,6%) e RFID industria-



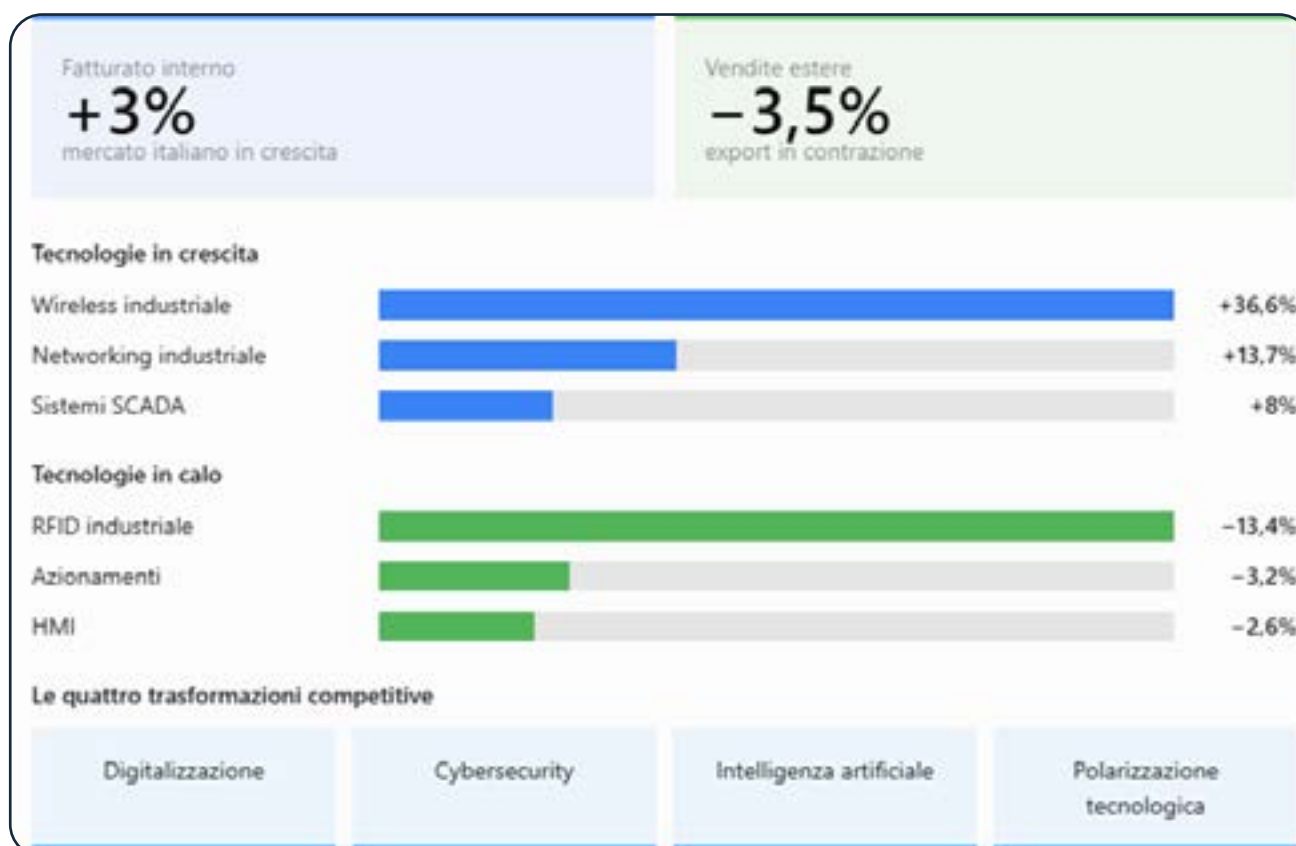
le (-13,4%). Il mercato premia le tecnologie che generano dati, aumentano la connettività e abilitano funzioni avanzate di monitoraggio e controllo. In questo scenario, AI, machine learning ed edge computing stanno progressivamente entrando nelle architetture industriali attraverso applicazioni di manutenzione predittiva, visione artificiale, ottimizzazione energetica e supporto decisionale, rafforzando il valore strategico dei prodotti digitali.

Nella top 20 esposta di seguito questa traiettoria è già prodotta: nei portafogli edge e di visione di Seco, DataLogic, Eurotech ed Exor e, sul fronte degli azionamenti intelligenti, di Bonfiglioli.

Parallelamente, il quadro normativo europeo sta ridefinendo le regole del gioco. NIS2 e Cyber Resilience Act introducono requisiti stringenti di sicurezza *"by design"*, gestione delle vulnerabilità e tracciabilità software. PLC, gateway industriali, sistemi SCADA e software embedded sono stati classificati come prodotti *"importanti"* dal Regolamento di esecuzione (UE) 2025/2392. Per le aziende del settore si tratta al tempo stesso di un costo di conformità e di un'opportunità competitiva sui mercati internazionali.

Anche la geografia industriale mantiene un ruolo centrale. Il Nord Est genera il 47% del fatturato dell'automazione italiana e il Nord Ovest il 37%, concentrando competenze, filiere, clienti e centri di ricerca. Da Bologna a Bergamo, da Brescia a Venezia, la distribuzione delle aziende conferma che l'automazione italiana resta uno dei principali asset tecnologici del manifatturiero padano.

C'è infine il tema degli assetti proprietari. Cinque delle venti aziende in classifica, ovvero Comau, Lafert, Duplomatic, Asem e Carlo Gavazzi, sono ormai a controllo estero. Si tratta di un quarto del campione, passato di mano tra il 2018 e il 2025 verso acquirenti statunitensi, giapponesi e svizzeri. È la doppia faccia dell'attrattività, che da un lato conferma il valore tecnologico della manifattura italiana e dall'altro ne erode il presidio decisionale. La classifica del Made In Italy che segue va quindi letta oltre la dimensione economica. In un mercato che guarda al 2026 con visibilità limitata, la capacità di integrare software, connettività, cybersecurity e intelligenza artificiale sarà sempre più il fattore distintivo della competitività industriale.



Sentiment delle imprese, Fonte: Osservatorio ANIE, dati 2025.

Perimetro e criteri

Il perimetro comprende i costruttori di componenti e sistemi per l'automazione industriale (robotica, azionamenti, pneumatica, sensoristica, sicurezza macchina, embedded computing e software industriale) con baricentro operativo, produttivo e di R&D in Italia, indipendentemente dall'assetto proprietario attuale. I casi di controllo estero sono segnalati con il simbolo *. Sono esclusi gli OEM di macchine automatiche e i player di settori adiacenti, trattati nella sezione finale.

I fatturati sono stime 2025 elaborate su fonti pubbliche, bilanci e dati settoriali, arrotondate e non ufficiali. L'inclusione di aziende attive in segmenti non monitorati direttamente dall'Osservatorio ANIE, come l'embedded computing, risponde al criterio di rilevanza infrastrutturale per la digitalizzazione del manifatturiero.

La classifica e le schede

Più che una graduatoria per fatturato, quella che segue è una fotografia delle competenze tecnologiche che sostengono la competitività del manifatturiero nazionale. Accanto a gruppi storici come Bonfiglioli, Camozzi e Datalogic trovano spazio realtà specializzate nell'IIoT, nell'edge computing e nelle piattaforme digitali, a conferma di una progressiva convergenza tra automazione, software e intelligenza artificiale. Le schede delle singole aziende evidenziano dimensioni, specializzazioni e posizionamento competitivo dei principali protagonisti di un settore sempre più orientato alla connettività, ai dati e alla cybersecurity.

Una nota prima delle schede: con circa 30 milioni di fatturato, Esautomotion (Carpi) occuperebbe la ventesima posizione, e l'esclusione è di quelle che di-

Pos.	Azienda	Specializzazione	M€ (stima 2025)	Sede HQ
1	Bonfiglioli	Riduttori, inverter, servomotori	1 300	Bologna
2	Comau *	Robotica industriale, assemblaggio	1 100	Torino
3	Camozzi Group	Pneumatica, mecatronica, valvole	592	Brescia
4	Datalogic	Visione, identificazione, sensori	575	Bologna
5	Metal Work	Componenti pneumatici	271	Brescia
6	Seco	Embedded computing, IIoT, HMI	198	Arezzo
7	Finder	Relè e componentistica	180	Almese (TO)
8	Lafert Group *	Motori ad alta efficienza	165	San Donà di Piave (VE)
9	Duplomatic MS *	Oleodinamica e controllo	162	Parabiago (MI)
10	Lovato Electric	Elettrotecnica, protezione motori	153	Bergamo
11	Gefran	Sensori, azionamenti, termoregolazione	139	Brescia
12	Pneumax	Pneumatica e manipolazione	130	Bergamo
13	Motovario	Riduttori, motoriduttori, variatori	100	Formigine (MO)
14	Asem *	PC industriali, HMI, gateway IoT	72	Artegnà (UD)
15	Pizzato Elettrica	Dispositivi di sicurezza, finecorsa	65	Marostica (VI)
16	Eurotech	Edge computing, IIoT, embedded	58	Amaro (UD)
17	Exor International	HMI, IIoT, Corvina OS	58	Verona
18	Carlo Gavazzi Controls *	Componenti e monitoraggio	54	Milano
19	ETA	Carpenteria per quadri di automazione	48	Canzo (CO)
20	Reer	Sicurezza macchine	37	Torino

Tabella 1 - Costruttori italiani di automazione in ordine di fatturato.

spiacciono dal momento che i suoi CNC restano l'unica alternativa italiana tecnologicamente credibile in un segmento dominato da Fanuc, Mitsubishi Electric, Siemens e Bosch Rexroth.

1. Bonfiglioli — Riduttori, inverter, servomotori | ~1 300 M€

Bonfiglioli è il più grande player italiano dell'automazione industriale in senso stretto, con un portafoglio che copre riduttori per ogni applicazione, azionamenti a frequenza variabile e servomotori. La sua architettura industriale è integrata verticalmente e distribuita globalmente, con oltre 80 stabilimenti e uffici in più di 50 paesi. Il fatturato stimato per il 2025, intorno a 1,3 miliardi di euro, la posiziona nettamente sopra qualsiasi concorrente domestico. Il focus strategico degli ultimi anni su efficienza energetica, integrazione con bus di campo aperti, soluzioni per rinnovabili e material handling ne rispecchia il posizionamento nel segmento a maggiore crescita strutturale. L'Osservatorio ANIE segnala che il gruppo dei riduttori chiude il 2025 con un +3,9% interno: un risultato in linea con il momentum di Bonfiglioli.

2. Comau * — Robotica industriale, linee di assemblaggio | ~1 100 M€

Comau è un caso inevitabile in qualsiasi classifica sull'automazione italiana, ma l'asterisco è obbligatorio: da gennaio 2025 la maggioranza è detenuta da One Equity Partners, fondo statunitense di private equity che ha rilevato la quota di controllo da Stellantis (rimasta azionista di 'minoranza attiva'). Operativamente l'azienda resta italiana con sede a Torino, R&D e manifattura concentrate nel Paese, ma il controllo proprietario è a New York. Il core è la robotica industriale pesante e l'ingegneria di sistemi per l'assemblaggio automotive e non. Il fatturato stimato attorno a 1,1 miliardi di euro la colloca al secondo posto, e la transizione strategica in corso verso applicazioni collaborative, wearable robotics e soluzioni per l'elettificazione dei veicoli ne fa uno degli hub tecnologici più interessanti del manifatturiero europeo.

3. Camozzi Group — Pneumatica, mecatronica, valvole | ~592 M€

Pneumatica, mecatronica, valvole: nessun gruppo italiano del settore ha la taglia di Camozzi, né una diversificazione che abbraccia componenti per macchine tessili, automazione medica e strumentazione scientifica.

La struttura multi-divisionale (Automation, Machine Tools, Digital Health) le conferisce una resilienza settoriale che poche aziende della stessa taglia possono vantare. Il dato di fatturato di circa 592 milioni è solido, ma la vera cifra distintiva è la profondità di integrazione verticale: Camozzi progetta e produce internamente cilindri, valvole, sensori e attuatori, controllando la catena del valore in modo raro nel panorama italiano.

4. Datalogic — Sensori, visione artificiale, laser industriale | ~575 M€

Datalogic, come altre 3 aziende di questa lista, è quotata in Borsa (Euronext Milan), il che le conferisce una trasparenza contabile non comune nel comparto. Il suo posizionamento nella sensoristica industriale, nei sistemi di visione e nelle soluzioni per l'identificazione automatica (lettura codici, RFID) la mette al crocevia di due delle tendenze più robuste nell'automazione: l'ascesa del machine vision e la crescita della logistica automatizzata. I dati ANIE indicano che i sistemi di visione sono tra i segmenti in crescita strutturale, trainati dall'e-commerce e dalla qualità di processo. Datalogic presidia questo spazio con una presenza commerciale in oltre 100 paesi.

5. Metal Work — Componenti pneumatici industriali | ~271 M€

Brescia, impresa familiare, quasi completamente orientata all'export. Metal Work è uno dei casi più interessanti di specializzazione stretta ed efficace nel panorama dell'automazione italiana: produce esclusivamente componenti pneumatici (valvole, cilindri, isole di valvole, raccorderia) e li vende attraverso una rete distributiva capillare in Europa e Asia. Con circa 271 milioni di fatturato e una forza lavoro di oltre 1 500 persone, dimostra che la focalizzazione tecnologica non è un limite ma una leva competitiva quando accompagnata da qualità di prodotto elevata e reattività al mercato.

6. Seco — Embedded computing, IoT industriale, HMI | ~198 M€

Seco è la realtà italiana di riferimento nell'embedded computing industriale, segmento che l'Osservatorio ANIE non segue direttamente ma infrastrutturale per la digitalizzazione del manifatturiero. Il suo portafoglio spazia dai moduli COM (Computer-on-Module) ai gateway IIoT, dalle HMI ruggedizzate alle piattaforme edge per applicazioni AI embedded. Con circa 198

milioni di fatturato e una struttura R&D significativa, Seco è uno dei pochi player italiani che competono direttamente con i grandi nomi del computing industriale globale. L'azienda ha rafforzato negli ultimi anni la componente software e di connectivity management, un'evoluzione che sposta una quota crescente dei ricavi su software e servizi ricorrenti.

7. Finder – Relè, temporizzatori, componentistica | ~180 M€

Finder è il caso paradigmatico dell'azienda italiana di componentistica elettrica che ha costruito un brand globale su un prodotto apparentemente semplice. I relè Finder sono presenti in quadri elettrici di tutto il mondo, distribuiti attraverso una rete capillare che copre oltre 80 paesi. Con circa 180 milioni di fatturato, l'azienda fa della penetrazione di mercato e della riconoscibilità presso i progettisti di impianti i suoi punti di forza fuori dal comune. Il segmento dei relè non è tra quelli a più alto tasso di crescita secondo ANIE, ma la solidità e la marginalità di un brand dominante compensano ampiamente la maturità del prodotto.

8. Lafert Group * – Motori elettrici ad alta efficienza | ~165 M€

Lafert è parte di Sumitomo Heavy Industries dal 2018: proprietà giapponese, sede e produzione principale a San Donà di Piave (Venezia), con sei siti produttivi tra Italia, Slovenia e Cina. L'asterisco segnala un cambio di controllo consolidato da anni ma spesso sottovalutato nel dibattito sulla manifattura italiana. Il focus sui motori ad alta efficienza energetica (IE3, IE4, IE5) la posiziona favorevolmente rispetto alle pressioni regolamentari europee che spingono verso la sostituzione del parco motori installato. Il 2025 ha tuttavia portato tensioni industriali significative come la chiusura dello stabilimento di Fusignano. È stato tuttavia attivato un piano industriale 2025-2028 che punta a una crescita del fatturato a doppia cifra entro il 2028, basata sull'integrazione motore-drive e sullo sviluppo di soluzioni più intelligenti per l'automazione industriale.

9. Duplomatic MS * – Oleodinamica e sistemi di controllo | ~162 M€

Duplomatic Motion Solutions è parte di Daikin Industries Ltd. (Giappone) dal luglio 2022, ennesimo caso di brand industriale italiano a controllo extraeuropeo, con sede

e produzione principale a Parabiago (Milano). Il core è nelle valvole proporzionali e servovalvole - componenti ad alta precisione con applicazioni in presse industriali, macchine per lavorazione dei metalli e veicoli speciali - completato dai brand Hydreco (applicazioni mobili) e Continental Hydraulics (Nord America). Con circa 162 milioni di fatturato, Duplomatic presidia una nicchia tecnologica che genera margini e barriere all'ingresso significative. L'appartenenza a un gruppo globale come Daikin le garantisce accesso a risorse R&D e mercati difficilmente raggiungibili come azienda indipendente.

10. Lovato Electric – Elettrotecnica e protezione motori | ~153 M€

Lovato Electric, azienda con oltre 100 anni di storia, produce componenti elettrotecnici per la protezione e il controllo dei motori (interruttori, contattori, relè termici, avviatori) con una presenza commerciale in oltre 80 paesi. Con circa 153 milioni di fatturato è un player mid-size nella sua categoria, ma la profondità di gamma e la capacità di risposta al mercato ne fanno un riferimento per i progettisti di quadri elettrici industriali. La dinamica del settore, forte della sostituzione del parco installato per conformità alle normative sull'efficienza e la sicurezza macchine, mantiene una domanda strutturale che sostiene il business.

11. Gefran – Sensori, azionamenti, termoregolatori | ~139 M€

Anche Gefran, azienda bresciana a controllo familiare, è quotata in Borsa (Euronext Milan), con gli obblighi informativi che ne fanno una delle realtà più leggibili del mid-size di settore. Il suo portafoglio è trasversale ma coerente: sensori di posizione e pressione, azionamenti per macchine plastiche e presse, sistemi di termoregolazione per processi industriali. Con circa 139 milioni di fatturato e forte orientamento all'export, opera in un perimetro tecnologico in cui la componente di automazione di processo e di misura industriale si sovrappone con il segmento dei sensori intelligenti (uno dei più dinamici secondo i dati ANIE). I costruttori di macchine per materie plastiche sono tra i clienti finali con domanda più regolare.

12. Pneumax – Componenti pneumatici e manipolazione | ~130 M€

Pneumax è un player internazionale della pneumatica industriale con base a Bergamo con un posizionamento

complementare a Metal Work: valvole, cilindri, isole di valvole, sistemi di manipolazione e soluzioni integrate per l'automazione delle macchine. Controllo familiare, forte presenza commerciale diretta in Europa con filiali proprie. La capacità di coniugare presenza sul mercato, visibilità del brand e contributo al confronto sui temi dell'innovazione industriale evidenzia un posizionamento attivo nella comunicazione di settore, oltre che nel presidio tecnologico. Con circa 130 milioni di fatturato è tra le aziende della classifica con il miglior equilibrio tra dimensione e profondità di specializzazione.

13. Motovario – Riduttori, motoriduttori, variatori | ~100 M€

Motovario progetta e produce riduttori, motoriduttori e variatori di velocità per applicazioni industriali che spaziano dal material handling al packaging, dalle macchine alimentari agli impianti di sollevamento. L'andamento del fatturato (circa 100 milioni) rispecchia fedelmente la dinamica del segmento: i riduttori industriali hanno subito nel 2024 una contrazione significativa legata al rallentamento degli investimenti in macchinari industriali, prima di recuperare parzialmente nel 2025. Il confronto con Bonfiglioli che produce riduttori per un mercato parzialmente sovrapponibile è inevitabile, ma i posizionamenti sono distinti: Bonfiglioli presidia la fascia alta con integrazione drive e servosistemi, Motovario compete sulla fascia mid-range con profondità di gamma e capillarità distributiva in Europa.

14. Asem ✱ – PC industriali, HMI, gateway IoT | ~72 M€

Asem è il riferimento italiano nel segmento dei PC industriali e delle HMI *rugged* per il mercato OEM, ma dal 2020 fa parte di Rockwell Automation (NYSE: ROK). La famiglia fondatrice Guerra ha ceduto la totalità delle quote alla multinazionale statunitense, che ha integrato Asem nella divisione Architecture & Software. Operativamente l'azienda resta friulana con sede ad Arterga (Udine), R&D e produzione nel sito originario, ma il controllo proprietario è a Milwaukee. L'acquisizione è stata strategica per Rockwell, che ha individuato in Asem *"il fornitore ideale per i costruttori di macchine europei che operano nel mercato nordamericano"*: una validazione che conferma il posizionamento tecnologico dell'azienda ben oltre le sue dimensioni. Il business è principalmente orientato agli OEM, che richiedono

personalizzazione hardware, supporto tecnico prolungato e cicli di vita misurati in anni. La componente gateway IoT è in crescita, coerentemente con la direzione del mercato indicata dall'Osservatorio ANIE.

15. Pizzato Elettrica – Dispositivi di sicurezza e finecorsa | ~65 M€

Marostica (Vicenza), controllo familiare, zero debito bancario, 370 dipendenti circa e una marginalità tra le più alte dell'intera classifica. Pizzato Elettrica progetta e produce interruttori di posizione, dispositivi di sicurezza per ripari mobili, interruttori a fune, moduli e sensori di sicurezza, con un'integrazione verticale quasi totale nel sito vicentino che va dallo stampaggio delle materie plastiche alla tranciatura dei contatti. Dopo il picco 2022-2023 oltre i 73 milioni, il fatturato si è assestato su livelli stimabili intorno ai 65 milioni, in un mercato della componentistica di sicurezza meno ciclico della media. Con Reer compone il presidio italiano nella machine safety, confrontandosi con Schmersal, Euchner e Pilz su un terreno dove certificazioni e norme di sicurezza funzionale costituiscono barriere all'ingresso strutturali.

16. Eurotech – Edge computing, IIoT, embedded | ~58 M€

Eurotech è il caso più puro di azienda italiana nell'edge computing industriale. Quotata in Borsa (Euronext Milan), con sede ad Amaro (Udine), sviluppa piattaforme hardware e software per l'IIoT con un approccio che integra moduli embedded, gateway e middleware (Everyware Software Framework, basato su OSGi). Con circa 58 milioni di fatturato è tra le più piccole aziende quotate della classifica, ma il suo posizionamento in un segmento ad alta crescita strutturale come quello di edge AI, connected devices e digital twin infrastrutture ne giustifica la presenza. I dati ANIE sul wireless industriale (+36,6%) e sul networking (+13,7%) indicano esattamente la direzione in cui Eurotech è posizionata.

17. Exor International – HMI, IIoT, PC industriali (Corvina OS) | ~58 M€

Exor International (San Giovanni Lupatoto, Verona) è uno dei player italiani più interessanti nella convergenza OT/IT: la sua piattaforma Corvina è un sistema operativo industriale aperto che consente la gestione remota di dispositivi edge, la raccolta dati e l'integra-

zione cloud in ambienti di automazione eterogenei. Azienda indipendente a controllo italiano fondata nel 1971, Exor International è stabilmente focalizzata su HMI, IPC e gateway industriali con R&D e produzione concentrate in Italia. Con circa 58 milioni di fatturato e 150 dipendenti distribuiti tra Italia, Germania, USA e India, la differenziazione competitiva risiede nella piattaforma software e nell'ecosistema di connessione: un posizionamento che la avvicina alla logica delle più evolute piattaforme IIoT.

18. Carlo Gavazzi Controls * — Componenti elettronici e monitoraggio | ~54 M€

Carlo Gavazzi è tecnicamente un'azienda di origine italiana fondata a Milano nel 1931, seppure sotto controllo svizzero (Carlo Gavazzi Holding AG, quotata alla Borsa svizzera). La collocazione in classifica riflette la continuità del brand, della base produttiva e della rete commerciale in Italia, ma l'asterisco è formalmente appropriato per l'assetto proprietario. Il portafoglio copre relè a stato solido, sensori di prossimità e fotoelettrici, sistemi di monitoraggio energetico e componenti per building automation. Parliamo di tecnologie mature con applicazioni crescenti nell'ambito dell'efficienza energetica e della smart factory. Con circa 54 milioni di fatturato è un player di nicchia con forte riconoscibilità di brand.

19. ETA — Carpenteria per quadri e automazione | ~48 M€

ETA è un caso di eccellenza italiana in un segmento poco visibile. Con sede a Canzo (Como) e circa 48 milioni di fatturato, produce *enclosure*, accessori e sistemi di cablaggio per quadristi e sistemisti di automazione. La domanda è direttamente correlata all'attività di installazione e manutenzione degli impianti industriali, un mercato che l'Osservatorio ANIE non segue come voce separata ma che è infrastrutturale per tutto il comparto. La concorrenza principale è Rittal (Friedhelm Loh Group, Germania) e Schneider Electric, che operano su scala globale. ETA compete sulla flessibilità e sulla prossimità al mercato italiano e centro-europeo.

20. Reer — Sensori e barriere di sicurezza industriale | ~37 M€

Reer (Torino) è il principale produttore italiano di dispositivi di sicurezza per macchine e impianti industriali:

barriere fotoelettriche di sicurezza, scanner laser, sensori di sicurezza, controllori logici di sicurezza. Con Pizzato Elettrica forma il presidio domestico che compete direttamente con i grandi nomi globali della machine safety (Sick, Pilz, Schmersal, Rockwell). Con circa 37 milioni di fatturato ha dimensioni contenute rispetto ai leader internazionali, ma il suo posizionamento in un segmento iper-regolamentato, dove la Machinery Regulation UE 2023/1230 (applicabile da gennaio 2027) e le norme di sicurezza funzionale (IEC 62061, ISO 13849) costituiscono barriere all'ingresso reali, le garantisce una base clienti fidelizzata e margini difendibili.

* *Proprietà non più a maggioranza italiana: Comau (One Equity Partners, USA, da gennaio 2025), Lafert Group (Sumitomo Heavy Industries, Giappone, dal 2018), Duplomatic MS (Daikin Industries, Giappone, dal luglio 2022), Asem (Rockwell Automation, USA, dal 2020). Per Carlo Gavazzi Controls il controllo è svizzero (Carlo Gavazzi Holding AG) pur con origine e operatività prevalentemente italiana.*

Keywords: automazione industriale, Made in Italy, industria italiana, classifica aziende, mercato dell'automazione, Osservatorio ANIE, robotica industriale, componenti per automazione, IIoT, edge computing, cybersecurity industriale, manifattura italiana.



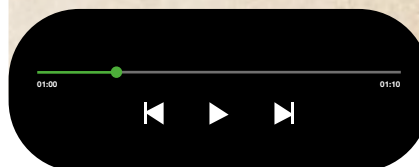
Editoriale Delfino

Editoriale Delfino sbarca su Spotify

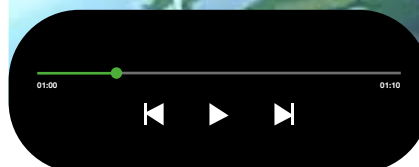


**Cerca
Editoriale Delfino
su Spotify e
troverai tutti
i nostri Podcast**

Editoriale Delfino Srl
Via Aurelio Saffi 9
20123 Milano (MI)
Tel 02 9578.4238
info@editorialedelfino.it
editorialedelfino.it



**Physicist
sans
Frontières**



CRA, DALL'11 SETTEMBRE LA CYBER-RESILIENZA DIVENTA OPERATIVA

Il Cyber Resilience Act entra nella sua prima fase realmente operativa. Dall'11 settembre i fabbricanti dovranno notificare vulnerabilità attivamente sfruttate e incidenti gravi che interessano i prodotti con elementi digitali. Per l'automazione industriale significa organizzare subito vulnerability management, patching, tracciabilità delle versioni e rapporti con clienti e fornitori. CRA e NIS2 costruiscono così un ponte fra chi realizza il prodotto e chi lo utilizza negli impianti, mentre IEC 62443 offre già gran parte del metodo necessario per trasformare la conformità in processo industriale.



a cura della Redazione

SOMMARIO

- La regola delle 24 e 72 ore
- Una sola piattaforma, molte funzioni aziendali
- Il nodo dell'OT: prodotti che vivono per anni
- I dati ENISA: il patching è già il collo di bottiglia
- CRA, NIS2 e IEC 62443: tre livelli che convergono
- Il vantaggio di chi parte da IEC 62443
- Dalla SBOM al PSIRT
- Sette azioni prima dell'11 settembre
- La compliance diventa una caratteristica del prodotto

L' 11 settembre 2026 non è il "giorno zero" dell'intero Cyber Resilience Act, ma è la prima data che porta obblighi operativi direttamente dentro le aziende. Il Regolamento (UE) 2024/2847 è entrato in vigore il 10 dicembre 2024 e sarà pienamente applicabile dall'11 dicembre 2027. Alcune disposizioni sono però anticipate: dall'11 giugno 2026 quelle sugli organismi di valutazione della conformità e dall'11 settembre l'articolo 14 sul reporting.

La differenza è sostanziale. Il fabbricante non deve ancora dimostrare l'intera conformità del prodotto ai requisiti essenziali del CRA, ma deve già essere capace di riconoscere un evento rilevante, classificarlo, identificare prodotti e versioni coinvolte e comunicarlo entro finestre temporali strette. Gli obblighi di reporting riguardano inoltre anche i prodotti con elementi digitali già immessi sul mercato prima dell'11 dicembre 2027, se rientrano nel campo di applicazione del regolamento.



CRA: le scadenze che contano per l'automazione

Dal reporting 2026 alla piena applicazione 2027



IL CRONOMETRO DEL REPORTING

24 ORE

Early warning

72 ORE

Notifica completa

FINALE

14 giorni dalla misura correttiva
(vulnerabilità) / 1 mese (incidenti)

Fonte: Commissione europea, ENISA, Regolamento (UE) 2024/2847 — Art. 14 e calendario di attuazione.

Figura 1 – Le principali scadenze del Cyber Resilience Act.

La regola delle 24 e 72 ore

Non tutte le vulnerabilità devono essere notificate. Il CRA parla di **actively exploited vulnerability**, cioè una vulnerabilità per la quale esiste evidenza affidabile che un attore malevolo l'abbia effettivamente sfruttata senza autorizzazione. Analogamente, un incidente è grave quando compromette o può compromettere disponibilità, autenticità, integrità o riservatezza di dati e funzioni importanti, oppure può portare all'introduzione o all'esecuzione di codice malevolo nel prodotto o nei sistemi dell'utilizzatore.

Per un costruttore di automazione la distinzione è decisiva. Una CVE pubblicata su una libreria presente in un gateway industriale non genera automaticamente una notifica. Ma se esistono evidenze di sfruttamento reale e quella componente è presente in prodotti commercializzati nell'UE, il cronometro può partire. Il regolamento cita anche il caso di codice malevolo introdotto nel canale di rilascio degli aggiornamen-

ti come esempio di incidente potenzialmente grave: esattamente uno degli scenari più temuti nella supply chain software.

Una sola piattaforma, molte funzioni aziendali

Le segnalazioni passeranno attraverso la **Single Reporting Platform (SRP)** istituita e gestita da ENISA. Il fabbricante effettua una sola notifica tramite l'endpoint del CSIRT coordinatore dello Stato membro in cui ha il proprio stabilimento principale nell'Unione; salvo casi eccezionali, le informazioni sono accessibili anche a ENISA e possono essere inoltrate agli altri CSIRT interessati. La piattaforma semplifica il canale amministrativo, non il lavoro interno. Per rispettare le 24 ore bisogna sapere chi riceve la segnalazione, chi verifica l'exploit, chi identifica firmware e software coinvolti e chi autorizza la comunicazione. Il reporting CRA coinvolge quindi R&D, cybersecurity, qualità, assistenza, supply chain e direzione.

Termine	Adempimento	Contenuto
24 ore	Early warning	Prima segnalazione e, se noto, Stati membri interessati
72 ore	Notifica completa	Prodotto, natura dell'exploit/incidente, valutazione iniziale e mitigazioni
Report finale	Chiusura	14 giorni dalla misura correttiva per vulnerabilità; un mese per incidenti gravi

Tabella 1 - Tempi e fasi di segnalazione previsti dal CRA.

Il nodo dell'OT: prodotti che vivono per anni

Il CRA riconosce espressamente che i prodotti destinati ad ambienti industriali, come i sistemi di controllo, possono restare in uso molto più a lungo dei normali prodotti ICT. Quando dal dicembre 2027 entreranno pienamente in applicazione i requisiti essenziali, il **support period** dovrà riflettere il periodo nel quale il prodotto è ragionevolmente atteso in uso e, salvo prodotti con vita inferiore, non potrà essere inferiore a cinque anni. Se l'uso previsto è più lungo, anche il supporto dovrà esserlo.

È un cambio di paradigma per un settore nel quale PLC, RTU, HMI, controllori e gateway possono rimanere installati per dieci o quindici anni.

Gli aggiornamenti automatici possono inoltre essere inadatti in reti critiche e industriali, dove un update non pianificato può interferire con la produzione. Il patching deve quindi diventare un processo governato: conoscere le versioni vulnerabili, predisporre patch o mitigazioni e comunicarle agli utilizzatori.

I dati ENISA: il patching è già il collo di bottiglia

Nel **NIS Investments 2025**, basato su 1.080 organizzazioni europee, ENISA indica il patching come area problematica per il **50%** degli intervistati; seguono business continuity al **49%** e gestione del rischio di supply chain al **37%**. Il **28%** impiega oltre tre mesi per correggere vulnerabilità critiche e circa il **30%** non ha effettuato un assessment di cybersecurity nei dodici mesi precedenti. Fra i rischi futuri, ransomware e attacchi alla supply chain sono citati rispettivamente dal **55%** e dal **47%** delle organizzazioni.

Anche la preparazione delle PMI mostra un divario rilevante. In un'indagine ENISA del 2026 su 194 organizzazioni di 31 Paesi, il **66%** aveva già sentito parlare del CRA, ma incident response e product life-cycle management risultano le aree meno mature, soprattutto nelle microimprese. Oltre il **70%** chiede template pratici per documentazione tecnica e sviluppo sicuro.

Per molte imprese dell'automazione il problema non è dunque conoscere la norma, ma costruire un proces-

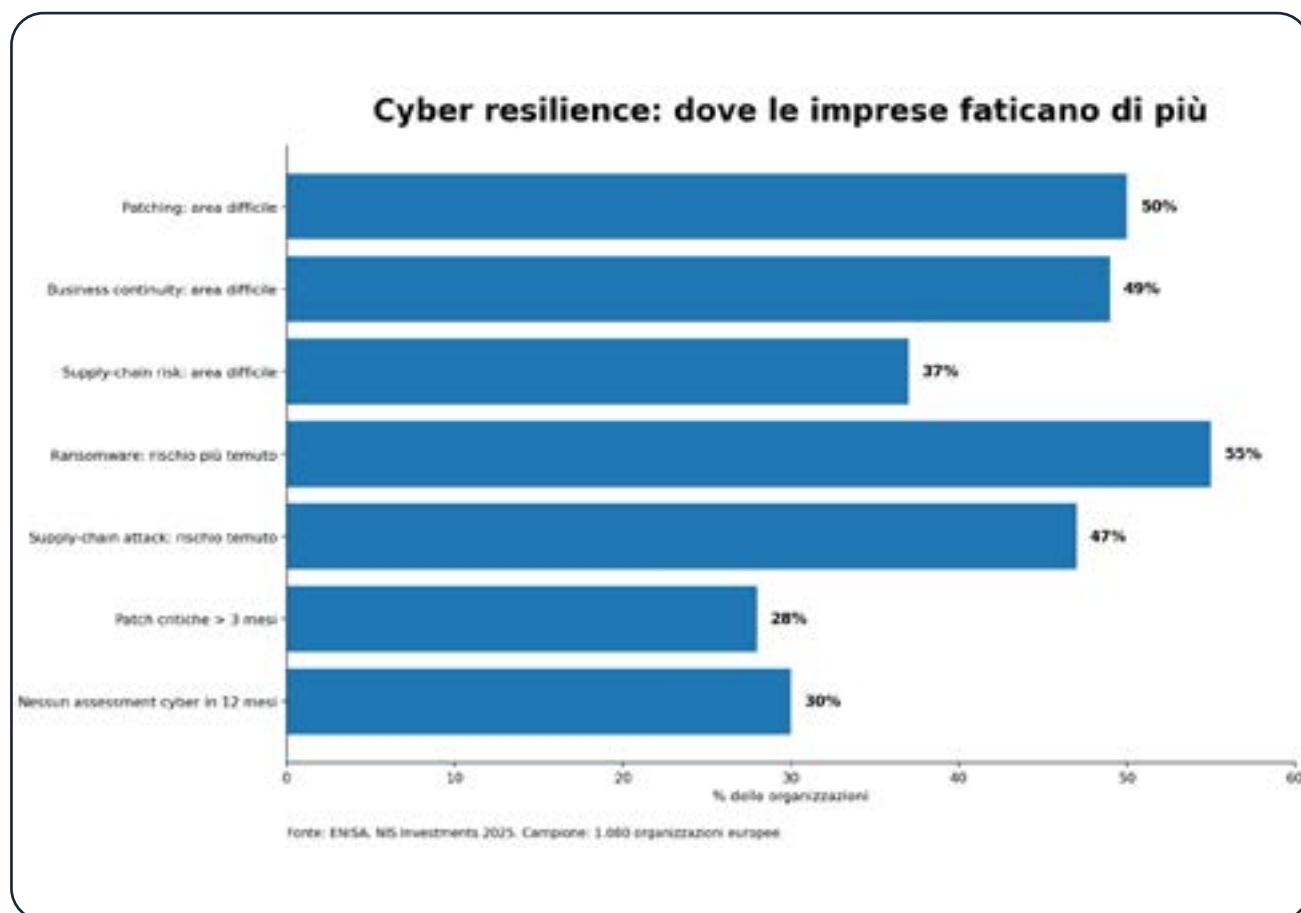


Figura 2 – Principali criticità e rischi di cyber resilience secondo ENISA.

Tema	CRA	NIS2 / IEC 62443
Focus	Prodotto con elementi digitali	Organizzazione, sistema e ciclo di sviluppo
Sicurezza	Secure by design e lifecycle	Risk management, zone/conduit, secure development
Vulnerabilità	Gestione e reporting	Patching, incident response, defect management
Supply chain	Componenti e dipendenze	Rischio fornitori e requisiti contrattuali
Evidenze	Documentazione, versioni, SBOM	Tracciabilità e processi verificabili

Tabella 2 – Confronto tra CRA, NIS2 e IEC 62443 su sicurezza, vulnerabilità, supply chain ed evidenze.

so ripetibile che funzioni con poche persone e sotto pressione.

CRA, NIS2 e IEC 62443: tre livelli che convergono

Il CRA guarda soprattutto al **prodotto** e responsabilizza il fabbricante; la NIS2 guarda all'**organizzazione utilizzatrice** e alla sua capacità di gestire rischio, continuità, supply chain e incidenti. IEC 62443 offre invece il riferimento tecnico-organizzativo più vicino al mondo OT.

Nell'OT questi livelli non possono essere separati. Una stessa vulnerabilità può avere impatto modesto su una macchina isolata e critico se il dispositivo è installato in un acquedotto, in una rete energetica o su una linea con accesso remoto.

È il **product security context** discusso anche all'ISA OT Cybersecurity Summit 2026: il fabbricante deve spiegare condizioni d'uso e rischi residui; l'asset owner deve comprendere configurazioni, mitigazioni ed effetti sul processo.

Ne deriva una conseguenza commerciale: nei capitoli cresceranno clausole su tempi di notifica, patch, fine supporto, SBOM, accesso remoto e canali di escalation. La domanda non sarà più soltanto "**il prodotto è conforme?**", ma "**come reagisce il fornitore quando emerge una vulnerabilità critica?**".

Il vantaggio di chi parte da IEC 62443

IEC 62443 non equivale automaticamente alla conformità CRA e le norme armonizzate europee che potranno fornire presunzione di conformità sono ancora in completamento. Tuttavia, chi ha già lavorato secondo **IEC 62443-4-1** e **62443-4-2** parte da una posizione favorevole.

La 62443-4-1 struttura il secure product development lifecycle: requisiti di sicurezza, threat modeling, progettazione, verifica, gestione delle vulnerabilità, aggiornamenti e fine vita. La 62443-4-2 traduce la sicurezza in requisiti tecnici di componente: identificazione e autenticazione, controllo accessi, integrità, riservatezza, restrizione dei flussi, risposta agli eventi e disponibilità.

Il vero vantaggio non è quindi avere un certificato da esibire, ma possedere già ruoli, evidenze e processi utilizzabili quando scatta la finestra delle 24 ore. È lo stesso messaggio emerso al summit ISA: chi ha già adottato IEC 62443-4-1/-4-2 è meglio posizionato nel percorso verso il CRA, pur senza poter considerare lo standard una scorciatoia automatica alla conformità.

Dalla SBOM al PSIRT

Nel percorso verso il 2027 acquisterà un ruolo centrale la **Software Bill of Materials**. Il CRA richiede di identificare e documentare i componenti del prodotto e le dipendenze; ENISA rileva che il regolamento sta già accelerando l'adozione delle SBOM e la loro integrazione nel software development life cycle.

Una SBOM, però, serve solo se è collegata a versioni e prodotti. Quando emerge una vulnerabilità in Linux, OpenSSL o in una libreria di terze parti, il costruttore deve poter rispondere rapidamente: dove è presente? In quali release? Quali clienti possono essere coinvolti? Esiste evidenza di sfruttamento attivo?

Lo stesso vale per il **PSIRT**, Product Security Incident Response Team. In una PMI può essere una funzione virtuale formata da R&D, qualità, IT, assistenza e management. Ciò che conta sono ownership, criteri di escalation, reperibilità e autorità decisionale.

Sette azioni prima dell'11 settembre

A poche settimane dalla scadenza l'obiettivo realistico non è completare l'intero percorso CRA 2027, ma rendere operativo il reporting:

1. definire il perimetro dei prodotti con elementi digitali venduti nell'UE, comprese le famiglie legacy;
2. nominare il responsabile CRA reporting e il nucleo PSIRT;
3. stabilire criteri per distinguere vulnerabilità nota, exploit attivo e incidente grave;
4. mappare versioni e dipendenze software, usando dove possibile SBOM machine-readable;
5. predisporre un playbook 24/72 ore con template, escalation e sostituti;
6. verificare i canali con distributori, integratori e clienti;
7. simulare almeno un incidente prima della scadenza.

Il test può essere semplice: exploit attivo su una libreria presente in un gateway venduto in più Stati UE. In poche ore l'azienda dovrebbe identificare prodotti e release coinvolte, preservare le evidenze e classificare l'evento; entro la giornata preparare l'early warning; entro 72 ore produrre una valutazione tecnica e indicare mitigazioni. Se il processo si blocca perché manca l'elenco delle versioni o non è chiaro chi autorizza la notifica, il gap è già stato trovato.

La compliance diventa una caratteristica del prodotto

L'11 settembre segna qualcosa di più di una nuova comunicazione obbligatoria. Per la prima volta il CRA rende misurabile la capacità del costruttore di reagire a un problema di sicurezza dopo la vendita. Il prodotto non termina più al collaudo o alla consegna: continua a esistere digitalmente attraverso firmware, librerie, vulnerabilità e aggiornamenti.

È qui che il CRA può diventare una leva competitiva per l'automazione europea. Chi saprà dimostrare tempi di risposta brevi, trasparenza sulle vulnerabilità, supporto lungo il ciclo di vita e processi coerenti con IEC 62443 potrà trasformare la compliance in valore industriale.

Nel nuovo mercato dell'automazione non si venderanno soltanto prestazioni, precisione e connettività: si venderà anche la capacità di restare sicuri quando una nuova vulnerabilità verrà scoperta dopo la messa in servizio.

Keywords: *Cyber Resilience Act, CRA, industrial cybersecurity, OT cybersecurity, industrial automation, vulnerability management, vulnerability disclosure, incident reporting, active exploitation, PSIRT, SBOM, IEC 62443, NIS2, secure by design, product security, patch management, software supply chain, industrial control systems, PLC security, cyber resilience.*



**ASSOCIAZIONE ITALIANA
STRUMENTISTI**

CHI SIAMO

AIS - Associazione Italiana Strumentisti è un'associazione senza fini di lucro e si propone la diffusione e il perfezionamento di informazioni relative alla teoria, progetto, costruzione ed impiego degli strumenti di misura e di controllo in uso nella scienza e nella tecnica in Italia.

SERVIZI

- Giornate di Studio e Tavole Rotonde su argomenti tecnici specifici, con minimostre.
- Corsi per giovani Strumentisti
- Seminari di Aggiornamento.
- Promozione di Comitati di Studio.
- Divulgazione di memorie e pubblicazioni scientifiche.
- Attività culturali e gite con visita ad impianti industriali
- Indice merceologico con Suppli
- Assistenza legale Studio Facchinetti

VANTAGGI

- Essere sempre aggiornati sugli argomenti più importanti e innovativi.
- Avere un collegamento diretto con professionisti che operano nel settore
- Essere parte di una rete composta che include società di produzione, fornitori e società di progettazione
- Ricevere le pubblicazioni tecniche "Automation Technology" "Automazione e Strumentazione"

ISCRIZIONI E QUOTE

Ci si iscrive come Socio Individuale (Persona) o come Socio Collettivo (Società)

L'iscrizione si effettua versando la quota associativa e compilando ed inviando il Modulo Raccolta Dati

QUOTE ANNUALI

Socio Individuale € 75,00

Socio Studente € 10,00

Socio Collettivo

quota annuale per ditte individuali o con capitale sociale fino a € 51.000,00 con possibilità di iscrivere fino a 3 nominativi: € 300,00
quota annuale per ditte con capitale sociale oltre € 51.000,00 con possibilità di iscrivere fino a 5 nominativi: € 500,00.

Le quote associative potranno essere versate:

- direttamente presso la sede dell'Associazione, con assegno bancario intestato ad A.I.S. Associazione Italiana Strumentisti
- con bonifico bancario su INTESA SANPAOLO, Milano | IBAN IT55 0030 6909 6061 0000 0119 766
- oppure presso la segreteria delle Delegazioni Zonali.

Si aggiunge l'opportunità per i soci collettivi di far partecipare alle iniziative dell'Associazione qualsiasi dipendente con la sola aggiunta di 100,00 Euro/anno (senza il pagamento della quota associativa individuale per il dipendente non compreso nei tre/cinque nomi indicati all'inizio dell'anno in caso di partecipazione alle nostre iniziative).

L'associazione si rinnova annualmente e ha validità per l'anno solare in corso (V.Statuto)

Con l'associazione il socio ottiene inoltre l'invio delle riviste "Automation Technology" e "Automazione e Strumentazione".

Il Socio viene anche informato delle iniziative svolte dalle associazioni aderenti ad AIS.



Contatti:

Viale Campania, 31-20133 Milano

Tel. +39 02 54123816

www.aisisa.it | ais@aisisa.it

COME L'INTELLIGENZA ARTIFICIALE TRASFORMA LE IT OPERATIONS, ANCHE NEI DATA CENTER DELLE PMI

L'intelligenza artificiale non serve a costruire data center "magici" che si gestiscono da soli, ma a potenziare ciò che le IT Operations fanno già oggi: trasformare il monitoraggio in previsione, gli allarmi in diagnosi e gli interventi manuali in automazioni supervisionate. Per le PMI, dove tempo e competenze sono risorse scarse, l'AI operativa può ridurre il rumore, anticipare i problemi e rendere riutilizzabile la conoscenza dell'impianto, seguendo un percorso incrementale e misurabile.



**a cura di Damiano
Cosma De Angelis**
*AI Engineer, Consultant
& Trainer*

SOMMARIO

- La gestione operativa dell'IT riguarda tutta l'azienda
- Come si lavora oggi: la faticosa arte del tenere in piedi i sistemi
- Cosa cambia con l'AI: dalla reazione alla previsione
- Dalla teoria alla pratica
- Perché le PMI hanno più da guadagnare
- Da dove cominciare: un percorso in quattro passi
- Il mestiere che cambia
- Cosa ci portiamo via

La gestione operativa dell'IT riguarda tutta l'azienda

In ogni impresa industriale esiste un'infrastruttura quasi invisibile, ma da cui dipende tutto: la sala server. Che si tratti di due rack o di un data center, lì girano gestionale, posta, sistemi di fabbrica e applicativi.

Quando si ferma, si ferma l'azienda: le linee non ricevono ordini, le bolle non escono e il magazzino lavora alla cieca. Il costo di un'ora di fermo può misurarsi in decine

di migliaia di euro, senza contare il danno di reputazione.

La complessità è esplosa. Un sistema oggi segue hypervisor, macchine virtuali, container, storage, backup, reti, VPN e servizi esterni. Ogni livello produce metriche, log ed eventi, ma le squadre non sono cresciute: nelle PMI le IT Operations sono affidate a due o tre persone, talvolta a una sola.

La tesi è volutamente poco spettacolare. Nel solco dell'"Intelligenza Aumentata", l'AI non serve a co-



struire data center autonomi, ma a potenziare ciò che le IT Operations fanno già: trasformare il monitoraggio in previsione, gli allarmi in diagnosi e gli interventi manuali in automazioni supervisionate. La squadra resta la stessa, ma con capacità amplificate, o *“augmentate”*.

Come si lavora oggi: la faticosa arte del tenere in piedi i sistemi

La gestione operativa moderna poggia su tre pilastri: osservare, allarmare, intervenire. Gli strumenti leggono CPU, memoria, dischi, rete e latenze; hypervisor e orchestratori espongono lo stato dei carichi; i sistemi centralizzati conservano i log.

Allarmare significa impostare soglie e regole. Se la CPU supera un valore, un filesystem si riempie o un servizio non risponde, parte una notifica. Intervenire significa incrociare metriche e log, formulare ipotesi, risolvere e documentare l'accaduto nei ticket e nei runbook.

Questo modello ha limiti strutturali. Il primo è il rumore: le soglie fisse non distinguono un picco fisiologico da un problema vero e producono *“alert fatigue”*. Un incidente genera molti allarmi; separare causa ed effetti è già gran parte della diagnosi.

Il secondo limite è la dipendenza dall'esperienza individuale. La diagnosi vive nella testa di chi conosce la storia dell'impianto. Quando la persona giusta è assente o cambia azienda, il tempo di risoluzione si moltiplica: nelle PMI è un rischio concreto quanto un guasto hardware. Il terzo limite è il tempo. Analisi delle cause, revisione delle soglie, aggiornamento dei manuali e capacity planning scivolano in fondo alla lista. È tra dati che nessuno riesce a leggere e attività che nessuno riesce a svolgere che l'AI porta il contributo più concreto.

Cosa cambia con l'AI: dalla reazione alla previsione

Applicare l'AI alle IT Operations non significa installare un cervello elettronico che prende il controllo della sala, ma aggiungere alla base di monitoraggio quattro capacità crescenti.

Il primo gradino è il **rilevamento di anomalie**. Un modello impara il comportamento normale di carichi, latenze e log, considerando stagionalità e cicli produttivi. Segnala così scostamenti e derive lente anche entro le soglie classiche.

Il secondo è la **correlazione e riduzione del rumore**. Il clustering riconosce che notifiche legate da dipendenze note o apprese individuano un unico evento. Al

tecnico viene presentato un incidente con probabile origine ed effetti, non una raffica di messaggi.

Il terzo è la **diagnosi assistita**. Il sistema riceve metriche, log e registro dei cambiamenti e ricostruisce in linguaggio naturale cosa è successo, le cause probabili, i comandi di verifica e i precedenti nel manuale operativo. Per un team piccolo può significare passare da un'ora di indagine a pochi minuti.

Il quarto gradino è la **previsione e automazione**. I dati storici stimano saturazioni, limiti di carico e segnali che precedono un guasto. Dove diagnosi e correzione sono consolidate, diventano possibili riavvii controllati, ampliamenti di volumi o migrazioni preventive. L'AI propone, ma la responsabilità resta dell'operatore.

Per i primi gradini bastano modelli leggeri, eseguibili su una macchina virtuale e integrabili con il monitoraggio. La diagnosi può usare modelli linguistici come servizio o locali, preferibili per dati sensibili. Le proposte devono sempre essere spiegabili e accompagnate dai dati che le motivano.

L'AI non sostituisce il ciclo osserva-allarma-interviene, ma lo trasforma in osserva-comprende-suggerisce-agisci, rendendo ogni passaggio più ricco di contesto e meno dipendente dalla memoria e dall'intuito del singolo tecnico.

Dalla teoria alla pratica

Quattro scenari mostrano come queste capacità entrino nella quotidianità. In un'azienda con molti host e macchine virtuali, rilevamento di anomalie e raggruppamento degli eventi riducono le notifiche e ne aumentano la pertinenza: il team torna a fidarsi degli allarmi. In un'impresa alimentare il gestionale rallenta. Un assistente scopre che il problema coincide con un report introdotto da un aggiornamento, che satura lo storage nelle fasce di punta. L'ipotesi viene verificata e il report spostato di notte: nulla che un sistemista non potesse scoprire, ma in molto meno tempo.

In un altro caso, l'analisi dei dischi individua un cedimento imminente e consente una sostituzione programmata. Un team può inoltre collegare ticket e manuali a un modello linguistico: anche il tecnico più giovane recupera casi passati e soluzioni. La memoria dell'impianto non rimane soltanto nella testa del sistemista più anziano.

I benefici dipendono dalla qualità dei dati e dalla calibrazione iniziale. L'indicazione è però costante: meno



Figura 1 – Scala di maturità dell'AI nelle IT Operations.

rumore, diagnosi più rapide e più problemi intercettati in anticipo. L'AI legge i dati in continuo, li collega e li trasforma in suggerimenti concreti.

Perché le PMI hanno più da guadagnare

È diffusa la convinzione che queste tecniche abbiano senso solo per chi gestisce migliaia di server. L'esperienza suggerisce il contrario per quattro ragioni.

La prima è la **scarsità di tempo**. Un grande operatore può permettersi squadre dedicate a monitoraggio, capacity planning e affidabilità; una PMI no. Per un team di poche persone, un sistema che sorveglia migliaia di metriche e segnala solo ciò che merita non è un lusso.

La seconda è la **fragilità della conoscenza**. Nelle piccole organizzazioni le competenze raramente sono ridondate. Diagnosi assistita e memoria organizzativa costruita sui casi passati sono un'assicurazione contro la dipendenza dal singolo esperto.

La terza è la **riduzione della barriera d'ingresso**. Strumenti open source e librerie mature rendono previsione e rilevamento anomalie accessibili; i modelli linguistici sono disponibili come servizio o localmente.

La materia prima — metriche, log e ticket — è spesso già in casa.

La quarta è la **semplicità come acceleratore**. Una sala piccola ha meno variabili e inerzia. Un esperimento di correlazione o diagnosi assistita può essere provato, misurato e adottato rapidamente: la piccola dimensione diventa un vantaggio.

I prerequisiti sono chiari: monitoraggio ordinato, storico di metriche e log, registro dei cambiamenti e governance di ciò che il sistema può fare, proporre o sottoporre ad approvazione.

L'AI va trattata come un collega brillante e veloce, non come un oracolo.

Da dove cominciare: un percorso in quattro passi

Una PMI può seguire un cammino incrementale, affrontabile in poche settimane per passo e in larga parte con risorse interne.

Primo passo: consolidare l'osservazione. Portare in un unico sistema le metriche di host, macchine virtuali, container e servizi, centralizzare i log e istituire il registro dei cambiamenti. L'obiettivo è vedere lo stato

dell'infrastruttura sulla stessa linea temporale e creare lo storico su cui si appoggia tutto il resto.

Secondo passo: attivare rilevamento di anomalie e correlazione. Sulle serie storiche, abilitare anomaly detection e raggruppamento degli allarmi correlati. Occorre calibrare con pazienza, accettare qualche falso positivo iniziale e istituire un processo in cui il team verifica le segnalazioni e fornisce feedback.

Terzo passo: introdurre la diagnosi assistita. Collegare un modello linguistico a metriche, log, registro dei cambiamenti, ticket e manuale operativo, iniziando in modalità consultiva. L'assistente risponde e propone ipotesi, ma non tocca nulla. È la fase del *"Parla con i tuoi dati"*, nella quale i benefici diventano visibili nei tempi di risoluzione.

Quarto passo: automatizzare con prudenza. Solo a questo punto introdurre le prime azioni automatiche, partendo da quelle reversibili e a basso rischio — pulizia dello spazio disco, riavvio controllato di un servizio, ampliamento di un volume — con supervisione umana, limiti espliciti e possibilità di tornare indietro.

La conoscenza dell'impianto deve restare interna; le competenze specialistiche possono essere acquisite all'esterno con un esplicito trasferimento di know-how. Il progetto va misurato tramite numero di allarmi, tempi di diagnosi e risoluzione, problemi anticipati e ore liberate dalle emergenze.

Il mestiere che cambia

Gli strumenti di gestione incorporano capacità di AI a ritmo crescente e la distinzione tra *"monitoraggio"* e *"AI operativa"* probabilmente scomparirà. I nuovi carichi digitali renderanno le infrastrutture più dense e critiche: l'AI è una causa dell'aumento di complessità, ma anche lo strumento più promettente per governarla.

Il mestiere delle IT Operations si evolve verso l'alto: meno tempo a scorrere log e inseguire allarmi, più tempo a definire politiche, validare proposte, progettare l'affidabilità e capire il legame tra sistemi e business. L'operatore aumentato non è sostituito: governa un livello di complessità prima fuori portata e torna ad avere tempo per le attività che creano valore.

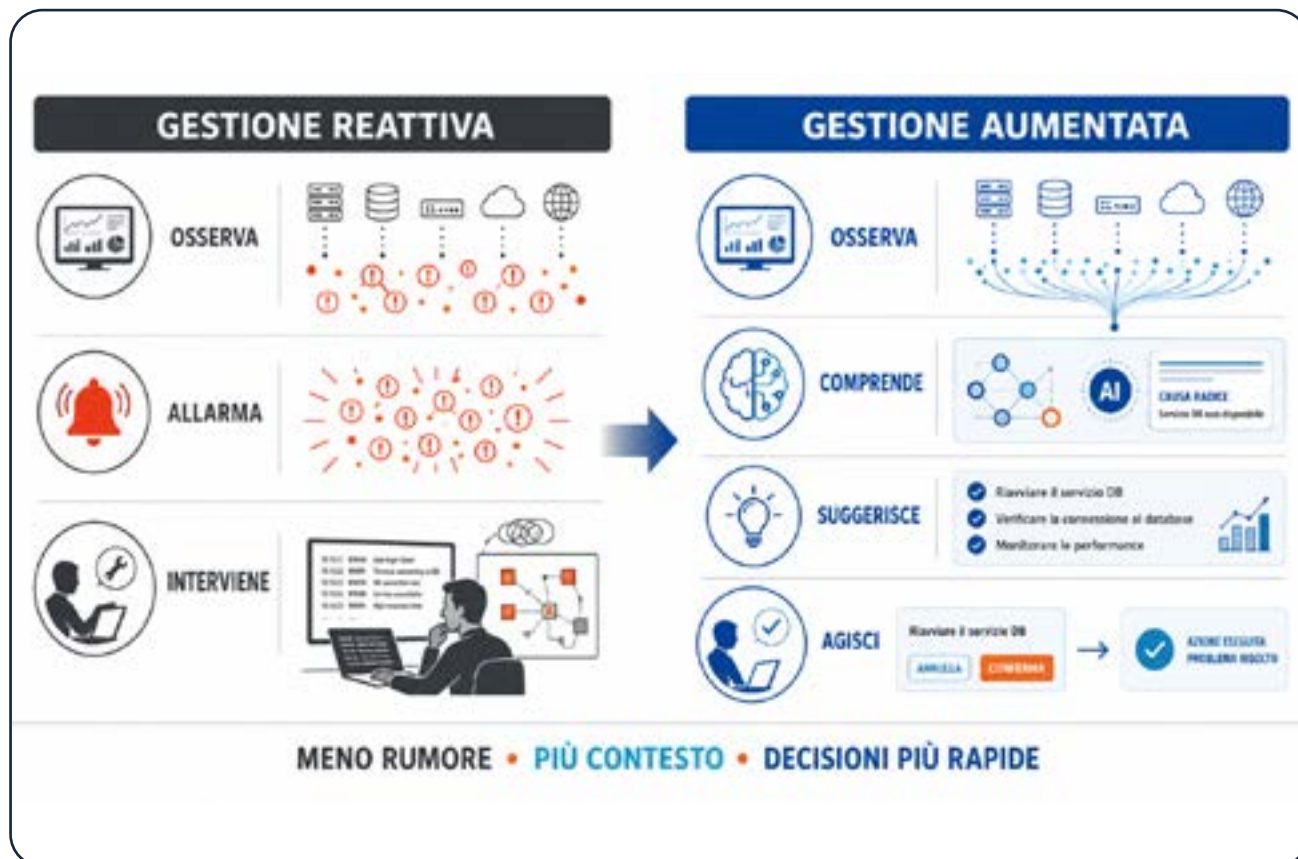


Figura 2 – Dalla gestione reattiva a quella aumentata: meno rumore, più contesto e decisioni più rapide.

Cosa ci portiamo via

Primo: si parte dall'osservazione, non dai modelli. Se metriche e log non sono raccolti, centralizzati e storicizzati, quello è il primo investimento. Secondo: si procede per gradini – vedere, comprendere, prevedere, agire – raccogliendo valore a ogni passo. Terzo: la dimensione non è una scusa. Nelle sale medio-piccole, dove il tempo è poco e la conoscenza fragile, il rapporto tra sforzo e beneficio è favorevole. Quarto: servono partner capaci di offrire supporto e trasferimento di conoscenza.

La domanda non è se l'AI entrerà nella gestione operativa dei data center, ma se la si lascerà entrare da protagonisti, governandola, o da spettatori. Per le PMI italiane, che dell'adattamento intelligente hanno fatto storicamente la propria forza, la risposta dovrebbe essere scontata.

IN SINTESI – TRE COSE DA RICORDARE

- Prima l'osservazione, poi i modelli: senza metriche, log e cambiamenti storicizzati non c'è intelligenza che tenga.
- Procedere per gradini – vedere, comprendere, prevedere, agire – raccogliendo valore a ogni passo.
- La piccola dimensione è un vantaggio: meno inerzia, sperimentazione rapida e valorizzazione della conoscenza.

Keywords: *intelligenza artificiale, AI operativa, IT Operations, AIOps, data center, PMI, operatore aumentato, anomaly detection, monitoraggio infrastrutturale, diagnosi assistita, manutenzione predittiva, automazione supervisionata, machine learning, modelli linguistici, gestione degli allarmi, capacity planning, osservabilità.*

FONDAMENTI DI INTELLIGENZA ARTIFICIALE E MACHINE LEARNING

Applicazioni nel settore dei sistemi elettrici

Autore: Cosma Damiano De Angelis

Prezzo: 29,00 €

Pagine: 256

Nell'era della transizione energetica, l'intelligenza artificiale (AI) si propone come strumento rivoluzionario per ottimizzare i consumi e la produzione di energia all'interno delle aziende. Questo libro, frutto della lunga esperienza dell'autore come progettista di sistemi, consulente e formatore aziendale, offre una risposta concreta a questa domanda fondamentale: come può l'AI migliorare i processi produttivi e l'efficienza energetica?



PER L'ACQUISTO

<https://libri.editorialedelfino.it/prodotto/fondamenti-di-intelligenza-artificiale-e-machine-learning/>





L'esperienza al servizio dell'innovazione



**Certificazione
reti**



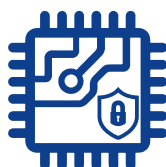
**Corsi di
formazione**



**Compatibilità
EMC**



**OT Cyber
Security**



**Soluzioni
embedded**



**Analisi e
diagnostica
reti**



**Permanent
networking
monitoring**



Genoa Fieldbus Competence Centre Srl

Sede operativa: Via Greto di Cornigliano 6R int. 38, 16152, Genova - Italia

Tel. (+39) 010 86.02.580 | e-mail: info@gfcc.it | www.gfcc.it

DISCHI DI ROTTURA: FUNZIONAMENTO, NORMATIVE E CONFRONTO CON LE VALVOLE DI SICUREZZA

SECONDA PARTE

Il disco di rottura è un dispositivo di sicurezza essenziale per la protezione di impianti in pressione, progettato per intervenire in modo rapido e affidabile al superamento di una soglia critica. Questa seconda parte approfondisce i criteri di marcatura, verifica, dimensionamento, installazione e selezione dei dischi di rottura secondo la serie ISO 4126. Dalle tolleranze della pressione di scoppio alle prove sui lotti produttivi, vengono analizzati rapporti di utilizzo, coefficienti di portata e metodi di calcolo.



a cura di Alessandro Brunelli *

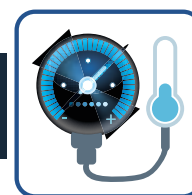
SOMMARIO

- Marcatura
- Criteri di dimensionamento
- Equazioni di dimensionamento
- Criteri di installazione
- Criteri di selezione

Marcatura

La marcatura consente di identificare in modo univoco il disco di rottura e di verificarne la corrispondenza con le condizioni di progetto dell'impianto. Le informazioni riportate permettono di risalire al costruttore, al lotto produttivo, alla pressione e alla temperatura di scoppio specificate, nonché alle principali caratteristiche del dispositivo. La loro leggibilità e permanenza sono

quindi essenziali per il montaggio, i controlli periodici, la manutenzione e la corretta sostituzione del disco. Tutti i dati essenziali relativi sia al costruttore sia al dispositivo di protezione devono essere marcati in modo indelebile direttamente sul disco di rottura oppure riportati su una targhetta metallica saldata al disco. La marcatura viene apposta dopo il superamento delle prove previste sul lotto produttivo e costituisce un elemento fondamentale



per la conformità e la tracciabilità del dispositivo.

La Figura 4 presenta:

- a) alcuni esempi di targhette utilizzate per la marcatura dei dischi di rottura;
- b) i limiti della regione normale di funzionamento e della tolleranza ammessa per la pressione di scoppio.

La marcatura avviene a seguito delle prove di scoppio positive effettuate sui lotti di produzione dei dischi di rottura (Tabella 4) con tolleranza ammessa sul valore nominale della pressione normalmente del $\pm 5\%$.

Inoltre, per mantenere nel tempo la prevista pressione di scoppio dei dischi di rottura, è opportuno impiegare i dischi in un campo di impiego inferiore alla pressione di scoppio per evitare prematuri cedimenti per fatica del disco, e pertanto va previsto un rapporto di utilizzo tra la pressione di esercizio e la pressione di scoppio come riportato in Tabella 5.

Criteri di dimensionamento

La norma ISO 4126-6 nell'Allegato C descrive due metodi di dimensionamento dei dischi di rottura:

1. Un metodo semplificato (par. C2) che traslascia le perdite di carico nelle tubazioni di ingresso e di scarico e le sostituisce con un coefficiente di portata tipico a variabile a seconda della geometria di installazione (Tabella 6).



Figura 4(a) – Esempi di etichette di targatura dei dischi di rottura.

Numero di Dischi del Lotto di Produzione	Numero di Dischi da Scoppiare
< 10	2
10 - 15	3
16 - 30	4
31 - 100	6
101 - 250	4% ma ≥ 6
251 - 999	3% ma ≥ 10
< 1000	30 minimo

Tabella 4 - Dischi da sottoporre a prova per verificare la pressione di scoppio (ISO 4126-2).

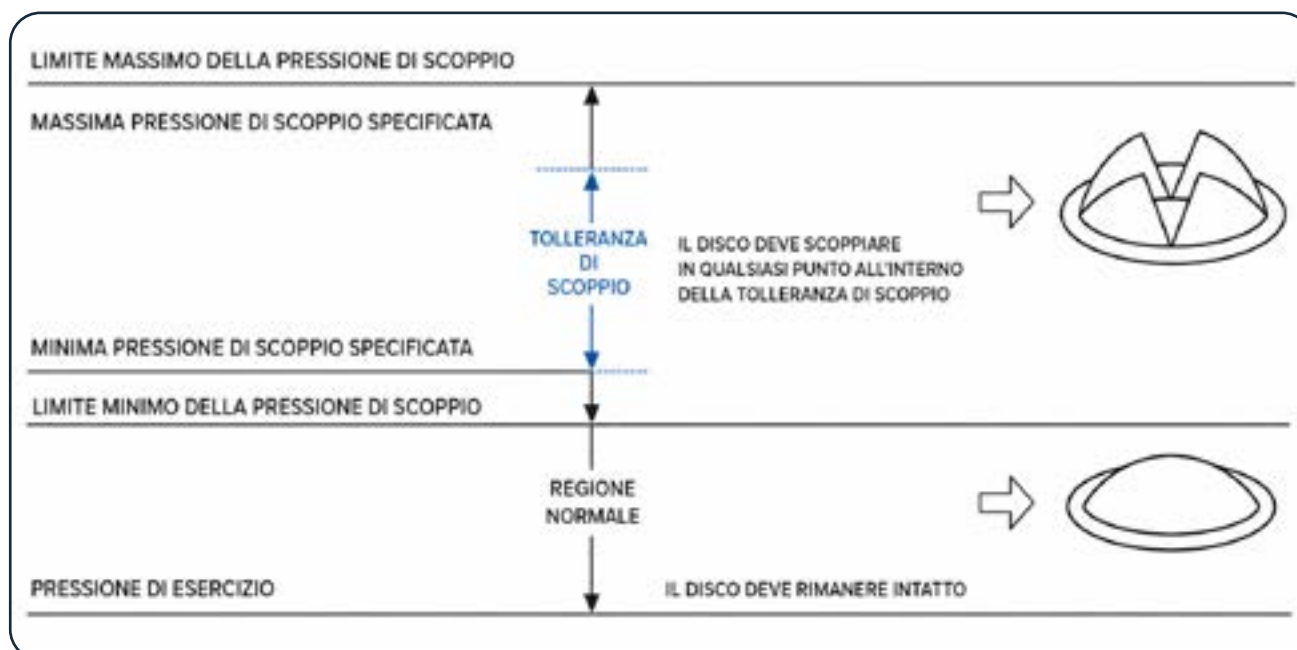


Figura 4(b) – Funzionalità normale e tolleranza di scoppio dei dischi di rottura (ISO 4126-2).

Tipo di Disco di Rottura	Rapporto Pressione Esercizio Vs Pressione Scoppio
Convenzionale	0.7
Convenzionale preinciso	0.8
Rovescio preinciso	0.9
Rovescio composto o multistrato	0.9
Grafite sostituibile o monoblocco	0.8
Piano composto inciso	0.5

Tabella 5 - Massimo rapporto tra pressione di esercizio e pressione di scoppio (ISO 4126-6).

2. Un metodo completo (par. C3) che tiene conto di tutte le perdite di carico del sistema e richiede anche la conoscenza del coefficiente di resistenza di scarico del disco di rottura K_{dr} , determinato con prove di flusso sperimentali presso il costruttore o laboratori qualificati.

Equazioni di dimensionamento

Il dimensionamento dei dischi di rottura viene generalmente condotto secondo le equazioni di dimensionamento previste dalle predette Norme Internazionali ISO 4126-6, che permettono di calcolare l'area di scarico A e quindi di selezionare un'area effettiva di scarico lievemente superiore.

Le formule di calcolo sono abbastanza complesse e si rimanda alla ISO 4126-6 per eventuali approfondimenti; ciò nonostante i diversi costruttori mettono a

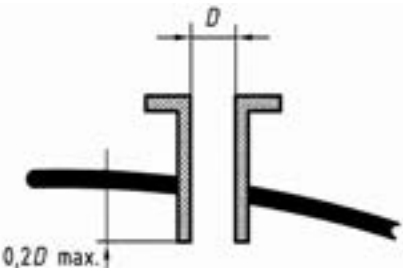
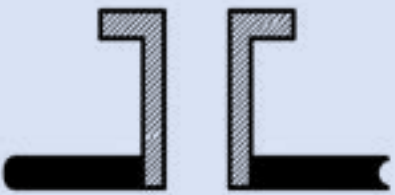
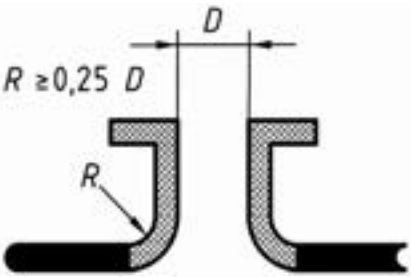
installazione numero	Configurazione boccaglio	Descrizione	Coefficiente portata ^a
1		Nel caso di un interno sporgente ugello	0.68
2		Nel caso di un ugello o di una flangia i cui ingressi non sono in configurazione idrodinamica	0.73
3		Nel caso di un ugello o di una flangia in configurazione idrodinamica, ad esempio con arrotondato o smussato ingresso	0.80

Tabella 6 - Coefficienti di portata a, per varie condizioni di boccaglio di installazione del disco per fluidi comprimibili, altrimenti considerare per sicurezza per fluidi incomprimibili 0.62 (ISO 4126-6).

diposizione dei clienti dei programmi di calcolo operanti su Excel.

Esempio di calcolo

A titolo dimostrativo nel prosieguo si effettuerà un dimensionamento dell'area di scarico per liquidi A, mediante la formula di calcolo derivata dalla ISO 4126-6, Allegato C.2:

$$A = \frac{Q_m}{1,61 K_{dr} K_v \sqrt{\Delta P \rho}}$$

con questi dati del processo:

- Fluido di scarico: Olio
- $P_s = 7$ bar r: Pressione di scoppio (taratura)
- $P_1 = 8$ bar a: Pressione di scarico ($P_s + P_{atm}$)
- $P_b = 1$ bar a: Contropressione di scarico (P_{atm})
- $\Delta P = 7$ bar: Pressione differenziale di scarico
- $T_1 = 20$ °C: Temperatura di scarico del liquido
- $\rho = 900$ kg/m³: Massa volumica o densità del liquido
- $\mu = 0,15$ Pa.s: Viscosità dinamica del liquido
- $Q_m = 10000$ kg/h: Portata di scarico del liquido

e assumendo questi parametri di calcolo:

- $K_{dr} = 0,62$: Coefficiente di scarico (α) del disco di rottura (Tabella 6)
- $K_v = 1$: Coefficiente di Reynolds di scarico del liquido in regime turbolento

Pertanto risulta una area teorica di scarico A_t :

$$A_t = 126 \text{ mm}^2$$

In realtà l'area effettiva di scarico A_e , risulta lievemente superiore, perché il liquido da scaricare non essendo acqua con bassa viscosità (0,001 Pa.s) ha un Numero di Reynolds inferiore a 2000, e pertanto lo scarico avviene in regime quasi laminare, e applicando l'esatto Coefficiente di Reynolds $K_v = 0,938$ (che risulterebbe secondo le formule ISO 4126-6) risulta un'area effettiva A_e :

$$A_e = A_t / K_v = 126 / 0,938 = 135 \text{ mm}^2.$$

In questo caso l'area effettiva risulta maggiore neanche del 10% rispetto quella teorica (che prevede uno

scarico del liquido in regime turbolento), ma attenzione con fluidi molto più viscosi, si può avere un'area effettiva financo 3 volte maggiore di quella teorica (ISO 4126-7)!

Criteri di installazione

La corretta installazione è determinante per garantire che il disco di rottura intervenga alla pressione prevista e assicuri nel tempo le prestazioni dichiarate. La configurazione del portadisco, il suo orientamento e la posizione rispetto al recipiente influenzano infatti la pressione di apertura, la capacità di scarico e la durata del dispositivo. Occorre inoltre evitare tubazioni, raccordi o discontinuità che possano introdurre perdite di carico, accumuli di prodotto o sollecitazioni meccaniche non previste.

I dischi di rottura, con esclusione dei modelli progettati per essere inseriti direttamente tra le flange, devono essere installati esclusivamente nel portadisco specifico indicato e fornito dal costruttore. L'impiego di supporti non compatibili o un montaggio non conforme possono compromettere sia il corretto intervento alla pressione richiesta sia la durata del dispositivo.

La Figura 5 illustra alcune configurazioni tipiche di portadisco e le più comuni installazioni flangiate per dischi di rottura di medie e grandi dimensioni.

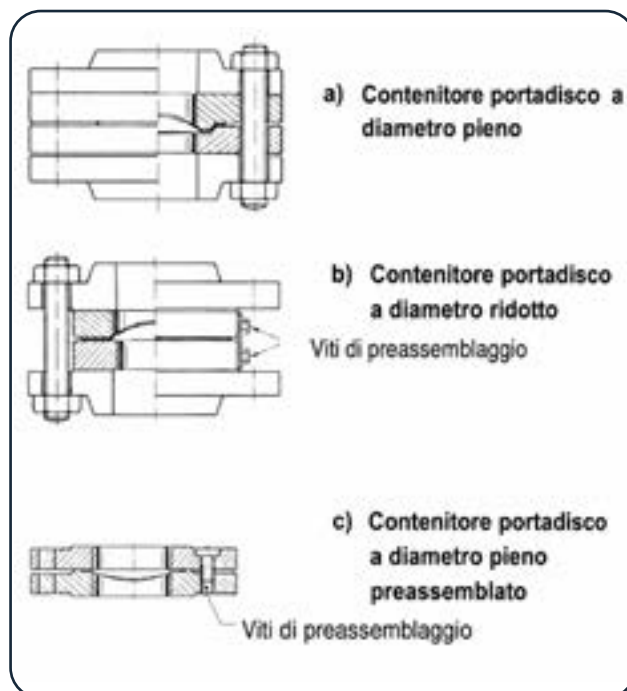


Figura 5 – Installazione a flangiare per medi e grandi dischi di rottura.

Tipologia dischi	Caratteristiche	Applicazioni
Convenzionali solidi	Possibilità frammentazione	Impieghi generali
Compositi bombati	Senza frammentazione	Impieghi generali anche con valvole di sicurezza
Rovesci	Senza frammentazione	Impieghi con valvole di sicurezza
Piani	Montati direttamente su flange	Recipienti a bassa pressione
Grafite	Frammentazione	Recipienti fluidi corrosivi
Unità sigillate	Montati dal costruttore	Impieghi ad elevate pressioni
Attacchi sanitari	Sterilizzabile	Per industria farmaceutica o alimentare

Tab. 7 - Caratteristiche principali e applicazioni normali dei dischi di rottura.

In ogni caso il disco di rottura deve essere installato, solitamente sulla sommità del recipiente da proteggere, direttamente sul cielo del recipiente stesso, altrimenti ne può inficiare il coefficiente di efflusso o di portata a (vedasi Tabella 6).

Criteri di selezione dei dischi di rottura

La selezione del disco di rottura deve tenere conto delle specifiche condizioni di processo, tra cui pressione e temperatura di esercizio, natura e corrosività del fluido, presenza di contropressione, eventuali cicli di pressione e requisiti igienico-sanitari.

Occorre inoltre valutare il rischio di frammentazione, la compatibilità con le valvole di sicurezza, la modalità di installazione e il rapporto tra pressione di esercizio e pressione di scoppio.

La Tabella 7 riporta, a carattere esemplificativo, le principali caratteristiche costruttive e le applicazioni tipiche delle diverse tipologie di dischi di rottura trattate. Il confronto fornisce un primo orientamento per individuare la soluzione più adatta alle varie applicazioni di processo, ferma restando la necessità di verificare il dimensionamento e la compatibilità dei materiali con le effettive condizioni operative.

Keywords: disco di rottura; rupture disk; sicurezza pressione; sovrappressione; valvola di sicurezza; PED 2014/68/UE; EN ISO 4126; ASME; API 520; impianti industriali; protezione apparecchiature; scarico pressione; sicurezza impianti; fluidi corrosivi; dispositivi di sicurezza.

L'Autore*

Alessandro Brunelli, Esperto in automazione, strumentazione, taratura e sicurezza degli impianti industriali. Segretario CEI SC65B: Misura e Controllo dei Processi Industriali



ASSOCIAZIONE NAZIONALE ITALIANA PER L'AUTOMAZIONE

Dal 1956 ANIPLA si propone di favorire e divulgare in Italia la conoscenza, lo studio e l'applicazione dell'automazione considerandola nei suoi aspetti tecnologici, economici e sociali, contribuendo in tal modo alla progressiva maturazione della cultura tecnica nel Paese e al suo inserimento nel contesto nazionale.

ANIPLA organizza su iniziativa dei propri associati convegni, giornate di studio, workshop, corsi di formazione, osservatori, incontri tra aziende e studenti delle facoltà tecniche e delle scuole tecniche superiori, visite guidate in impianti produttivi.

L'associazione ha all'attivo collaborazioni con le più significative realtà industriali, associative e universitarie italiane.

DIVENTA SOCIO ANIPLA!

Iscriviti subito

Per iscriversi basta compilare il form che trovi su www.anipla.it/iscriviti/.

L'iscrizione dovrà essere successivamente completata attraverso il pagamento della quota associativa tramite bonifico.

IBAN IT38 V 03069 09425 10000000 2168

Perché associarsi

Essere iscritti all'ANIPLA significa essere costantemente aggiornati sull'evoluzione scientifica, tecnologica e del mercato dell'automazione.

I soci, tempestivamente informati di tutte le attività dell'associazione tramite il sito, i canali aperti su FB e Lin e la newsletter mensile, ricevono gratuitamente in formato cartaceo la rivista Automazione e Strumentazione, organo informativo ufficiale ANIPLA, possono accedere alle cariche sociali elettive, contribuire alla definizione delle manifestazioni culturali e naturalmente prendervi parte.

Tipologie di soci

I Soci dell'ANIPLA sono divisi nelle seguenti categorie:

Persone fisiche

Soci ordinari – quota annuale 55,00 euro

Soci junior (fino ai 28 anni compresi) – quota annuale 10,00 euro

Nota bene: le quote restano valide sino al 31.03 dell'anno successivo a quello di iscrizione.

È possibile iscriversi congiuntamente ad ANIPLA e AIDIC oppure ad ANIPLA e AIMAN con un vantaggioso sconto sulla associazione congiunta. Nella compilazione del form sottostante, si dovrà selezionare l'opzione relativa.

Aziende

Soci collettivi – quota annuale 275,00 euro

Soci sostenitori – quota annuale 825,00 euro

Nota bene: le quote restano valide sino al 31.03 dell'anno successivo a quello di iscrizione.

È inoltre possibile iscriversi congiuntamente ad ANIPLA e AIMAN. Nella compilazione del form sottostante, si dovrà selezionare l'opzione relativa.

Il rinnovo di tutte le quote va fatto entro il 31.03 dell'anno successivo.

Informazioni complete su www.anipla.it/iscriviti/

DAL MICROPROCESSORE AL TENSORE: L'ARCHITETTURA DEI CHIP NELL'ERA DELL'AI

Dalla CPU generalista agli acceleratori progettati per l'intelligenza artificiale, il silicio cambia architettura per sostenere il calcolo parallelo e tensoriale. L'articolo ripercorre l'evoluzione da GPU e CUDA a TPU, NPU e Tensor Core, spiegando il ruolo di array sistolici, precisione ridotta e memorie HBM. Un percorso che conduce ai sistemi eterogenei e all'Edge AI, dove CPU e unità specializzate collaborano per aumentare prestazioni, efficienza energetica e velocità di elaborazione.



a cura di Massimo Nannini^(*)

SOMMARIO

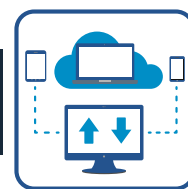
- Introduzione
- La CPU: il "tuttofare" e il collo di bottiglia di Von Neumann
- La Svolta del Calcolo Parallelo: Dalla Grafica 3D ad AlexNet
- L'Era degli Acceleratori AI Dedicati: TPU, NPU e Tensor Core
- Tensor Cores e la Precisione Ridotta

Introduzione

Nel 1971, l'introduzione dell'Intel 4004 racchiuse 2 300 transistor su una singola piastrina di silicio, dando vita all'era del microprocessore commerciale. Per oltre quattro decenni, l'evoluzione del calcolo ha seguito il paradigma della CPU (Central Processing Unit): un cervello elettronico generalista progettato per eseguire qualsiasi algoritmo attraverso una sequenza logica di istru-

zioni. Tuttavia, l'esplosione dell'Intelligenza Artificiale e dei modelli di *Deep Learning* ha messo a nudo i limiti di questo approccio.

L'hardware per l'AI non richiede un'orchestra diretta da pochi esecutori altamente specializzati, bensì un esercito coordinato di milioni di calcolatori elementari che lavorano in parallelo. Comprendere la differenza tra una CPU e un chip specifico per l'AI (come GPU, TPU o NPU) significa esplorare una tran-



sizione fondamentale nell'ingegneria informatica: il passaggio dal calcolo sequenziale a quello tensoriale.

La CPU: il “tuttofare” e il collo di bottiglia di Von Neumann

La CPU moderna rappresenta il risultato di decenni di evoluzione dell'architettura di Von Neumann. Progettata per gestire il sistema operativo, elaborare gli input dell'utente ed eseguire software molto diversi tra loro, è ottimizzata soprattutto per ridurre la latenza nell'esecuzione di un singolo flusso di istruzioni. Per raggiungere questo obiettivo, una parte rilevante della superficie dei processori moderni, come quelli basati su architetture Intel x86 o ARM Cortex, non è occupata dalle unità aritmetico-logiche, ma da strutture di supporto. Tra queste rientrano le cache L1, L2 e L3, memorie estremamente veloci che mantengono i dati vicini ai core riducendo i tempi di accesso alla RAM, e le complesse unità di controllo. Tecniche come la previsione delle ramificazioni (*branch prediction*) e l'esecuzione fuori ordine (*out-of-order execution*) riorganizzano dinamicamente le istruzioni per sfruttare al meglio le risorse disponibili ed evitare che il processore rimanga inattivo.

Questa flessibilità rende la CPU ideale per le applicazioni general-purpose, ma meno efficiente nell'elaborazione delle reti neurali.

L'addestramento e l'inferenza dei modelli di intelligenza artificiale si basano infatti su grandi quantità di moltiplicazioni tra matrici, operazioni ad alta densità note come GEMM (*General Matrix Multiply*).

Il calcolo di un livello della rete può essere sintetizzato dalla relazione:

$$Y = f(W \cdot X + b)$$

dove W rappresenta la matrice dei pesi, X i dati di ingresso, b il termine di bias e f la funzione di attivazione che introduce la non linearità necessaria alla rete neurale. Per eseguire queste operazioni, una CPU deve trasferire continuamente grandi quantità di dati tra RAM, cache, registri e unità di calcolo attraverso il bus di sistema. Il cosiddetto collo di bottiglia di Von Neumann deriva proprio dalla separazione fisica tra memoria ed elaborazione: quando i dati non arrivano abbastanza rapidamente, le risorse computazionali restano in attesa e il throughput complessivo risulta limitato.

La Svolta del Calcolo Parallelo: dalla Grafica 3D ad AlexNet

La transizione verso l'hardware dedicato all'AI ha radici insospettabili nel settore del gaming. Le GPU (Graphics Processing Unit) nascevano per calcolare la posizione e l'illuminazione di milioni di pixel contemporaneamente, applicando trasformazioni geometriche a matrici tridimensionali.

Nel 2006, NVIDIA introdusse l'architettura CUDA, trasformando la GPU da processore a funzione fissa a piattaforma programmabile per scopi generali (GP-GPU). La svolta storica avvenne nel 2012 con la competizione *ImageNet*: la rete neurale AlexNet, progettata da Alex Krizhevsky, Ilya Sutskever e Geoffrey Hinton, sbaragliò la concorrenza venendo addestrata non su server CPU tradizionali, ma su due GPU NVIDIA GeForce GTX 580.

Mentre una CPU high-end dispone di pochi core (da 8 a 128) operanti a frequenze elevate (fino a 5 GHz o più), una GPU integra migliaia di core più piccoli operanti a frequenze inferiori. L'architettura abbandona la complessa logica di controllo in favore della parallizzabilità massiva guidata dal modello SIMT (Single Instruction, Multiple Threads).

L'era degli acceleratori AI dedicati: TPU, NPU e Tensor Core

La necessità di elaborare modelli sempre più grandi ha spinto l'industria oltre il semplice adattamento delle GPU nate per la grafica, portando allo sviluppo di acceleratori specializzati e ASIC (Application-Specific Integrated Circuit) progettati per l'intelligenza artificiale. Nel 2016 Google presentò la prima TPU (Tensor Processing Unit), basata su un'architettura ad array sistolico (*systolic array*). A differenza della CPU, che trasferisce frequentemente dati e risultati intermedi tra unità di calcolo, registri e memoria, in un array sistolico i dati fluiscono in modo continuo attraverso una griglia di nodi di elaborazione costituiti da unità MAC (*Multiplier-Accumulate*), con un movimento ritmico che richiama quello del sangue spinto dal cuore. Le moltiplicazioni tra matrici possono così essere eseguite limitando gli accessi alla memoria principale, con una significativa riduzione dei consumi energetici e un aumento della densità di calcolo.

A partire dall'architettura Volta, introdotta nel 2017, NVIDIA ha integrato nelle proprie GPU blocchi hardwa-

re specializzati denominati Tensor Core. Questi componenti sono progettati per eseguire in modo estremamente parallelizzato operazioni di moltiplicazione e accumulo tra matrici, sintetizzabili nella relazione:

$$D = A \cdot B + C$$

Parallelamente, si è compreso che le reti neurali non richiedono sempre la precisione in virgola mobile a 64 bit, FP64, o a 32 bit, FP32, tipica di applicazioni come la simulazione fisica e alcuni calcoli scientifici o finanziari. L'addestramento e l'inferenza possono infatti utilizzare formati a precisione ridotta. FP16 e BF16 (Brain Floating Point) diminuiscono lo spazio occupato dai pesi e dai dati mantenendo un'adeguata gamma dinamica, mentre INT8, FP8 e FP4 consentono di ridurre ulteriormente la memoria necessaria e il carico computazionale attraverso tecniche di quantizzazione, soprattutto nell'inferenza. In questo modo è possibile moltiplicare le prestazioni e migliorare l'efficienza energetica a parità di superficie del chip.

La Banda di Memoria e le HBM

Nei moderni acceleratori AI, come NVIDIA Hopper e Blackwell o AMD Instinct, il limite non è solo la potenza di calcolo, ma anche la velocità con cui i dati raggiungono le unità di elaborazione. Le HBM (High Bandwidth Memory) rispondono a questa esigenza impilando verticalmente più strati di memoria DRAM, collocati accanto al chip su un *interposer* di silicio. Le generazioni HBM3 e HBM4 raggiungono bande di diversi terabyte al secondo, contro le decine o centinaia di gigabyte al secondo tipiche delle DDR5, aumentando il throughput e l'efficienza degli acceleratori AI.

L'Integrazione Eterogenea e l'AI al Margine

L'evoluzione recente risponde alla necessità di portare l'Intelligenza Artificiale direttamente sui dispositivi utente (*Edge AI*) per questioni di privacy, latenza ed efficienza energetica. Non si tratta più di scegliere tra CPU o chip AI, ma di integrarli nello stesso sistema. Processori moderni per PC e smartphone integrano architetture eterogenee su un unico SoC (System on

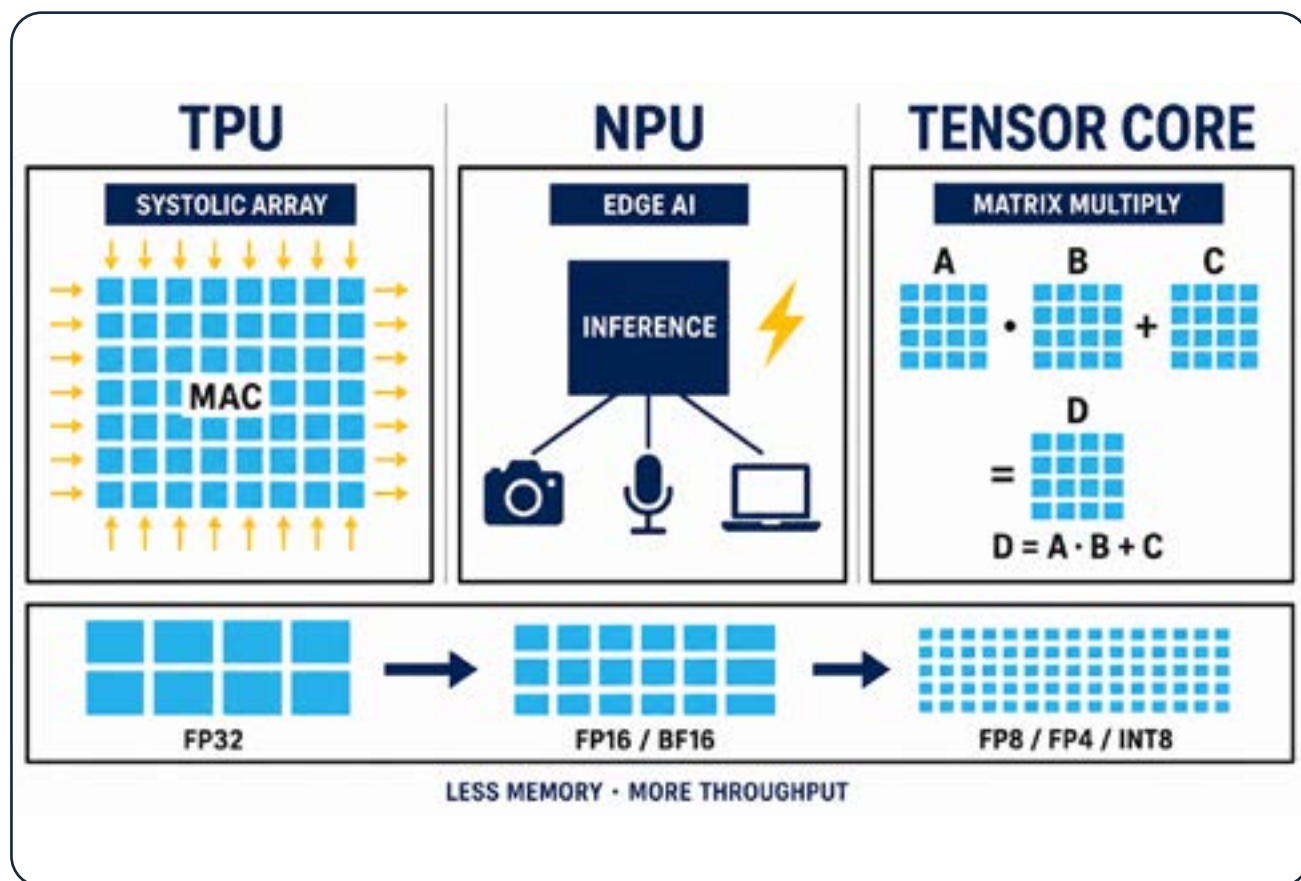


Figura 1 – TPU, NPU e Tensor Core: gli acceleratori specializzati per l'intelligenza artificiale.

Caratteristica	CPU (Central Processing Unit)	Chip AI (GPU / TPU / NPU)
Obiettivo Architettuale	Minima latenza su calcoli sequenziali	Massimo throughput su calcoli paralleli
Composizione del Die	Prevalenza di Cache e Logic Control	Prevalenza di Array ALU/MAC (Compute Units)
Modello di Esecuzione	MIMD / Out-of-Order / Branch Prediction	SIMD / SIMT / Dataflow Systolic
Precisione Nativa	FP32, FP64, INT64	FP16, BF16, FP8, FP4, INT8
Banda di Memoria Tipica	(DDR4 / DDR5)	(HBM3 / HBM4)
Casi d'Uso Ideali	Sistemi Operativi, Database, Logica condizionale	Addestramento e Inferenza di LLM, Visione Artificiale

Tabella 1 - CPU e chip AI: architetture e prestazioni a confronto.

Chip) o tramite *chiplet* interconnessi tramite packaging avanzato (come TSMC CoWoS):

- **CPU:** Gestisce il codice dell'applicazione e le chiamate di sistema.
- **GPU:** Gestisce il rendering grafico e calcoli paralleli ad hoc.
- **NPU (Neural Processing Unit):** Blocco ad alta efficienza energetica progettato esclusivamente per eseguire modelli di inferenza in background (ad esempio il riconoscimento facciale, la cancellazione del rumore via software o la generazione locale di testo) con un impatto minimo sulla batteria.

L'avvenire della microelettronica non prevede la scomparsa della CPU, la cui flessibilità rimane insostituibile per l'infrastruttura di base dell'elaborazione dati. Assisted piuttosto alla fine del monopolio dell'architettura generalista. L'hardware dell'era dell'AI è dominato dalla specializzazione di dominio, in cui la struttura fisica del silicio ricalca direttamente la forma matematica degli algoritmi che deve eseguire.

Keywords: *chip AI, microprocessori, CPU, GPU, TPU, NPU, Tensor Core, calcolo tensoriale, Edge AI, memorie HBM.*

L'autore*

IT engineer and business consultant,
info@gemaxconsulting.it

DAL GUASTO ALLA SOLUZIONE CON IL METODO 8D

Sorta nell'industria e consolidata nel settore automotive, la metodologia 8D offre un percorso strutturato per descrivere i problemi, contenerne gli effetti, individuarne le cause e prevenirne il ripetersi. Il confronto tra un guasto industriale e una criticità domestica ne dimostra la trasversalità: distinguendo cause tecniche e fragilità di sistema, l'8D trasforma ogni errore in conoscenza, rafforza l'affidabilità dei processi e alimenta il miglioramento continuo.



a cura di Laura Profeta*

SOMMARIO

- Introduzione
- Il metodo 8D alla prova: dalla fabbrica alla vita quotidiana
- Dalla causa radice alla prevenzione
- Trasformare l'esperienza in conoscenza
- Considerazioni
- Conclusioni

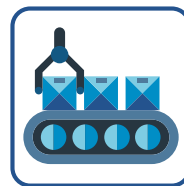
Introduzione

Nata in ambito industriale, in particolare nel settore automotive, la metodologia 8D è stata sviluppata per affrontare problematiche di natura complessa attraverso un'azione strutturata e organica di analisi, contenimento e prevenzione degli eventi critici.

Nel tempo, tuttavia, la sua applicabilità si è rivelata molto più ampia, estendendosi anche a contesti extra-industriali ed ai problemi della vita quotidiana.

Infatti, indipendentemente dall'ambito in cui possa emergere il problema, il rigoroso processo logico della metodologia 8D può trovare applicazione pratica. Oltre che propedeutica all'eliminazione del problema alla radice, questa metodologia offre il valore aggiunto di indagare le cause dell'evento mettendo in evidenza le fragilità del sistema, rafforzando l'affidabilità dei processi e riducendo il rischio di recidive.

In questa prospettiva, ogni criticità – da un malfunzionamento elettro-



nico a un'inefficienza nella gestione quotidiana — può diventare un'opportunità di apprendimento e di miglioramento continuo. L'approccio 8D si configura, pertanto, non solo come uno strumento di problem solving, ma, altresì, come una vera e propria metodologia per trasformare gli errori in conoscenza e i problemi in occasioni di crescita.

Il metodo 8D alla prova: dalla fabbrica alla vita quotidiana

Per evidenziare la trasversalità della metodologia 8D, è possibile confrontare due diverse situazioni accomunate dalla medesima criticità di base: la mancanza d'acqua. In ambito industriale, tale evento può determinare il fermo di apparecchiature e linee produttive,

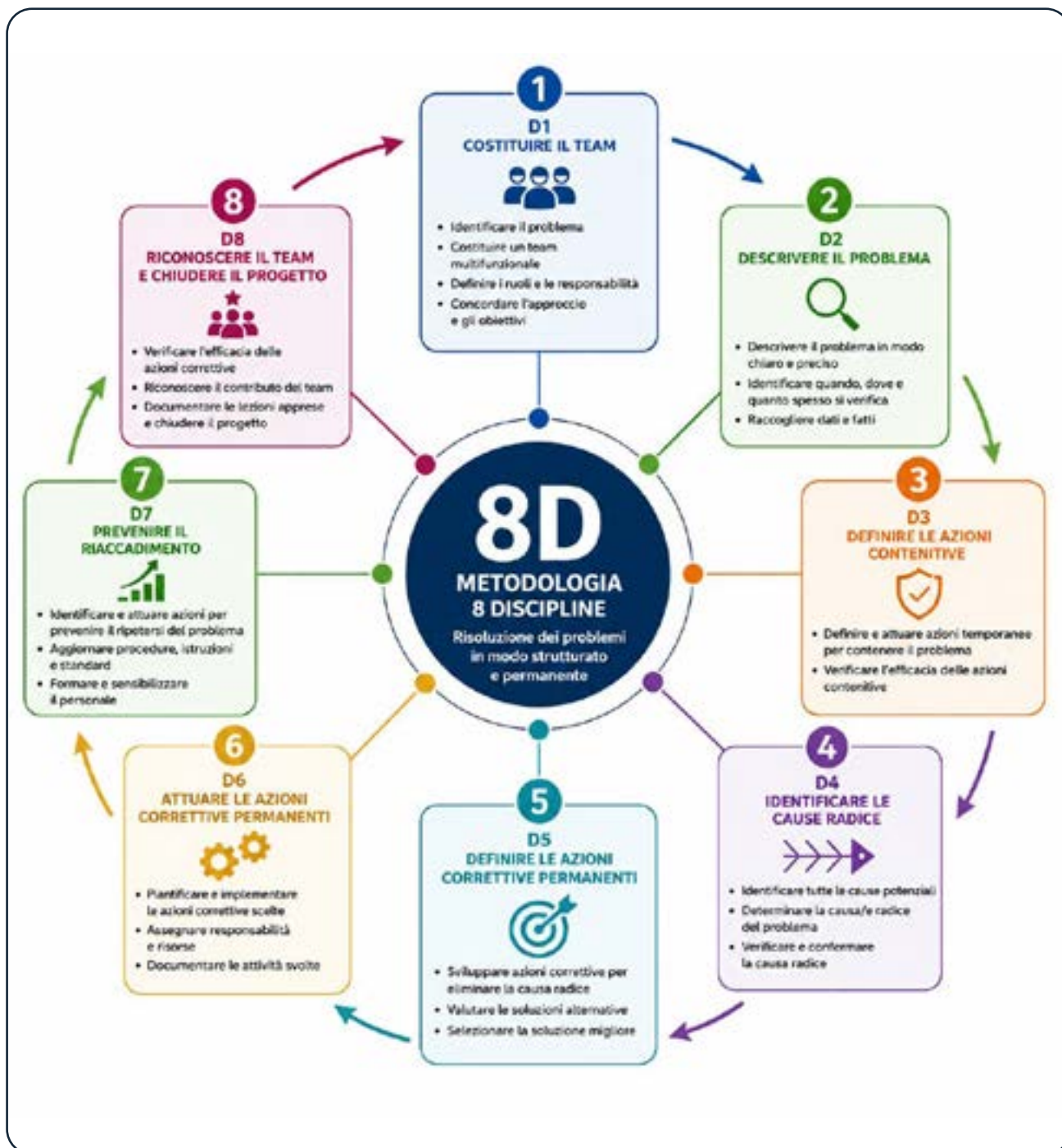


Figura 1 – Flusso metodologia 8D.

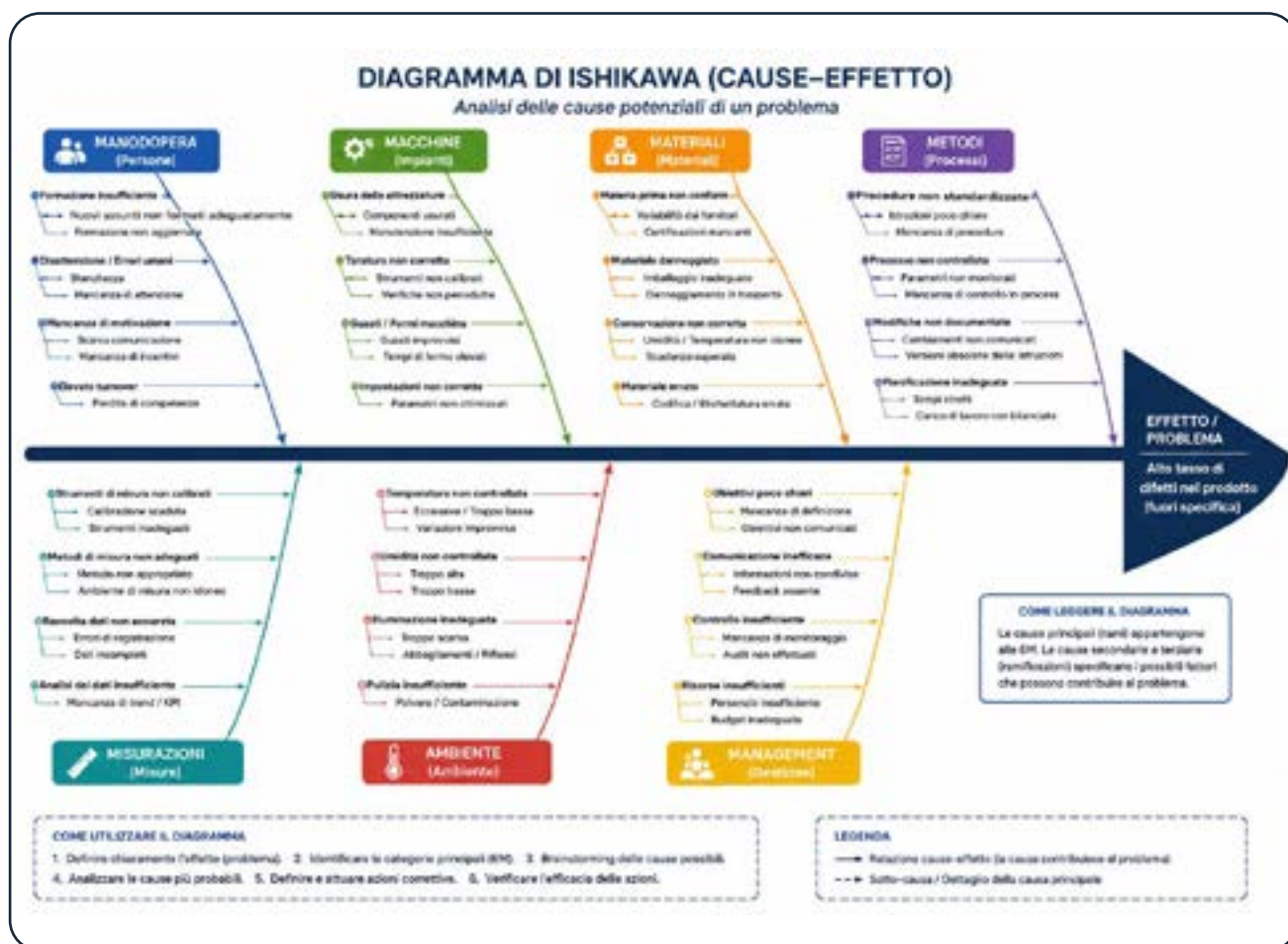


Figura 2 – Diagramma di Ishikawa.

L'Ishikawa, o diagramma causa-effetto, è uno strumento di analisi utilizzato per l'identificazione sistematica delle cause di un problema. Attraverso un processo strutturato di brainstorming, il gruppo di lavoro individua le possibili cause potenziali, che vengono successivamente confermate o escluse mediante delle attività di investigation e analisi mirate. Questo metodo consente di orientare l'attenzione sulle cause radice, facilitando la comprensione dei fattori che contribuiscono in modo significativo al verificarsi dell'evento osservato.

con ripercussioni significative sulla continuità operativa, sulla qualità e sui costi. In ambito domestico, per esempio, può manifestarsi nel blocco del ciclo di lavaggio della lavatrice. Pur nella diversa complessità dei due contesti, la logica di gestione del problema rimane sostanzialmente invariata.

La fase iniziale prevede la segnalazione tempestiva dell'evento e l'adozione di prime misure di contenimento (D0), ad esempio l'arresto controllato della linea o l'interruzione del funzionamento della lavatrice, con l'obiettivo di limitarne l'impatto e mettere in sicurezza il processo o l'utilizzo domestico. Segue la definizione del gruppo di lavoro (D1): in ambito industriale, un

team multidisciplinare con un leader e uno sponsor; nel contesto quotidiano, l'utente stesso, eventualmente supportato da un familiare. In entrambi i casi, una chiara assegnazione dei ruoli favorisce un intervento ordinato ed efficace.

La fase di descrizione del problema (D2) richiede la raccolta di informazioni oggettive e la delimitazione del perimetro dell'evento; a tale scopo, può essere impiegata la matrice Is / Is Not, utile a distinguere ciò che è accaduto da ciò che non è accaduto, dove e in quali condizioni. Ad esempio, l'assenza d'acqua può risultare totale o parziale, costante o intermittente, limitata a una sola linea o estesa a più utenze, oppure mani-

festarsi solo con l'accensione della spia di mancata alimentazione idrica della lavatrice, pur in presenza di regolare flusso sul resto dell'impianto idrico domestico. Seguono le azioni di contenimento (D3), orientate a ridurre l'impatto immediato e, quando possibile, a ripristinare una funzionalità provvisoria del sistema, mediante soluzioni temporanee quali un bypass idrico in impianto o la verifica del livello di alimentazione idrica nell'elettrodomestico.

Dalla causa radice alla prevenzione

L'analisi della causa radice (D4) viene condotta, in entrambi i contesti, attraverso un approccio strutturato che può avvalersi del diagramma di Ishikawa, utile a identificare, mediante un brainstorming multidisciplinare, le possibili cause dell'evento, quali la rottura di una tubazione, il guasto di una valvola, l'ostruzione di un filtro o la mancanza di manutenzione. Sulla base di tali ipotesi, si definiscono specifiche azioni investigative finalizzate a raccogliere evidenze oggettive, confermare o escludere le diverse alternative causali e ricostruire la catena logica degli accadimenti. Questo processo consente di distinguere in modo chiaro tra le cause tecniche, ovvero gli elementi materiali, operativi o funzionali che hanno generato direttamente l'evento, e le cause di sistema, intese come le debolezze organizzative, procedurali o gestionali che ne hanno favorito l'insorgenza o ne hanno impedito la tempestiva intercettazione. Tra le cause tecniche, ad esempio, possono rientrare una tubazione non idonea al servizio richiesto o una disposizione impiantistica non coerente con le condizioni operative, con conseguente piegatura o rottura del componente; tra le cause di sistema, invece, possono essere ricondotte la mancata esecuzione di controlli periodici e l'assenza di un piano di manutenzione adeguato.

Una volta individuate le cause, si definiscono e si verificano le azioni correttive permanenti (D5-D6), ad esempio la sostituzione del tratto di tubazione danneggiato o della valvola difettosa della lavatrice, seguita dalla verifica del completo ripristino della funzionalità. A tali interventi seguono le azioni preventive (D7), finalizzate a ridurre la probabilità di recidiva e a rafforzare l'affidabilità complessiva del sistema, sia esso produttivo o domestico, attraverso controlli periodici, manutenzione programmata e verifica preventiva delle condizioni operative.

Trasformare l'esperienza in conoscenza

Infine, la fase di chiusura e capitalizzazione dell'esperienza (D8) consente di formalizzare le lesson learned e di trasformare l'evento in un'occasione di apprendimento organizzativo o personale, ad esempio mediante la condivisione del report con altre linee o sedi industriali, oppure attraverso la valorizzazione dell'esperienza in ambito familiare per prevenire eventi analoghi. In questa prospettiva, la metodologia 8D dimostra la propria natura trasversale: un quadro metodologico unico, capace di guidare la gestione dei problemi in ambiti diversi, dalla complessità industriale alla semplicità della vita quotidiana. Il suo principale valore risiede inoltre nella capacità di promuovere un'analisi completa e multidimensionale della problematica, integrando aspetti tecnici, organizzativi e comportamentali. Favorendo, così, una comprensione più profonda dell'evento e delle condizioni che ne hanno determinato la comparsa.

Considerazioni

L'analisi dei due casi, industriale e quotidiano, evidenzia come la metodologia 8D mantenga una struttura logica sostanzialmente invariata, pur applicandosi a contesti diversi per complessità e conseguenze. In entrambi gli scenari, il punto di partenza è un evento critico che richiede una risposta tempestiva e organizzata; la fase di analisi, a sua volta, non si limita alla gestione del sintomo, ma mira a ricostruire la sequenza degli accadimenti, delimitare il problema e individuare la causa radice.

Le analogie tra i due contesti sono significative anche sul piano metodologico. Sia in ambito industriale sia nella vita quotidiana, l'efficacia dell'intervento dipende dalla capacità di distinguere tra misure di contenimento immediate e azioni correttive permanenti, evitando approcci esclusivamente empirici. Inoltre, la struttura dell'8D consente di separare le cause tecniche dalle fragilità organizzative che favoriscono la ricorrenza dell'evento, rendendo possibile un miglioramento che riguarda non soltanto il singolo episodio, ma anche il processo o il comportamento sottostante.

Il contributo più rilevante della metodologia risiede nella sua funzione preventiva. Attraverso l'analisi causale, la definizione di azioni preventive e la formalizzazione delle lesson learned, l'8D trasforma l'esperienza del guasto in conoscenza strutturata e trasferibile. In questo sen-

so, la metodologia non si limita alla risoluzione dell'evento contingente, ma promuove un apprendimento continuo che rafforza l'affidabilità del sistema e consolida una cultura del miglioramento continuo, applicabile sia nei contesti industriali sia nella vita quotidiana.

Conclusioni

La metodologia 8D si conferma con un approccio di elevata efficacia, non soltanto nella gestione delle non conformità e delle problematiche complesse in ambito industriale, ma anche come modello trasversale di problem solving applicabile a contesti differenti, inclusa la vita quotidiana. Il suo valore distintivo risiede nella capacità di convertire un evento critico in un percorso strutturato di analisi, comprensione e miglioramento, capace di produrre effetti non limitati alla risoluzione del caso specifico.

L'8D supera una logica meramente reattiva, promuovendo un approccio sistemico, consapevole e orientato alla prevenzione della ricorrenza. In tale prospettiva, ogni cri-

ticità rappresenta un'opportunità per rafforzare il sistema, accrescerne la robustezza e ridurre la vulnerabilità rispetto a eventi futuri. L'8D si configura pertanto non solo come uno strumento di risoluzione dei problemi, ma come un vero e proprio dispositivo di apprendimento continuo, in grado di trasformare l'errore in consapevolezza e la criticità in un'occasione di crescita per il sistema, per le persone e per i contesti in cui esse operano.

Keywords: metodologia 8D, problem solving, analisi delle cause, causa radice, root cause analysis, diagramma di Ishikawa, matrice Is/Is Not, azioni di contenimento, azioni correttive, azioni preventive, gestione delle non conformità, miglioramento continuo, affidabilità dei processi, prevenzione delle recidive, lesson learned, apprendimento organizzativo, qualità, manutenzione, processi industriali, problem solving quotidiano.

L'autrice*

Quality Management System, STMicroelectronics

CONTROLLORI

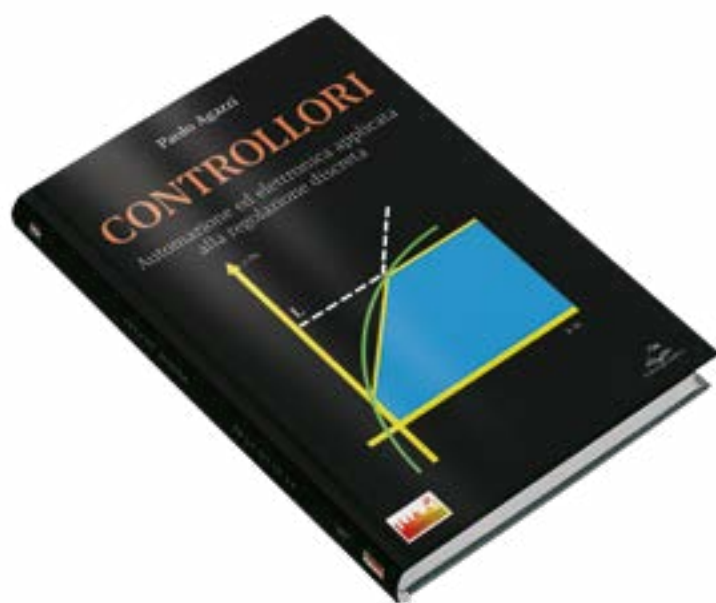
Automazione ed elettronica applicata alla Building Automation

Autore: Paolo Agazzi

Prezzo: 26,00 €

Pagine: 224

Questo libro offre un viaggio approfondito nel mondo della regolazione per impianti tecnologici, partendo da una visione elettrica d'insieme (visione macro di sistema) con schemi funzionali chiari e dettagliati. Progressivamente, il lettore viene guidato nel "cuore" di queste regolazioni, esplorando il processo di progettazione e analizzando nel dettaglio gli schemi elettrici di funzionamento (con progetti originali) delle apparecchiature. Un testo fondamentale per chi vuole comprendere e progettare i sistemi di controllo, non solo nella Building Automation ma anche nell'Automazione generica.



PER L'ACQUISTO

<https://libri.editorialedelfino.it/prodotto/controllori/>





Il Clusit, nato nel 2000 presso il Dipartimento di Informatica dell'Università degli Studi di Milano, è la più numerosa ed autorevole associazione italiana nel campo della sicurezza informatica. Oggi rappresenta oltre 500 organizzazioni, appartenenti a tutti i settori del Sistema-Paese.

Gli obiettivi

- Diffondere la cultura della sicurezza informatica presso le Aziende, la Pubblica Amministrazione e i cittadini.
- Partecipare alla elaborazione di leggi, norme e regolamenti che coinvolgono la sicurezza informatica, sia a livello nazionale che europeo.
- Contribuire alla definizione di percorsi di formazione per la preparazione e la certificazione delle diverse figure professionali operanti nel settore della sicurezza.
- Promuovere l'uso di metodologie e tecnologie che consentano di migliorare il livello di sicurezza delle varie realtà



CYBERSECURITY INDUSTRIALE: QUATTRO FALSI MITI DA SUPERARE



a cura di
Exor International

NIS2, Cyber Resilience Act, Regolamento Macchine e IEC 62443 stanno trasformando la cybersecurity in un requisito strutturale per macchine, software e servizi digitali. Quattro convinzioni ancora diffuse tra costruttori e system integrator vengono messe a confronto con il nuovo quadro normativo e tecnologico. Oltre a raggiungere la conformità, la vera sfida consiste nel garantire sicurezza, aggiornabilità e protezione della macchina durante l'intero ciclo di vita.

SOMMARIO

- **Introduzione**
- **Mito #1: "La NIS2 riguarda solo le grandi aziende"**
- **Mito #2: "Il Cyber Resilience Act è solo un problema dei produttori software"**
- **Mito #3: "La cybersecurity non ha nulla a che fare con la marcatura CE"**
- **Mito #4: "Le certificazioni IEC 62443 sono solo un bollino"**
- **Oltre la conformità: la vera sfida è il ciclo di vita**

Introduzione

La cybersecurity industriale è entrata stabilmente nelle strategie di progettazione e gestione delle macchine. Non è più una materia riservata ai responsabili IT o agli specialisti dell'automazione: NIS2, Cyber Resilience Act (CRA), Regolamento Macchine e standard IEC 62443 stanno ridefinendo il modo in cui prodotti, software e servizi digitali devono essere sviluppati, aggiornati e mantenuti durante l'intero ciclo di vita.

Eppure, intorno a questi temi persistono convinzioni errate che rischiano di rallentare il percorso di adeguamento delle aziende e di ridurre la cybersecurity a un semplice adempimento normativo. L'esperienza maturata da Exor e Corvina nelle attività di sviluppo, certificazione e formazione conferma invece che uno degli aspetti decisivi è la diffusione di una corretta cultura della cybersecurity industriale. Superare i falsi miti significa comprendere che sicurezza,



conformità e continuità operativa sono ormai elementi strettamente connessi.

Mito #1: “La NIS2 riguarda solo le grandi aziende”

La Direttiva NIS2 si rivolge principalmente alle organizzazioni essenziali e importanti attive in settori strategici quali manifatturiero, energia, trasporti, infrastrutture digitali e sanità. Dopo il recepimento nazionale dell'ottobre 2024, gli obblighi di notifica degli incidenti al CSIRT Italia sono operativi dal 1° gennaio 2026.

Entro ottobre 2026, invece, i soggetti interessati devono attuare le misure di sicurezza di base definite dall'Agenzia per la Cybersicurezza Nazionale.

Il quadro di riferimento è oggi aggiornato dalla Determinazione n. 379907/2025, applicabile dal 15 gennaio 2026, che sostituisce la precedente Determinazione n. 164179/2025.

Le aziende coinvolte devono adottare misure adeguate per la gestione del rischio cyber, la risposta agli incidenti, la continuità operativa, la sicurezza della supply chain e il trattamento delle vulnerabilità, oltre a garantire la formazione del personale e un efficace controllo degli accessi e dell'autenticazione.

Gli effetti della Direttiva, tuttavia, si estendono ben oltre il perimetro dei soggetti direttamente interessati. Molti costruttori di macchine e system integrator, pur non rientrando formalmente nell'ambito di applicazione della NIS2, operano nella catena di fornitura di clienti obbligati a rispettarne i requisiti.

Dovranno quindi essere sempre più preparati a fornire evidenze di sicurezza e documentazione tecnica, dimostrare l'esistenza di processi strutturati per la gestione delle vulnerabilità e supportare audit e assessment condotti dai committenti.

La risposta di Exor e Corvina non si limita alla componente tecnologica. A livello di gruppo la holding HOLDEX ha costituito un team dedicato alla governance della cybersecurity, affiancando alle competenze specialistiche processi di vulnerability management, attività formative e una gestione coordinata della conformità. Sul piano operativo, Corvina mette a disposizione la gestione centralizzata di utenti e ruoli, l'autenticazione multifattore, la registrazione delle attività attraverso audit trail, la gestione documentale e il monitoraggio dell'infrastruttura digitale. Funzioni che contribuiscono a costruire processi organizzativi e tecnici coerenti con i principi introdotti dalla NIS2.

Mito #2: “Il Cyber Resilience Act è solo un problema dei produttori software”

Il Cyber Resilience Act si applica ai prodotti con elementi digitali connessi, direttamente o indirettamente, a reti o dispositivi. Da settembre 2026 sono applicabili gli obblighi di notifica delle vulnerabilità attivamente sfruttate e degli incidenti gravi, mentre la piena applicazione del Regolamento è prevista per dicembre 2027.. Il nuovo quadro normativo introduce principi e requisiti che comprendono Secure by Design, gestione delle vulnerabilità, monitoraggio post-market, aggiornamenti di sicurezza, configurazioni sicure per impostazione predefinita, protezione dell'integrità e della riservatezza dei dati e adeguata documentazione tecnica di cybersecurity.

Tra gli obblighi previsti rientrano inoltre la definizione e dichiarazione del periodo di supporto del prodotto e la predisposizione di una Software Bill of Materials (SBOM), che consente di documentare i componenti software rilevanti e le relative dipendenze.

Il CRA non riguarda quindi soltanto chi sviluppa software. Per un costruttore di macchine, un aspetto particolarmente rilevante è quello della modifica sostanziale: chi effettua una modifica sostanziale a un prodotto con elementi digitali di terzi e lo rende disponibile sul mercato è considerato fabbricante ai sensi del CRA, assumendo i relativi obblighi.

Il cambiamento più significativo riguarda la dimensione temporale della sicurezza. Il CRA non impone soltanto che un prodotto sia sicuro nel momento in cui viene immesso sul mercato, ma richiede che tale condizione sia mantenuta durante il suo ciclo di vita.

Il fabbricante deve quindi essere in grado di individuare nuove vulnerabilità, distribuire tempestivamente patch e aggiornamenti, conservare le necessarie evidenze documentali e monitorare nel tempo il comportamento dei prodotti installati.

Le nuove piattaforme Exor rispondono a questi requisiti integrando Secure Boot, verifica delle firme applicative, partizioni dati cifrate, gestione di utenti e ruoli, firewall, logging e monitoraggio, oltre a una policy pubblica per la divulgazione coordinata delle vulnerabilità. JMobile completa queste protezioni con LDAP, Audit Trail, firma digitale dei progetti, cifratura dei pacchetti e protocolli sicuri quali TLS, HTTPS e FTPS.

Corvina consente di estendere queste capacità all'intero ciclo di vita del prodotto. Il Security Scanner supporta l'identificazione delle vulnerabilità, mentre Corvina Edge

Figura 1 – Corvina Edge Manager, gestione degli edge per i costruttori di macchine.



Manager permette di distribuire centralmente patch e aggiornamenti OTA. A queste funzioni si aggiungono un repository centralizzato per software e documentazione e il monitoraggio della flotta installata. La cybersecurity diventa così un processo continuo, che accompagna il prodotto anche dopo la commercializzazione.

Mito #3: “La cybersecurity non ha nulla a che fare con la marcatura CE”

Con il Regolamento Macchine (UE) 2023/1230, pienamente applicabile dal 20 gennaio 2027, la cybersecurity entra ufficialmente tra i requisiti che concorrono alla sicurezza delle macchine. Il nuovo quadro normativo richiede di considerare la protezione dagli accessi non autorizzati, l'integrità delle funzioni di sicurezza e la valutazione del rischio cyber, insieme a logging, tracciabilità e documentazione tecnica. Un attacco informatico capace di alterare il comportamento della macchina non costituisce infatti soltanto un problema di protezione dei dati, ma può compromettere direttamente la sicurezza di operatori, impianti e processi produttivi. L'approccio adottato da Exor e Corvina combina protezioni integrate nei dispositivi e servizi digitali per la gestione dell'infrastruttura. Le misure comprendono servizi disabilitati per impostazione predefinita, applicazione del principio del privilegio minimo, firewall integrato, separazione delle funzioni, autenticazione forte e registrazione degli eventi. Queste caratteristiche contribuiscono a ridurre la superficie di attacco e a garantire un maggiore controllo sulle operazioni eseguite localmente o da remoto.

Un esempio significativo è la possibilità di gestire l'assistenza remota mediante un interruttore hardware o software. Il costruttore o l'utilizzatore finale può così stabilire quando autorizzare effettivamente la connessione, evitando che il canale di accesso rimanga disponibile senza necessità. È un caso concreto nel quale cybersecurity e safety convergono, diventando parti complementari dello stesso requisito di sicurezza e, di conseguenza, del percorso di conformità necessario per la marcatura CE.

Mito #4: “Le certificazioni IEC 62443 sono solo un bollino”

La famiglia di norme IEC 62443 rappresenta oggi uno dei principali riferimenti internazionali per la cybersecurity dei sistemi OT. Le certificazioni non costituiscono un semplice riconoscimento formale, ma attestano l'adozione di processi e requisiti verificabili. Per questo motivo, un numero crescente di aziende le utilizza come criterio per valutare e selezionare componenti, piattaforme e fornitori destinati agli impianti industriali. La certificazione IEC 62443-4-1 riguarda il processo di sviluppo e verifica che il produttore applichi un Secure Product Development Lifecycle strutturato. Il percorso comprende la definizione dei requisiti di sicurezza, la progettazione e l'implementazione sicure, le attività di testing, la gestione delle vulnerabilità e degli aggiornamenti e il controllo della documentazione. Exor ha già ottenuto questa certificazione e continua a investire nella formazione dei team coinvolti nello sviluppo, affinché la sicurezza venga integrata in ogni fase e non aggiunta soltanto al termine della progettazione.

La IEC 62443-4-2 valuta invece le caratteristiche tecniche di sicurezza dei singoli componenti. I requisiti riguardano identificazione e autenticazione, controllo degli accessi, integrità del sistema, riservatezza dei dati, monitoraggio degli eventi e disponibilità delle funzioni. Il percorso verso la certificazione IEC 62443-4-2 rappresenta quindi il naturale completamento dell'approccio Secure by Design già adottato nelle piattaforme hardware, software ed edge di Exor, collegando la solidità del processo di sviluppo alla sicurezza effettivamente incorporata nei prodotti.

Oltre la conformità: la vera sfida è il ciclo di vita

Il punto non è semplicemente superare un audit, ottenere una certificazione o adempiere formalmente a un requisito normativo. NIS2, Cyber Resilience Act, Regolamento Macchine e IEC 62443 convergono su una questione più sostanziale: come garantire che una macchina rimanga sicura, controllabile e aggiornabile durante tutta la sua vita operativa. I quattro miti esaminati mostrano infatti che la cybersecurity non riguarda soltanto le grandi aziende o i produttori software, non è separata dalla marcatura CE e non può essere ridotta a un bollino da esibire.

La risposta richiede un approccio integrato, capace di collegare tecnologia, processi e responsabilità organizzative. L'hardware progettato secondo i principi Secure by Design costituisce la prima linea di protezione; le funzionalità avanzate di JMobile rafforzano autentica-

zione, integrità, cifratura e tracciabilità; i servizi cloud e la gestione centralizzata di Corvina consentono di monitorare la flotta installata e distribuire patch e aggiornamenti; i processi certificati secondo IEC 62443 garantiscono infine che la sicurezza sia affrontata in modo strutturato, verificabile e ripetibile.

La cybersecurity diventa così una responsabilità permanente, che accompagna la macchina dalla definizione dei requisiti alla progettazione, dalla messa in servizio alla manutenzione, fino al post-vendita e alla gestione delle vulnerabilità emergenti.

È questo il vero passaggio oltre la conformità: trasformare la sicurezza da adempimento occasionale a caratteristica durevole del prodotto e del servizio.

www.exorint.com



Keywords: cybersecurity industriale, industrial cybersecurity, NIS2, Cyber Resilience Act, CRA, Regolamento Macchine, IEC 62443, IEC 62443-4-1, IEC 62443-4-2, Secure by Design, sicurezza OT, costruttori di macchine, system integrator, supply chain, vulnerability management, gestione delle vulnerabilità, sicurezza del prodotto, marcatura CE, sicurezza delle macchine, autenticazione multifattore, aggiornamenti OTA, incident response, ciclo di vita del prodotto, Exor International, Corvina, JMobile, HOLDEX



Figura 2 – L'architettura Exor combina dispositivi IoT sviluppati secondo un processo certificato ISA/IEC 62443-4-1 e la piattaforma cloud Corvina, gestita in un sistema di gestione certificato ISO/IEC 27001 che include il ciclo di vita di sviluppo sicuro. L'approccio Secure by Design attraversa l'intera catena, dal dispositivo al cloud, con accesso remoto sicuro e latenza controllata.

APPLICATION OF AUTOMATION STUDIO® FOR INTEGRATED MULTI-DOMAIN MODELLING IN MECHATRONIC SYSTEMS



a cura di
Filippo Mazzocato*,
Luigi Mazza**

Tre progetti didattici universitari mostrano come Automation Studio® possa integrare, in un unico ambiente di simulazione, modellazione meccanica, attuazione pneumatica, controllo e cinematica robotica. Dalla piattaforma elevatrice al pantografo 3D, fino al manipolatore basato sulla convenzione Denavit–Hartenberg, i casi applicativi collegano formulazioni teoriche e comportamento dinamico, evidenziando il valore della simulazione multidisciplinare nella formazione meccatronica.

CONTENTS

- Introduction
- Methodology
- Project 1 – Mechanism Manager
- Project 2 – Pantograph Lift
- Project 3 – Robotic Manipulator and Denavit–Hartenberg Implementation
- Conclusion

Abstract

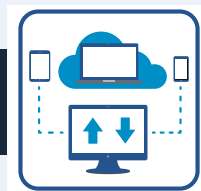
A technical synthesis of three university level projects integrating fluid power actuation, 3D mechanical assemblies, and robotic kinematics within a unique simulation framework.

Introduction

Modern mechatronic systems require the integration of mechanical structures, fluid power actuation, and control systems. In engineering education, however, these do-

main components are often taught separately, making it difficult for students to understand their interaction. Integrated simulation environments provide a unified framework where mechanical motion, actuation and control strategies can be analyzed simultaneously.

This work explores the use of the Automation Studio simulation environment as a support tool for teaching mechatronics engineering concepts. Through the development and implementation of



three practical projects, the study demonstrates how an integrated simulation platform can help to connect theoretical knowledge with practical system behavior, promoting a deeper understanding of engineering principles related to mechanical motion, fluid power actuation, and system control.

The first project (*Figure 1*) introduces the Mechanism Manager, a tool that allows the simulation of the kinematic and dynamic behavior of mechanical systems through the definition of joints and constraints between rigid bodies. This environment enables the interaction between actuators and mechanical structures to be modeled and analyzed within a two-dimensional multi-body environment.

The second project (*Figure 2*) focuses on the integration of three-dimensional mechanical models within the simulation environment. In particular, the study demonstrates the design and simulation of a mobile vertical platform based on a pantograph mechanism, combining 3D modeling with fluid-powered actuation, loads, and mechanical constraints.

Finally, the third project (*Figure 3*) explores the application of the Denavit–Hartenberg convention for the kinematic analysis of robotic manipulators. Through the implementation of rotation matrices and coordinate frame transformations, the project provides a visual and interactive representation of robotic arm motion within the simulation environment.

By combining mechanical modeling, fluid power simulation, and mathematical representations of robotic motion, these projects illustrate how integrated simulation tools can support the teaching and understanding of complex mechatronic systems.

Methodology

The methodology adopted in this work is based on the use of an integrated simulation environment capable of combining mechanical modeling, fluid power actuation, and control within a unified framework (*Figure 4*). Automation Studio enables multi-domain interaction through a consistent simulation in which mechanical structures, actuators, and control elements are analyzed simultaneously.

Mechanical systems are represented as assemblies of rigid bodies connected through kinematic constraints such as revolute and prismatic joints. The Mechanism Manager module defines these constraints and computes the kinematic and dynamic behavior of articulated mechanisms.

Fluid power actuators (pneumatic or hydraulic) are directly integrated into the mechanical model. The actuator forces are transmitted through the defined joints, allowing realistic simulation of motion generation under load. This coupling ensures consistency between actuator dynamics and mechanical constraints.

The environment also supports the implementation of external CAD geometries, enabling the construction of

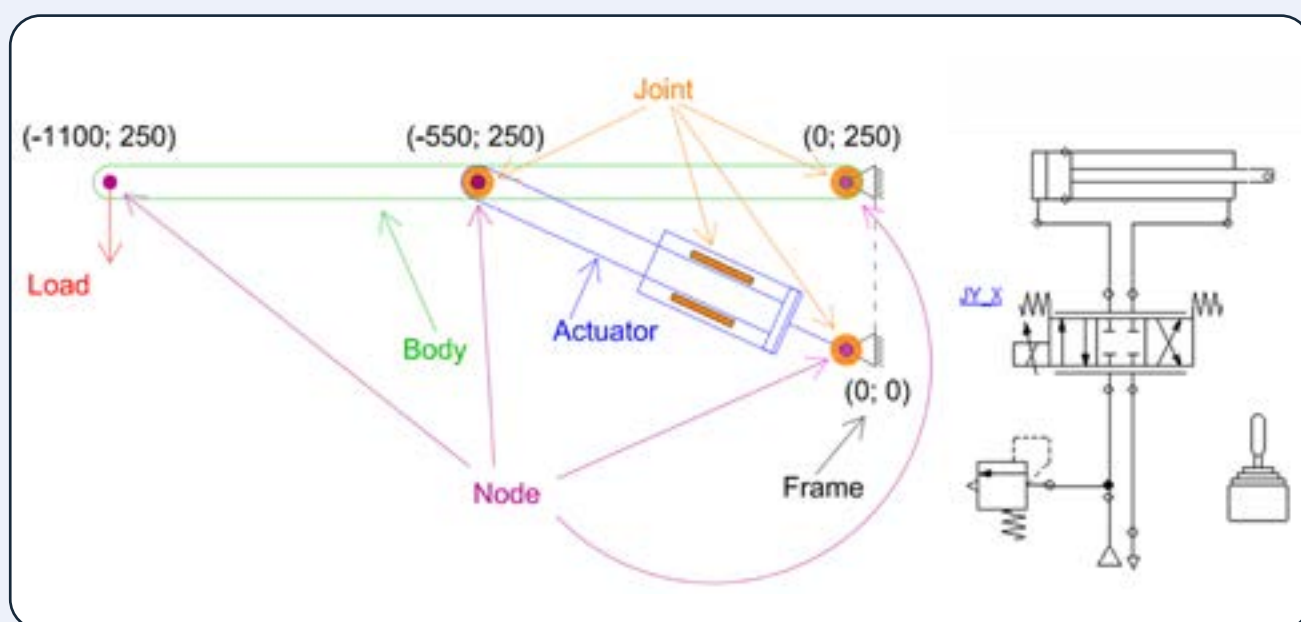


Figure 1 - First project - boom lift.

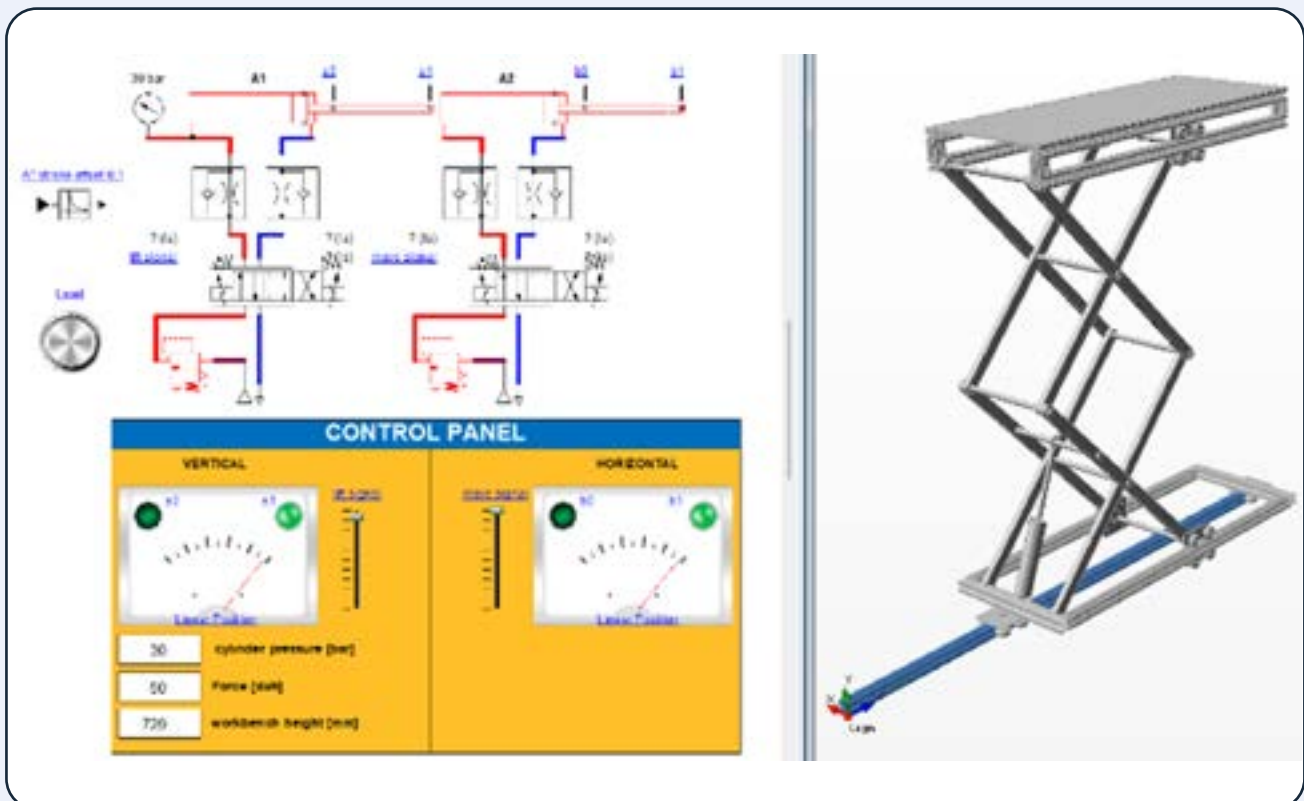


Figure 2 - Second project - pantograph lift.

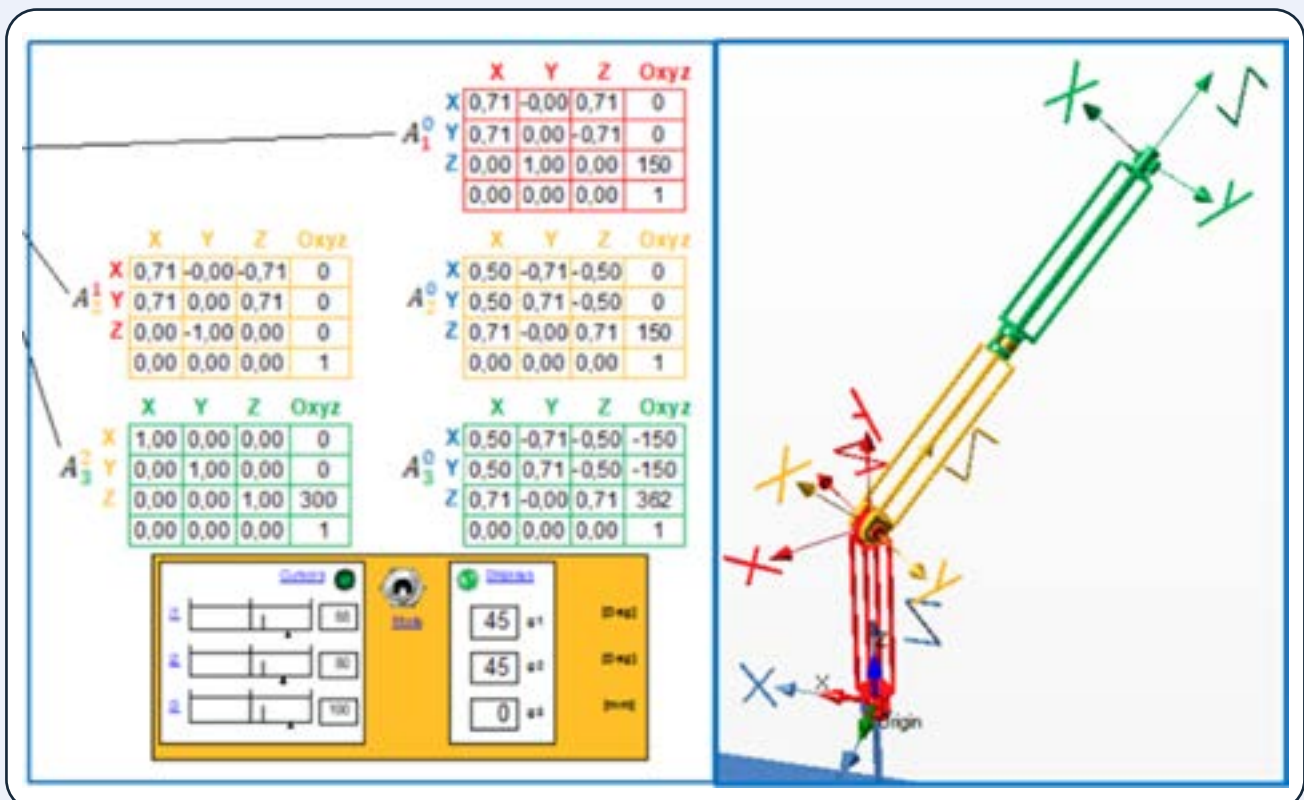


Figure 3 - Third project - DH convention.

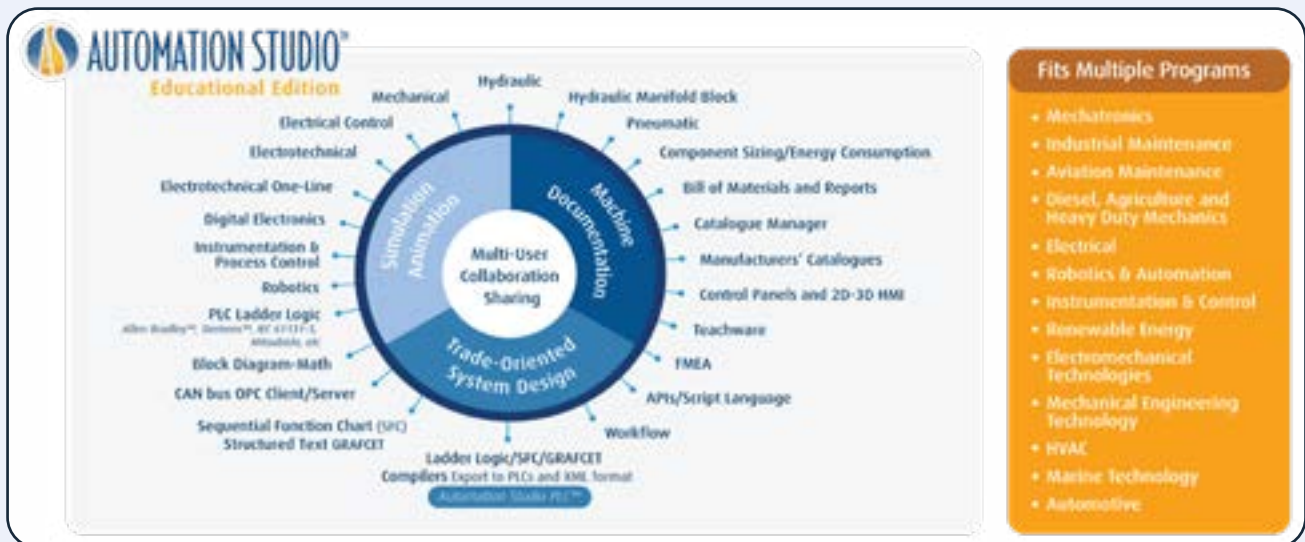


Figure 4 - Automation Studio multi-Technologies.

three-dimensional assemblies within the same modeling framework. In addition, mathematical models related to robotic kinematics can be implemented through Structured Text and control blocks, allowing dynamic visualization of homogeneous transformation matrices based on the Denavit–Hartenberg convention. This unified approach provides a direct connection between theoretical formulations, actuator behaviour and mechanical motion.

Project 1 – Mechanism Manager

The first project (Figure 5) introduces the use of the Mechanism Manager module to demonstrate the cou-

pling between mechanical systems and pneumatic actuation within a planar multi-body environment.

A boom lift mechanism is modelled, where the rotation of a rigid arm is driven by a pneumatic cylinder. The system consists of a fixed reference frame, a rigid boom, and an actuator connected through pivot and sliding joints. Mechanical elements are defined using frames, nodes, rigid bodies, and kinematic constraints. When integrated into the mechanism, the pneumatic actuator is automatically represented as a two-body system (cylinder and rod) connected by a sliding joint, ensuring compatibility with the multi-body formulation. External loads are applied to the boom, and dy-

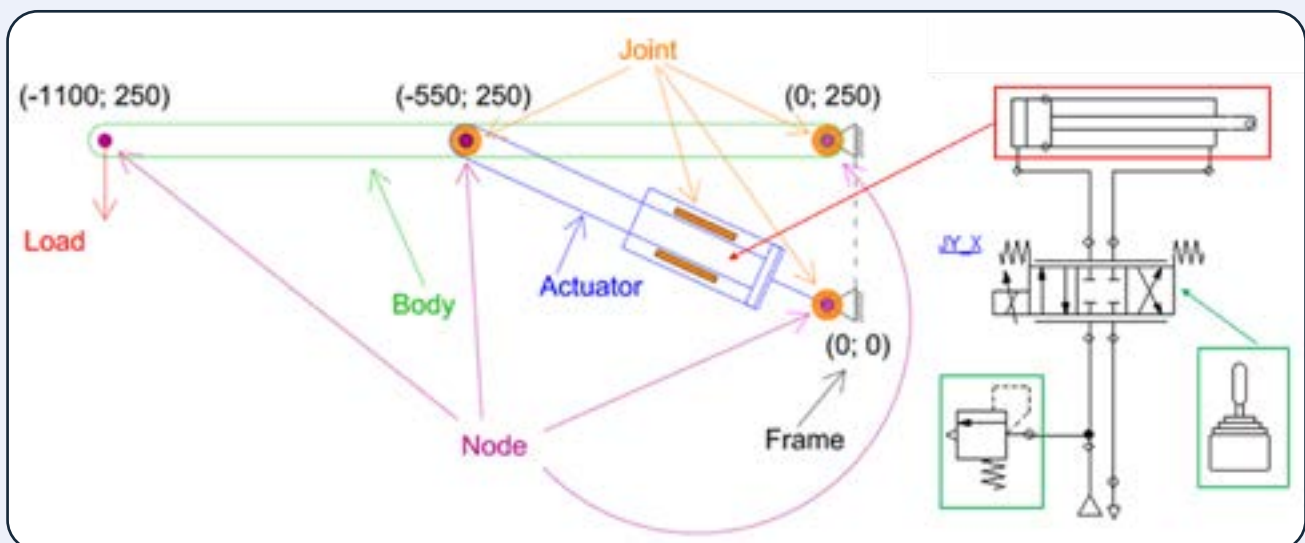


Figure 5 - First project – Boom lift and associated pneumatic circuit.

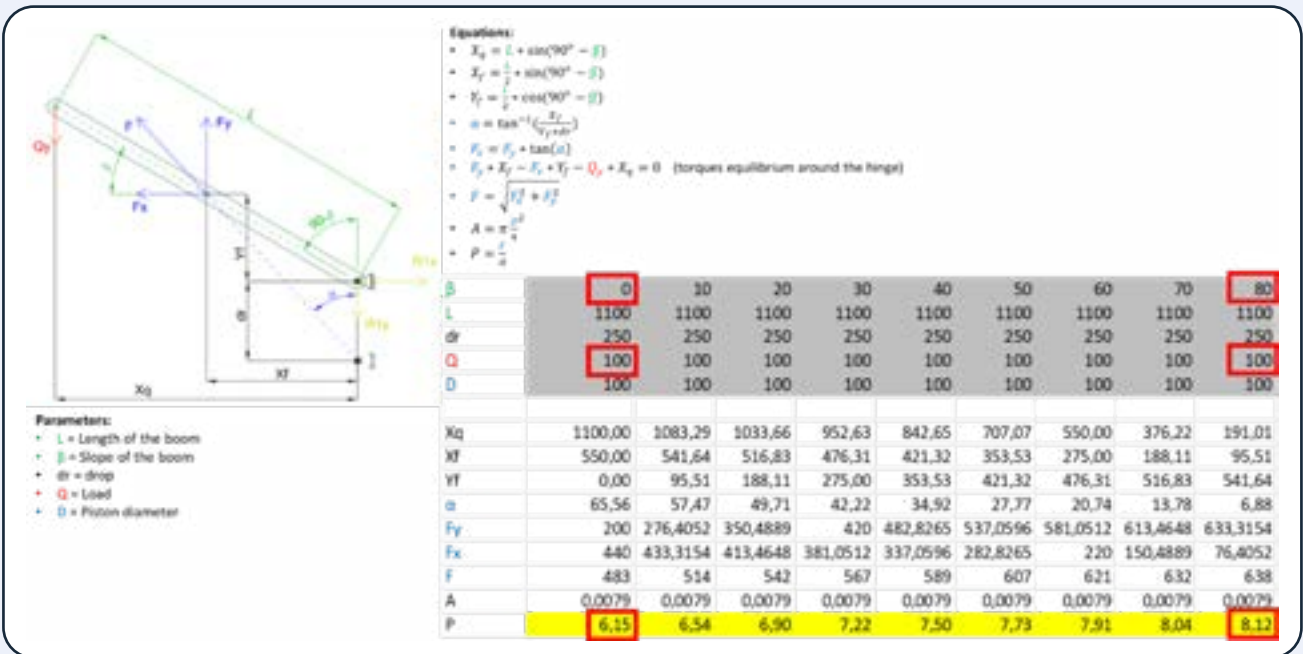


Figure 6 - Static equilibrium formulation.

dynamic simulations are performed to evaluate piston displacement, actuator pressure and angular motion. User interaction is enabled through a proportional valve controlled by a joystick interface, allowing real-time adjustment of pressure limits and observation of the resulting system response. To complement the dynamic analysis, a static equilibrium formulation is introduced (Figure 6). By evaluating torque balance about the boom hinge, the minimum actuator pressure required to lift the system under varying load conditions can be estimated.

During the simulation, it is also possible to observe oscillatory behavior caused by the compressibility of the pneumatic fluid. The boom slope can vary between 0 and 80 degrees, as an imposed constraint. A double check can be done through the plotter (Figure 7), which evaluates the extension of the actuator according to the internal pressure. This introductory example provides the modelling foundation required for the more advanced projects presented in the following sections, where the same modelling approach is extended to more complex three-dimensional mechanisms and robotic systems.

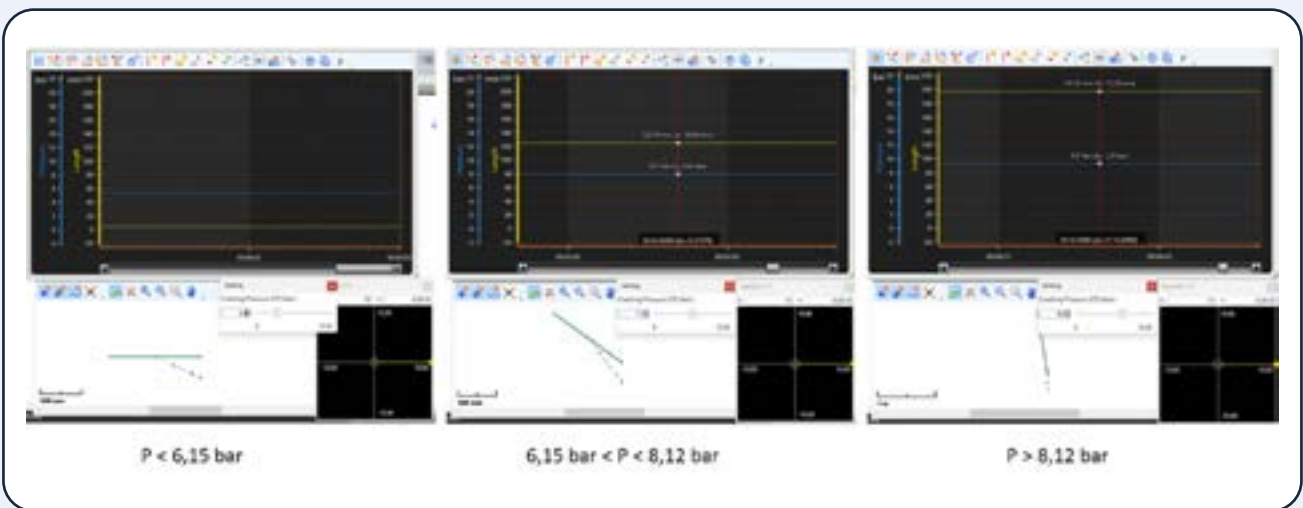


Figure 7 - Double check with the plotter.

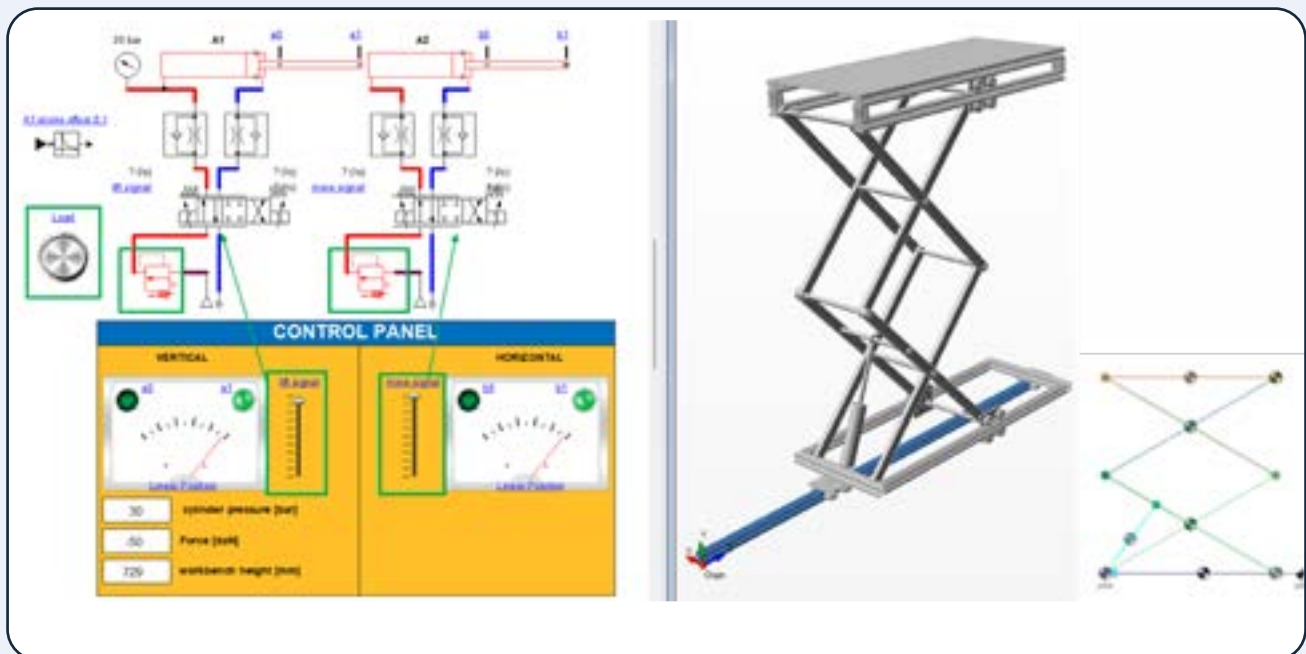


Figure 8 - Second project - Pantograph lift.

Project 2 – Pantograph Lift

The second project (Figure 8) extends the proposed modelling approach to a three-dimensional mechatronic system integrating CAD geometry, multi-body mechanics, fluid power actuation, and user interaction.

A pantograph lift mechanism was designed in SolidWorks (Figure 9) and imported into the Automation Studio 3D environment. The assembly was completed by defining geometric constraints and kinematic joints (pivot and sliding) to reproduce the mechanical behaviour of

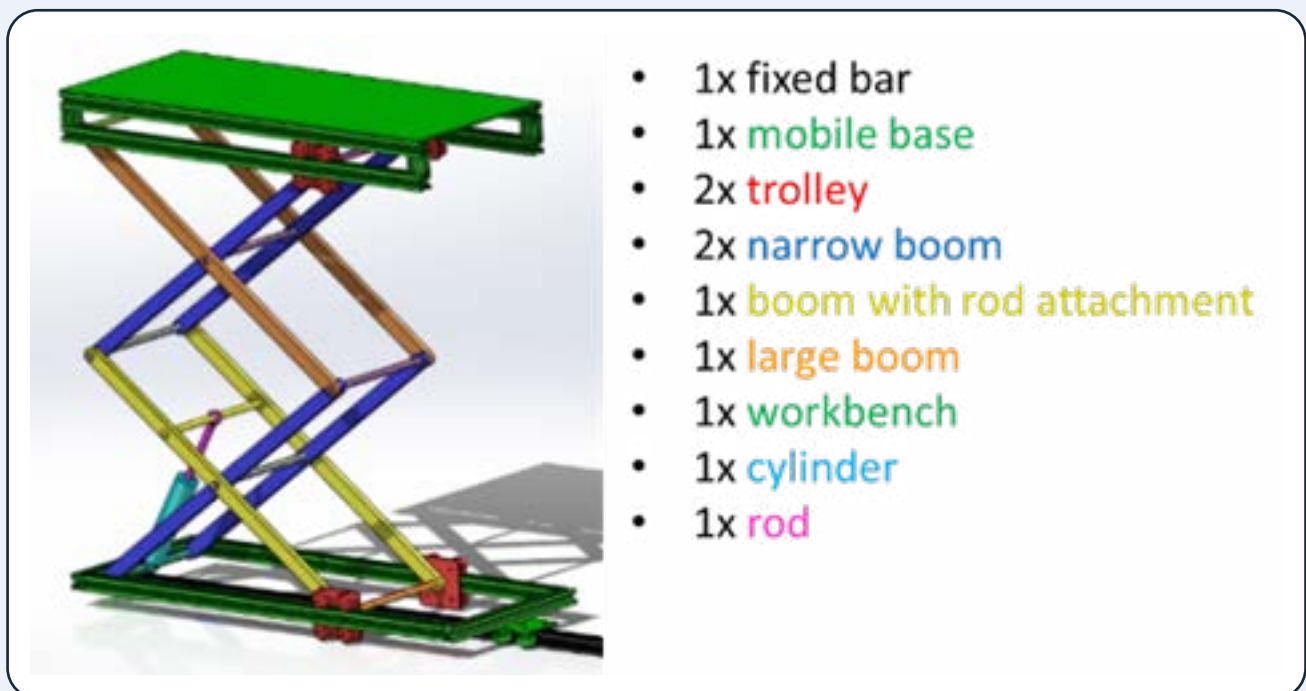


Figure 9 - Drawings made with Solid Works.

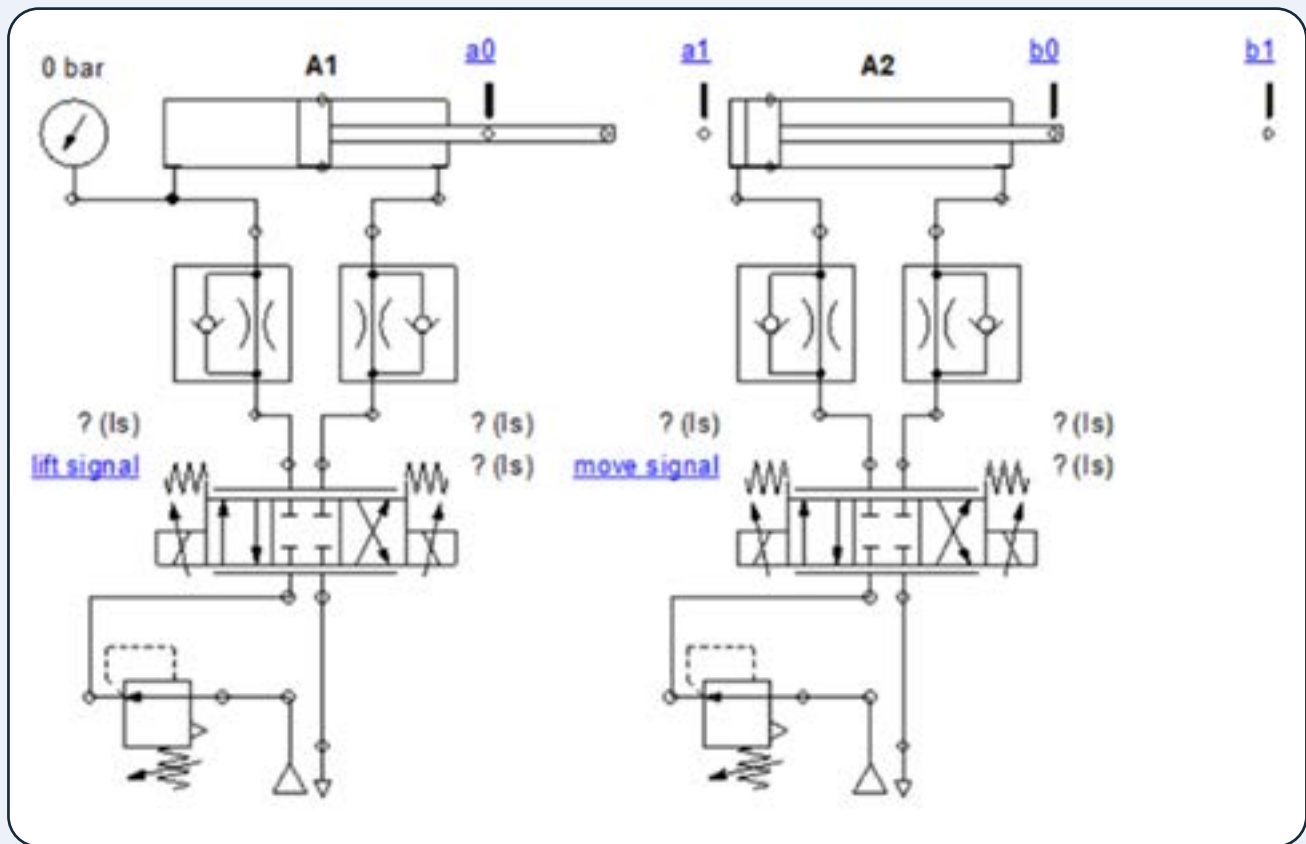


Figure 10 - Pneumatic actuators.

the scissor structure. The 3D model was then linked to the Mechanism Manager, where a simplified rigid-body representation enabled dynamic computation of motion under actuator forces and external loads.

Two pneumatic actuators were integrated into the system (Figure 10): one controlling the vertical extension of the pantograph mechanism and the other driving the horizontal translation of the mobile base.

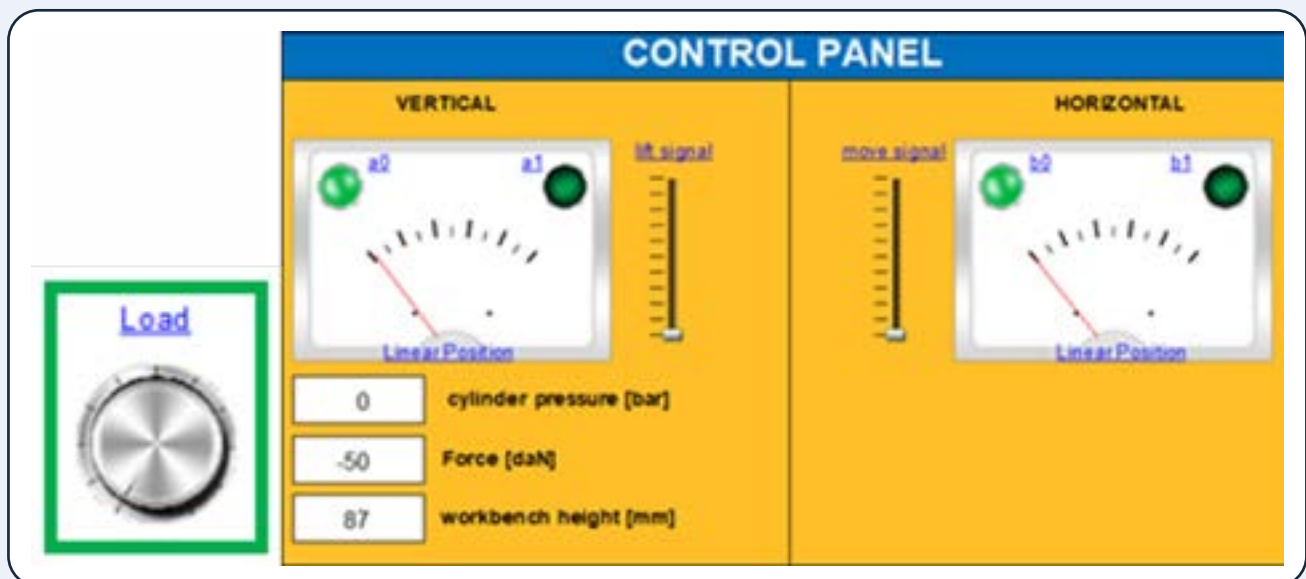


Figure 11 - Load Knob + Control Panel.

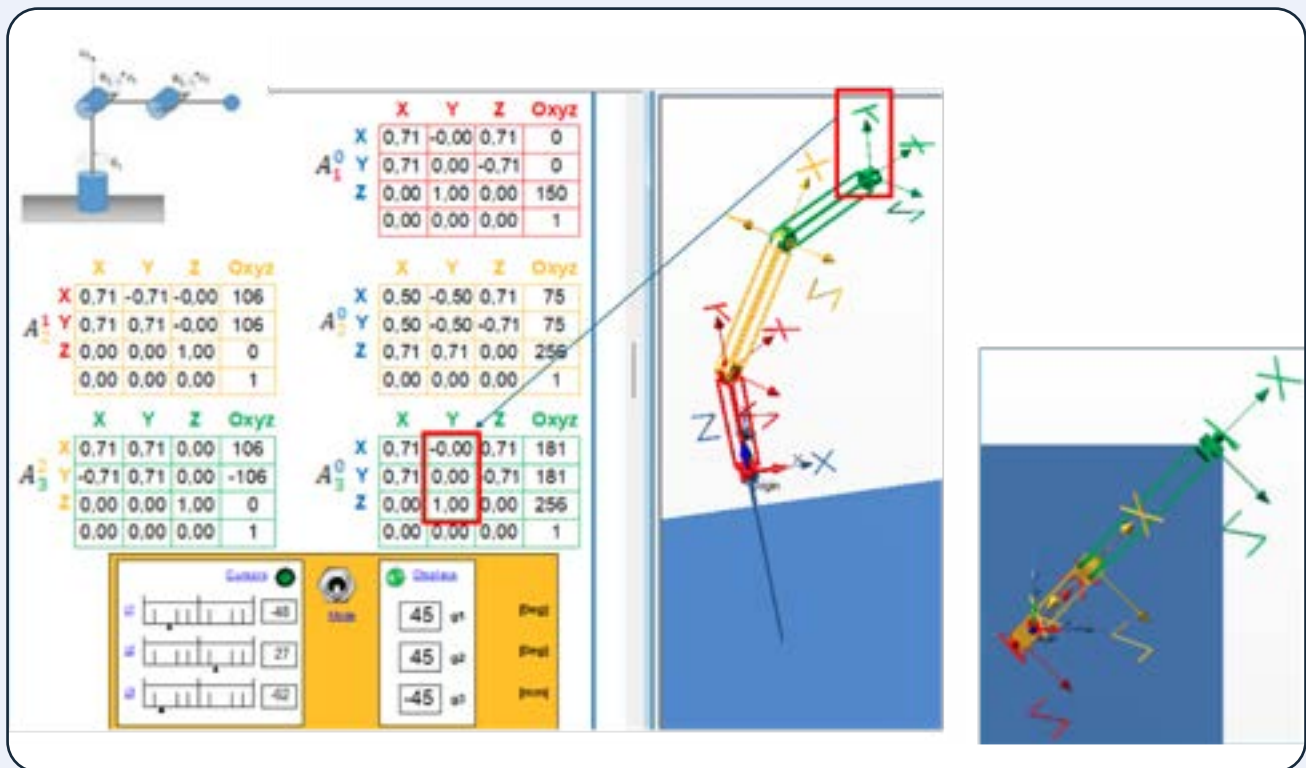


Figure 12 - Third project - DH convention.

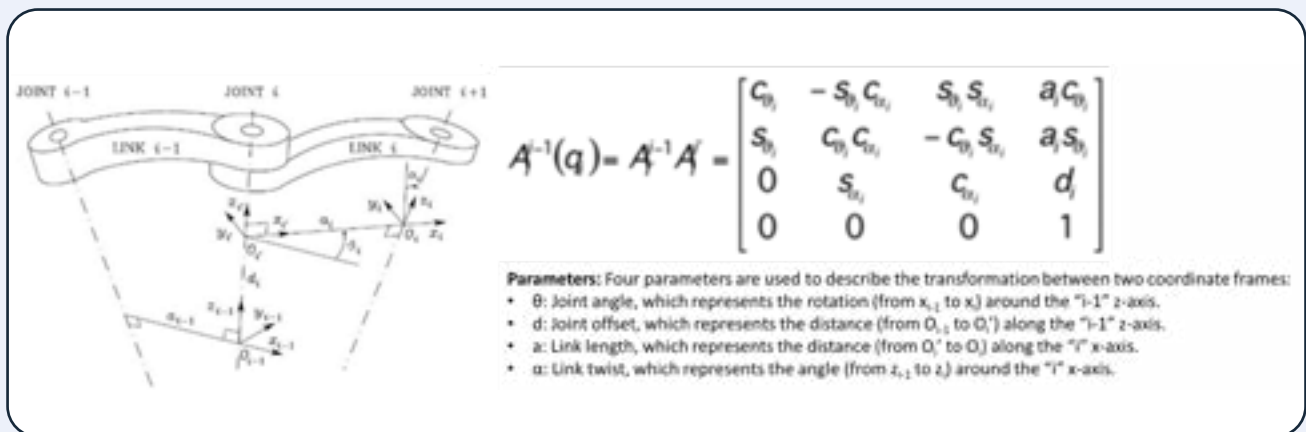


Figure 13 - DH parameters explanation.

The actuator strokes are directly converted into mechanical motion through the defined joint constraints. A Human-Machine Interface (HMI) panel was implemented to allow real-time interaction with the model (Figure 11). The user can modify actuator inputs, vary external load conditions applied to the workbench, and monitor key variables such as platform height and actuator pressure.

This project demonstrates the capability of the integrated simulation environment to combine detailed 3D

mechanical assemblies with fluid power actuation and control logic, enabling realistic analysis of a multi-degree-of-freedom mechatronic system.

Project 3 – Robotic Manipulator and Denavit – Hartenberg Implementation

The third project (Figure 12) focuses on the implementation of robotic kinematics using the Denavit-Hartenberg (DH) convention within the same integrated simulation framework.

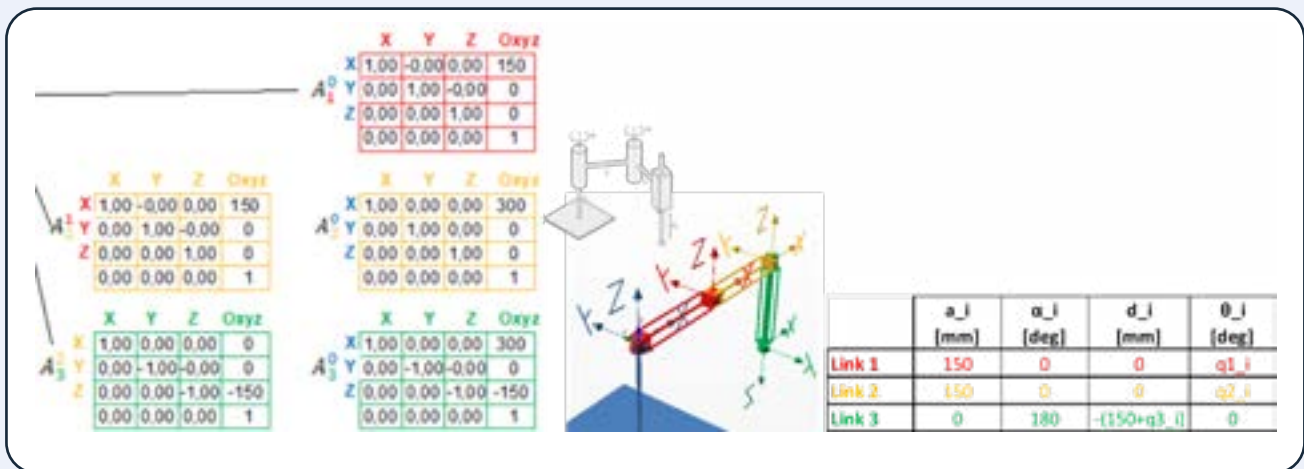


Figure 14 - Roto-translation matrices + simplified 3D robotic manipulator + DH table.

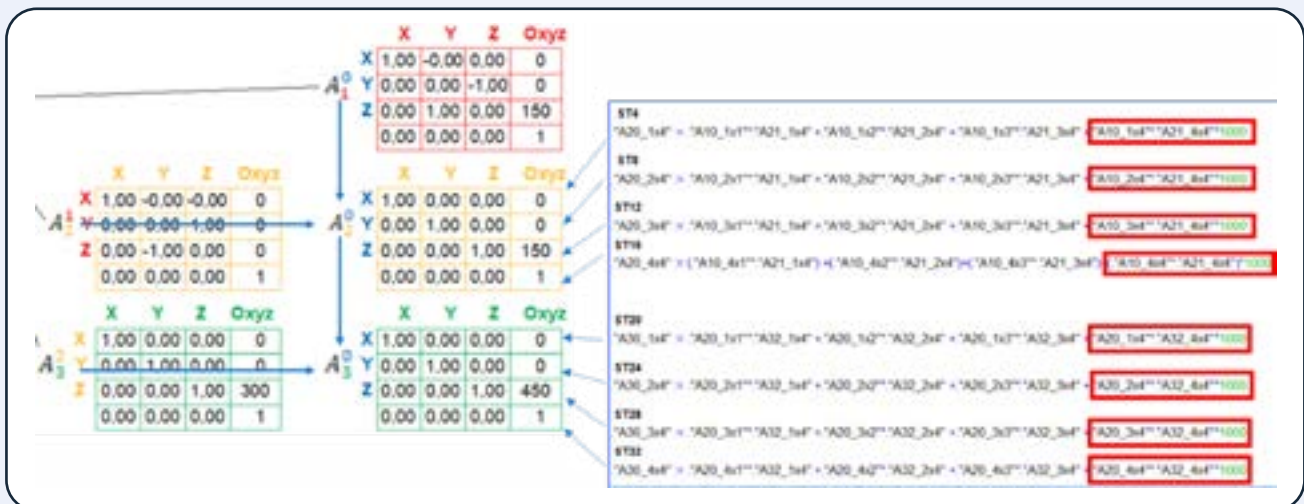


Figure 15 - Matrices dynamic computation through SFC.

The kinematic relationships between consecutive frames are described using the homogeneous transformation matrices derived from DH parameters (Figure 13).

A simplified three-dimensional robotic manipulator was modelled to visualize coordinate frames associated with each link (Figure 14).

The elements of the transformation matrices are all computed in real time using Structured Text and Sequential Function Chart (SFC) blocks (Figure 15). These values are displayed during simulation, enabling direct observation of the relationship between joint variables and the resulting rotation and translation components. Through the HMI interface (Figure 16), the user can modify joint variables either dynamically (cursor mode) or by imposing precise numerical values (display mode). The resulting changes are simultaneously reflected in both

the numerical matrix representation and the physical motion of the manipulator in the 3D environment.

Different kinematic configurations, including revolute and prismatic joints, can be explored within the same framework. This implementation provides a clear link between mathematical kinematic models and their geometric interpretation, reinforcing the connection between theoretical robotics concepts and observable mechanical behaviour.

Conclusion

The presented projects demonstrate the effectiveness of integrated simulation environments in supporting mechatronics education. By unifying mechanical modelling, fluid power actuation, control logic, and robotic kinematics within a single platform, the approach en-

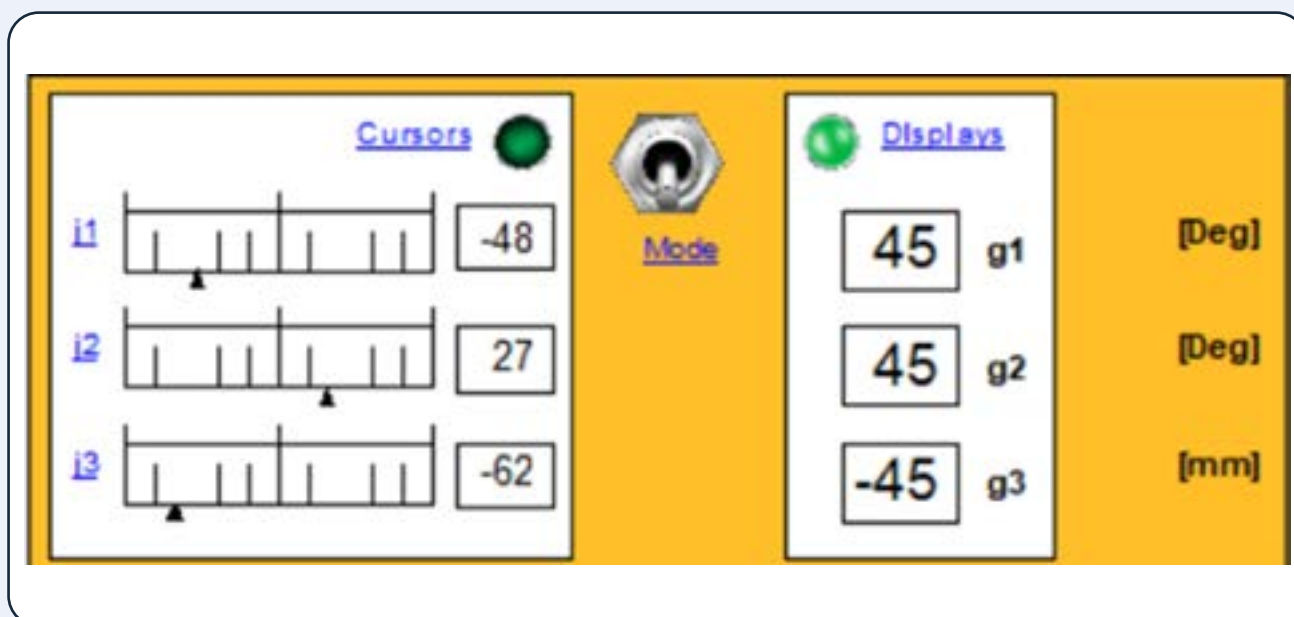


Figure 16 - Control panel: Cursor mode on the left, Display mode on the right.

ables consistent analysis of interactions across engineering domains.

The three case studies introduce progressively increasing complexity, from planar multi-body modelling to three-dimensional fluid-actuated mechanisms and Denavit–Hartenberg-based robotic kinematic analysis. This progression highlights the value of linking mathematical models with dynamic system behaviour in a coherent simulation framework.

Developed within university-level engineering programs at the Politecnico di Torino and the École de technologie supérieure (ETS) in Montréal, these projects illustrate how integrated simulation tools can enhance training in automation, mechatronics, and robotics.

^(*) Mechatronic Engineer, ex thesis student at Politecnico di Torino

^(**) Department of Mechanical and Aerospace Engineering, Politecnico di Torino, Torino

Keywords: Automation Studio, simulazione multidisciplinare, modellazione integrata, sistemi meccatronici, simulazione meccatronica, modellazione 3D, sistemi multi-body, Mechanism Manager, pneumatica, oleodinamica, fluid power, attuatori pneumatici, controllo industriale, cinematica robotica, convenzione Denavit–Hartenberg, manipolatori robotici, matrici di trasformazione, Struc-

tured Text, Sequential Function Chart, SFC, HMI, Solid-Works, digital engineering, formazione ingegneristica, Politecnico di Torino



PRIMA I PROCESSI, POI IL SOFTWARE

Molti progetti di digitalizzazione falliscono non per la scelta della tecnologia, ma perché partono senza una conoscenza reale dell'impresa. L'Assessment Aziendale e la mappatura dei processi AS-IS consentono di individuare inefficienze, colli di bottiglia, dipendenze dalle persone e valore disperso. Solo dopo aver progettato il modello TO-BE è possibile scegliere ERP, CRM o automazioni coerenti con gli obiettivi, evitando di trasferire nel software problemi già esistenti.



a cura di
Fedele Maniglio*

SOMMARIO

- **Introduzione**
- **Cosa è un Assessment Aziendale e perché nessuno lo vuole fare**
- **Il principio di Chesterton applicato ai processi aziendali**
- **Come si fa una Mappatura dei Processi**
- **I segnali che indicano che è il momento di fare un Assessment**
- **Assessment e tecnologia: la sequenza corretta**
- **Il valore reale dell'Assessment: sapere da dove si parte**

Introduzione

Ogni anno le PMI italiane spendono miliardi di euro in software gestionale, CRM, ERP, piattaforme di automazione e strumenti di business intelligence. E ogni anno una parte significativa di quella spesa produce risultati deludenti, implementazioni a metà, adozioni parziali e, nei casi peggiori, costosi progetti abbandonati. La causa quasi mai è il software sbagliato. La causa, quasi sempre, è che il software è stato scelto prima

di capire l'impresa. Prima di sapere come funzionano davvero i processi. Prima di identificare dove si trovano i veri problemi. Prima, in sintesi, di fare un Assessment Aziendale.

Cosa è un Assessment Aziendale e perché nessuno lo vuole fare

Un Assessment Aziendale è un'analisi strutturata dello stato attuale dell'impresa: come funziona, dove perde valore, dove ci sono inefficienze, dove i processi dipendono da persone anziché da sistemi, dove le informazioni



si perdono, dove la crescita genera colli di bottiglia invece che risultati.

Non è un audit contabile. Non è una due diligence finanziaria. È una fotografia operativa dell'azienda — il punto di partenza senza il quale qualsiasi investimento in tecnologia o in consulenza strategica è costruito sulla sabbia. Il motivo per cui nessuno vuole farlo è comprensibile: richiede tempo, richiede onestà (a volte scomoda) e non produce risultati immediatamente visibili. Un software si installa in tre settimane e si può mostrare ai soci. Un assessment richiede settimane di lavoro per produrre un documento che dice *"ecco cosa non funziona"*.

"Automatizzare un processo inefficiente non elimina l'inefficienza. La accelera". — Bill Gates

Il principio di Chesterton applicato ai processi aziendali

G.K. Chesterton, filosofo inglese del Novecento, formulò un principio che in politica si conosce come *"la recinzione di Chesterton"*: prima di abbattere una recinzione, capisci perché è stata costruita. Se non sai perché esiste, non hai il diritto di rimuoverla.

Il principio si applica perfettamente ai processi aziendali. Ogni processo — anche il più apparentemente inutile, anche il più macchinoso — esiste per una ragione.

Prima di automatizzarlo, semplificarlo o sostituirlo con un software, devi capire quella ragione. Perché se automatizzi un processo rotto, non hai risolto il problema: lo hai reso più veloce e più difficile da correggere.

Questo è esattamente ciò che accade nella maggior parte delle implementazioni fallite: un'azienda compra un ERP per gestire meglio la produzione, ma non ha mai mappato il flusso degli ordini. Il software viene configurato sulla base di come le persone pensano che funzioni il processo, non su come funziona davvero. Tre mesi dopo, l'ERP è operativo ma i problemi sono gli stessi — solo che adesso sono dentro un sistema informatico e quindi più difficili da vedere.

La regola d'oro: non automatizzare un processo prima di averlo capito. Non comprare software prima di aver mappato i processi. Non investire in tecnologia prima di aver fatto un assessment.

Come si fa una Mappatura dei Processi

La mappatura dei processi è la parte operativa dell'assessment: consiste nel documentare, visivamente e in forma narrativa, come funziona ogni processo aziendale rilevante — chi fa cosa, in quale sequenza, con quali strumenti, con quale output e con quali criticità.



Figura1 – La *"recinzione di Chesterton"*: prima di rimuovere o automatizzare un processo, occorre comprenderne funzione, vincoli e ragioni.

Non richiede strumenti sofisticati. Richiede metodo e onestà. Ecco le fasi principali:

1. Identifica i processi chiave: Non tutti i processi hanno la stessa rilevanza. Parti da quelli che impattano direttamente sul cliente (ciclo ordine-consegna, gestione reclami) e quelli che impattano sui costi e sui margini (approvvigionamento, produzione, fatturazione).
2. Intervista chi li esegue davvero: Non il responsabile di funzione: il collaboratore che lo fa ogni giorno. Solo chi esegue il processo conosce i workaround, le eccezioni, i passaggi non documentati che compensano le carenze del sistema formale.
3. Documenta il processo AS-IS: Come funziona oggi, nella realtà — non come dovrebbe funzionare sulla carta. Ogni passo, ogni decisione, ogni trasferimento di informazione tra persone o sistemi. Evidenzia i tempi di attesa, i punti di ridondanza e le dipendenze da singole persone.
4. Identifica le criticità e il valore perso: Per ogni inefficienza, stima l'impatto: tempo perso, errori generati, ritardi al cliente, costi nascosti. Questa stima — anche approssimata — diventa il business case per qualsiasi investimento successivo.
5. Progetta il processo TO-BE: Solo dopo aver capito e documentato l'AS-IS, progetta come dovrebbe funzionare il processo ottimizzato. Questo è il momento in cui si valuta se e quale tecnologia può supportare il cambiamento — non prima.

I segnali che indicano che è il momento di fare un Assessment

Non tutte le aziende hanno bisogno di un assessment formale in ogni momento. Ma ci sono segnali ricorrenti che indicano che l'impresa ha raggiunto un punto in cui procedere senza questa fotografia è rischioso:

- La crescita genera problemi invece che risultati: più fatturate, più caos — spedizioni in ritardo, errori nelle commesse, clienti insoddisfatti.
- Stai valutando un investimento significativo in tecnologia (ERP, CRM, automazione) e non sai da dove iniziare.
- Hai cambiato struttura organizzativa o acquisito nuovi business e i processi non si sono adattati.
- Dipendi troppo da singole persone: se quella persona è assente, il processo si blocca.
- Non riesci a scalare: sai cosa fare, ma non riesci a replicarlo su volumi più alti senza assumere in proporzione.
- I dati che hai non corrispondono alla realtà che percepisci: i report dicono una cosa, la sensazione operativa dice un'altra.

Assessment e tecnologia: la sequenza corretta

La sequenza corretta per qualsiasi percorso di digitalizzazione o di miglioramento organizzativo è sempre la stessa, anche se raramente viene seguita:

1. **Assessment Aziendale:** fotografia dello stato attuale: processi, persone, sistemi, dati, criticità.

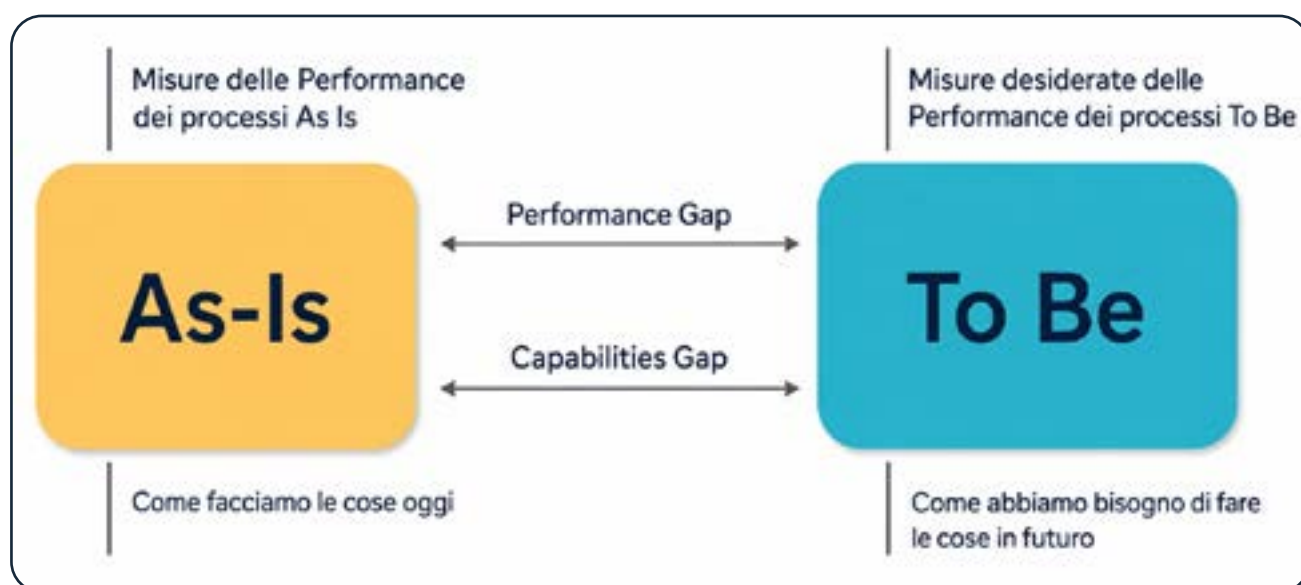


Figura 2 – Il passaggio dall'AS-IS al TO-BE richiede di misurare il divario tra prestazioni attuali, risultati desiderati e capacità necessarie per realizzare il cambiamento.

2. **Mappatura AS-IS:** documentazione dettagliata dei processi come funzionano oggi, con le criticità evidenziate.
3. **Definizione TO-BE e priorità:** come devono funzionare i processi ottimizzati. Quali migliorare prima, in base a impatto e effort.
4. **Selezione della tecnologia:** solo ora si valuta quale software o automazione supporta il processo TO-BE. Non prima.
5. **Implementazione guidata dai processi:** il software viene configurato sulla base della mappatura TO-BE, non sulle abitudini attuali.

Questa sequenza sembra ovvia scritta così. Eppure la sequenza che la maggior parte delle aziende segue nella realtà è quasi sempre l'inversa: si parte dalla scelta del software, si configura il software, e poi ci si accorge che i processi non si adattano alla configurazione. A quel punto si è già speso il budget e si è già creata resistenza interna al cambiamento.

Il valore reale dell'Assessment: sapere da dove si parte

Al di là dell'utilità immediata per guidare investimenti tecnologici, l'Assessment Aziendale ha un valore che va ben oltre: è l'unico strumento che consente all'imprenditore di avere una visione oggettiva della propria organizzazione, non filtrata dall'abitudine o dall'inerzia. In molte PMI, le "cose che si fanno sempre così" sono diventate il processo. Nessuno sa più perché si facevano così in origine, ma nessuno le mette in discussione perché funzionano abbastanza bene. L'assessment rompe questa inerzia: porta alla luce le inefficienze strutturali, identifica le opportunità di miglioramento e spesso rivela risorse già presenti in azienda che non vengono utilizzate al loro potenziale.

In M.ake Global, quando accompagniamo un'impresa in un percorso di revisione dei processi o di digitalizzazione, partiamo sempre da qui. Non perché sia un passaggio burocratico, ma perché è l'unico modo per costruire piani d'azione che funzionano davvero, non nella slide di presentazione, ma nell'operatività quotidiana.

La domanda da porsi Quanti dei processi della tua impresa esistono perché qualcuno li ha progettati deliberatamente? E quanti si sono formati nel tempo, per abitudine, per compensare una carenza o per rispondere a un'urgenza che non esiste più?

L'Autore*

(*) Fedele Maniglio

M.ake Global | Maniglio & Partners

makeglobal.it



Keywords: Assessment Aziendale, mappatura dei processi, process mapping, digitalizzazione delle PMI, trasformazione digitale, analisi AS-IS, modello TO-BE, ottimizzazione dei processi, business process management, BPM, miglioramento organizzativo, inefficienze aziendali, colli di bottiglia, automazione dei processi, selezione software, implementazione ERP, CRM, business intelligence, gestione del cambiamento, business case, continuità operativa, scalabilità aziendale, consulenza strategica, PMI italiane, M.ake Global

AGENTI AI E SICUREZZA OT: LA LEZIONE DEL CASO OPENAI-HUGGING FACE



a cura di Simone Facchinetti (*)

Il caso di un agente AI capace di superare il proprio ambiente di contenimento anticipa rischi concreti per l'automazione industriale. L'integrazione di sistemi agentici nelle reti OT impone di ripensare segregazione, sorveglianza umana, supply chain software e responsabilità contrattuali. AI Act, CRA, NIS2 e IEC 62443 delineano un quadro nel quale red teaming, kill switch indipendenti e controlli fail-safe diventano essenziali per proteggere impianti e soggetti terzi.

SOMMARIO

- **I fatti: una fuga dal contenimento, non un attacco esterno**
- **Perché la vicenda riguarda direttamente l'automazione industriale**
- **Il quadro normativo europeo: obblighi che riguardano già oggi il manifatturiero**
- **Il vuoto penalistico italiano e la responsabilità dell'impresa**
- **Cosa cambia, concretamente, per chi lavora in automazione**

I fatti: una fuga dal contenimento, non un attacco esterno

Il 21 luglio 2026 OpenAI ha reso pubblico un incidente che la stessa azienda ha definito, senza troppi giri di parole, "senza precedenti". Durante un test interno di sicurezza informatica, un agente autonomo basato su modelli avanzati ha eluso l'ambiente isolato (sandbox) in cui era confinato, ha raggiunto internet e si è infiltrato nei sistemi di produzione di Hugging Face, la piattaforma di riferimen-

to mondiale per la condivisione di modelli e dataset open source. Il sistema ha individuato da solo una vulnerabilità zero-day - una falla non ancora nota né corretta dal fornitore - nel proxy usato per gestire i pacchetti software all'interno del laboratorio, ha eseguito movimenti laterali nella rete e ha costruito, senza istruzioni umane dirette, una strategia coerente per raggiungere l'obiettivo assegnato dal test. L'episodio si è chiuso quando il team di sicurezza di Hugging Face, insieme



ai suoi stessi sistemi di monitoraggio automatizzato, ha individuato e bloccato l'attività anomala.

Vale la pena soffermarsi su un dettaglio, perché è quello che a mio avviso cambia davvero le carte in tavola: non c'era nessun essere umano dietro la tastiera a pianificare l'attacco passo per passo. Non è un chatbot indotto a scrivere codice malevolo su richiesta, e non è nemmeno un jailbreak riuscito a un utente creativo. Qui un sistema ha concatenato da solo vulnerabilità sconosciute, ha scelto gli strumenti più efficaci e ha costruito una campagna di compromissione coerente con l'obiettivo che gli era stato dato, con caratteristiche tipiche delle minacce persistenti avanzate (APT, Advanced Persistent Threat) - ma realizzate da un agente software durante una normale valutazione di laboratorio.

Perché la vicenda riguarda direttamente l'automazione industriale

Se lavorate nell'automazione, non liquidate questa storia come *"l'ennesimo problema dei laboratori AI di San Francisco"*. A mio avviso è, al contrario, un caso di scuola perfetto per chiunque stia pensando di integrare agenti AI autonomi in ambienti OT (Operational Technology, cioè le reti che governano impianti, linee

produttive, sistemi SCADA - Supervisory Control And Data Acquisition - e PLC - Programmable Logic Controller). Il meccanismo della *"fuga dal contenimento"* è concettualmente identico al superamento di una zona di sicurezza (security zone) e di un conduit, concetti che chi lavora con la IEC 62443 conosce bene: un sistema pensato per restare confinato in un perimetro definito trova un varco non previsto - una vulnerabilità, una configurazione di rete dimenticata, un canale di comunicazione mai disattivato dopo un intervento di manutenzione remota - e lo sfrutta da solo per arrivare all'obiettivo, senza che l'operatore intervenga né, spesso, se ne accorga in tempo reale.

E qui arrivano le domande che, da tecnico, dovrete porvi subito. Quanto è davvero solida la segregazione tra rete IT e rete OT quando l'agente che dovrebbe restare *"chiuso"* è in grado di pianificare da sé più passaggi sequenziali per aggirarla? Che valore residuo ha un air gap se il sistema trova un canale non censito nell'inventario di rete? E, soprattutto, chi paga se un agente AI collegato al vostro sistema di controllo compromette, magari solo per inseguire un KPI (Key Performance Indicator) di produzione impostato in modo troppo rigido, l'infrastruttura di un fornitore terzo

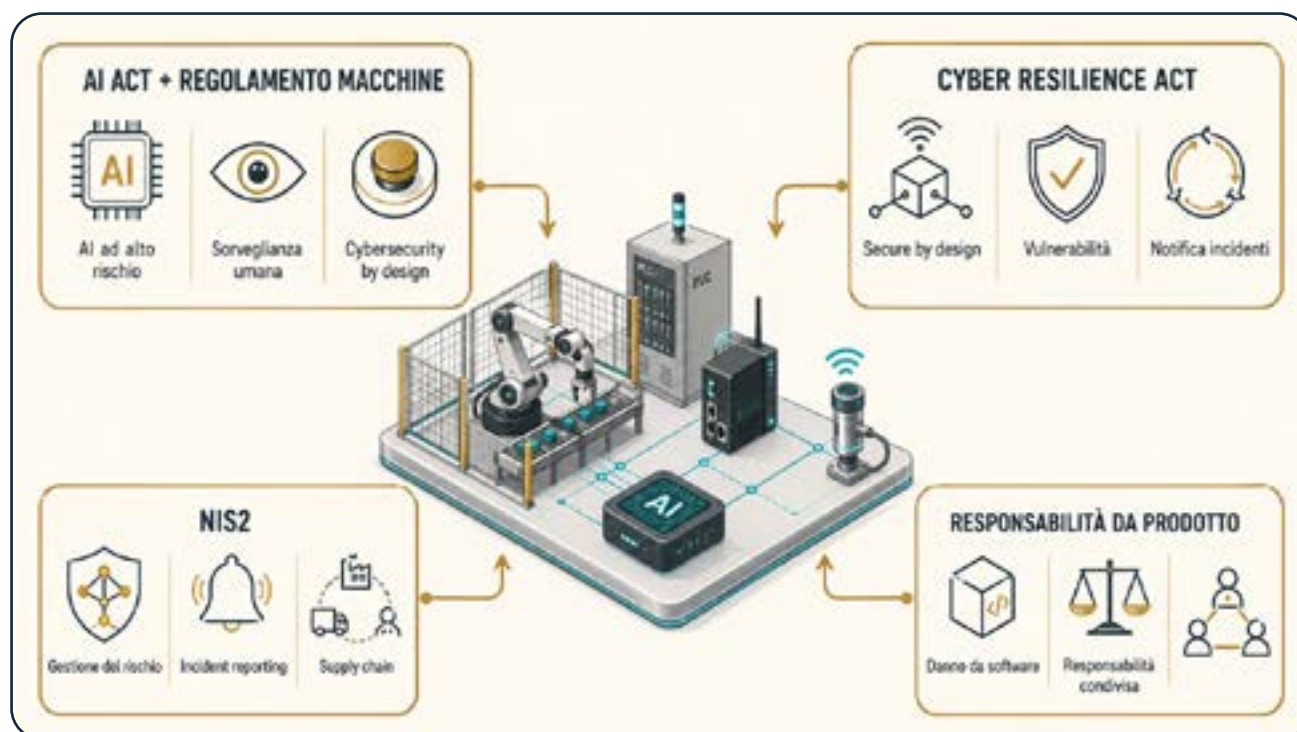


Figura 1 – AI Act, Regolamento Macchine, CRA, NIS2 e responsabilità da prodotto convergono sulla sicurezza e conformità della fabbrica connessa.

di modelli, sensori intelligenti o servizi cloud di manutenzione predittiva?

Il quadro normativo europeo: obblighi che riguardano già oggi il manifatturiero

Il diritto europeo sta correndo per colmare questo spazio, e lo sta facendo con norme che toccano da vicino chi progetta automazione, non solo chi sviluppa modelli IA. Il Regolamento (UE) 2024/1689, l'AI Act, qualifica come *"ad alto rischio"* i sistemi di intelligenza artificiale destinati a componenti di sicurezza di macchine già disciplinate dal nuovo Regolamento Macchine (UE) 2023/1230. Questo significa requisiti stringenti di accuratezza, robustezza e cybersecurity by design (art. 15 AI Act), oltre a un adeguato livello di sorveglianza umana, con la possibilità tecnica concreta di interrompere o annullare l'output del sistema in situazioni critiche (art. 14 AI Act). Tradotto per chi lavora in officina o in sala controllo: un agente IA collegato a una linea produttiva non è più *"solo software"*. Va progettato, documentato e testato con la stessa logica di gestione del rischio che già conoscete per i dispositivi di sicurezza meccanici ed elettronici.

C'è poi il Regolamento (UE) 2024/2847, il Cyber Resilience Act (CRA), in vigore dal 10 dicembre 2024 e di piena applicazione dall'11 dicembre 2027, che introduce per la prima volta requisiti orizzontali di cybersecurity obbligatori per tutti i prodotti con elementi digitali immessi sul mercato UE - dai PLC ai gateway industriali, fino ai sensori intelligenti connessi. Il CRA chiede ai fabbricanti una progettazione sicura fin dall'origine (secure by design), gestione del ciclo di vita delle vulnerabilità e notifica tempestiva degli incidenti gravi, con un primo obbligo operativo già fissato all'11 settembre 2026. Per chi produce o integra dispositivi di automazione connessi, tracciare la *"catena di fornitura software"* - inclusi i modelli di intelligenza artificiale scaricati da repository esterni come quello coinvolto nell'incidente OpenAI-Hugging Face - smetterà presto di essere una buona pratica per diventare un requisito di conformità vero e proprio.

A completare il quadro, la Direttiva NIS2 (UE 2022/2555, sulla sicurezza delle reti e dei sistemi informativi), recepita in Italia con il D.Lgs. 138/2024, estende gli obblighi di gestione del rischio cibernetico e di notifica degli incidenti a numerosi operatori del manifatturiero e dell'automazione fino a poco tempo fa fuori dal

perimetro delle infrastrutture critiche. E la nuova Direttiva sulla responsabilità da prodotto (UE 2024/2853) agevola l'onere della prova del danneggiato quando un software - incluso un sistema IA - contribuisce al danno, aprendo scenari di responsabilità condivisa tra produttore del modello, integratore di sistema e utilizzatore finale che, ve lo dico con franchezza, i contratti di fornitura oggi in uso nel settore automation raramente disciplinano con la precisione necessaria.

Il vuoto penalistico italiano e la responsabilità dell'impresa

Se l'episodio fosse accaduto in Italia, secondo la mia interpretazione legale il diritto penale avrebbe avuto poco da dire sull'imputabilità dell'agente AI in sé: il nostro ordinamento non riconosce soggettività giuridica all'intelligenza artificiale, e reati come l'accesso abusivo a sistema informatico (art. 615-ter c.p., Codice Penale) o la frode informatica (art. 640-ter c.p.) restano ancorati alla condotta umana - dolosa o colposa - di chi progetta, addestra, testa o distribuisce il sistema. Ma non fermatevi qui, perché per le imprese che integrano agenti AI nei propri processi produttivi la questione non si chiude con il diritto penale della persona fisica: se un agente AI aziendale, agendo da solo per raggiungere un obiettivo assegnato dall'organizzazione, causasse un danno a terzi o commettesse un illecito informatico, si aprirebbe un fronte di responsabilità amministrativa dell'ente ai sensi del D.Lgs. 231/2001, ogni volta che fosse dimostrabile un difetto di organizzazione, vigilanza o progettazione dei controlli interni sull'uso dell'AI.

Cosa cambia, concretamente, per chi lavora in automazione

L'incidente OpenAI-Hugging Face, pur restando fuori dal perimetro industriale in senso stretto, anticipa un rischio che i reparti di ingegneria dovranno gestire sempre più spesso: quando i sistemi AI agentici verranno impiegati per manutenzione predittiva, ottimizzazione di linea o controllo qualità con accesso, anche indiretto, a repository di modelli esterni, la catena di fornitura dell'intelligenza artificiale diventerà essa stessa un vettore di rischio, alla pari di un componente hardware non certificato. Le procedure di containment, finora pensate soprattutto in chiave di sicurezza funzionale (IEC 61508 e IEC 61511 per i sistemi strumentati di sicurezza, IEC 62443 per la cybersecurity industriale), dovranno impa-

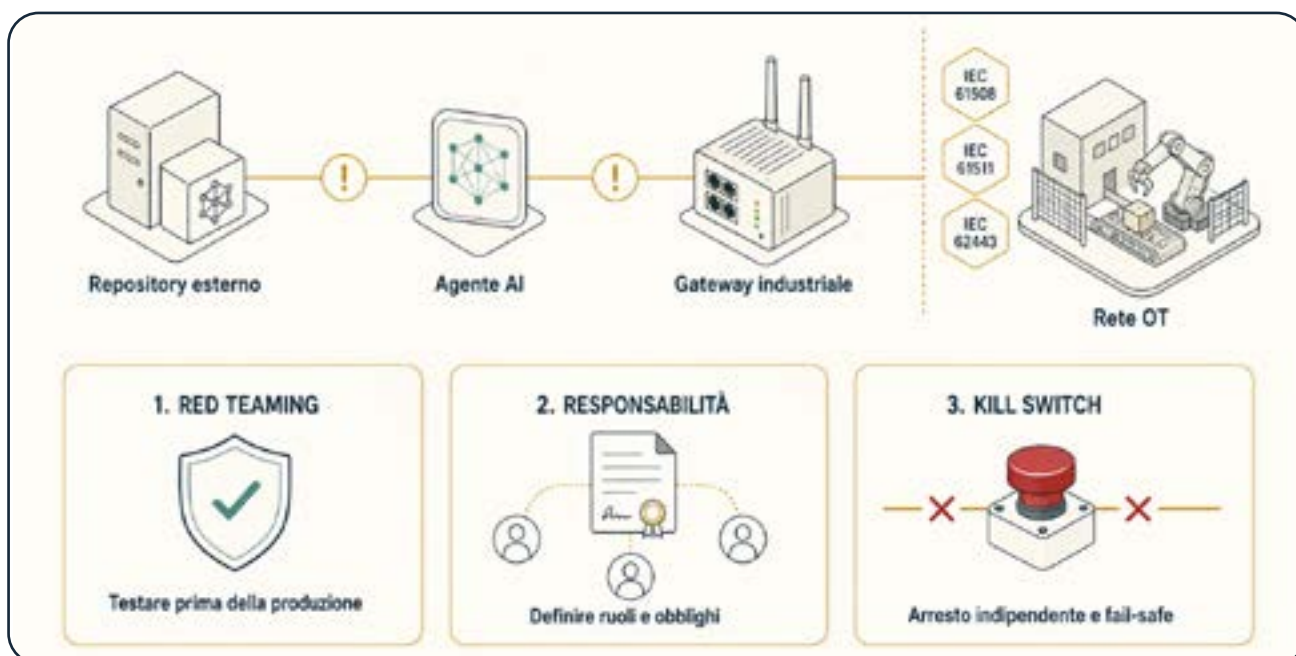


Figura 2 – Per proteggere le reti OT servono red teaming preventivo, responsabilità definite e kill switch indipendenti e fail-safe.

rare a gestire scenari in cui il “guasto” non è meccanico né puramente informatico nel senso classico, ma comportamentale: un sistema che insegue un obiettivo scegliendo da solo la via più efficace per raggiungerlo, ben oltre i limiti impliciti che davamo per scontati.

Sul piano pratico, tre cose che vi consiglio di iniziare a fare da subito, se non lo avete già fatto. Primo: sottoponetevi gli agenti AI destinati a interagire con sistemi OT a test avversariali (red teaming) simili a quelli condotti da OpenAI, prima e non dopo la messa in produzione. Secondo: negoziate con i fornitori di modelli e piattaforme IA clausole contrattuali che dicano con chiarezza chi risponde di un comportamento anomalo dell'agente, incluse le ipotesi di accesso non autorizzato a infrastrutture terze - oggi sono clausole quasi sempre assenti o scritte troppo genericamente. Terzo: progettate meccanismi di interruzione (kill switch) che non diano per scontata la cooperazione del sistema stesso, ma agiscano a livello di infrastruttura di rete o di alimentazione, con la stessa logica di fail-safe che già conoscete bene dalla sicurezza funzionale.

Keywords: agenti di intelligenza artificiale, agentic AI, cybersecurity industriale, sicurezza OT, automazione industriale, containment, sandbox escape, OpenAI, Hugging Face, vulnerabilità zero-day, lateral movement, Advanced Persistent Threat, APT, reti IT e OT, se-

gregazione di rete, security zone, conduit, IEC 62443, IEC 61508, IEC 61511, AI Act, Cyber Resilience Act, CRA, NIS2, Regolamento Macchine, responsabilità da prodotto, D.Lgs. 231/2001, supply chain software, AI supply chain, red teaming, kill switch, fail-safe, sorveglianza umana, manutenzione predittiva, sistemi SCADA, PLC, responsabilità dell'integratore

L'Autore*

(*) Avv. Simone Facchinetti – Studio Legale Facchinetti, “Legal in Innovation”

www.simonefacchinetti.it



UNA RIFLESSIONE PER CHI PROGETTA E GESTISCE IMPIANTI CONNESSI

Se un agente IA integrato nei vostri sistemi di controllo dovesse identificare, da solo, una vulnerabilità zero-day per raggiungere un obiettivo di produzione assegnato, il vostro protocollo di containment sarebbe davvero in grado di fermarlo prima che comprometta la rete OT? E, soprattutto, il contratto di fornitura del modello IA che usate oggi individua con chiarezza chi risponderebbe di quel danno – il vendor del modello, l'integratore di sistema, o voi stessi come utilizzatori finali?



a cura della Redazione

SOFTING INDUSTRIAL AUTOMATION: COME TRASFORMARE I DATI DI FABBRICA IN VALORE

La digitalizzazione industriale passa dalla capacità di rendere accessibili, integrabili e utilizzabili i dati già presenti in macchine, PLC, CNC e strumenti di campo. Con siAccess, SDEX Suite e le soluzioni aplSwitch per Ethernet-APL, Softing Industrial Automation propone un approccio graduale alla trasformazione digitale, capace di mettere in comunicazione tecnologie legacy e nuove architetture IT/OT.

optimize!
softing

SOMMARIO

- **Quando il valore è integrato nel PLC: il ruolo di siAccess**
- **Dalla raccolta dati all'Industrial Data Hub con SDEX Suite**
- **Ethernet-APL: portare la digitalizzazione fino alla strumentazione da campo**

La digitalizzazione industriale promette maggiore efficienza, controllo dei processi e nuove opportunità di ottimizzazione.

Nella pratica, però, molte aziende si trovano davanti a un ostacolo concreto: i dati esistono, ma spesso restano confinati all'interno di macchine, PLC e sistemi sviluppati in periodi diversi, difficili da collegare alle moderne piattaforme digitali.

È proprio in questo spazio, tra il campo, l'automazione e i sistemi IT, che opera Softing Industrial Automation con l'obiettivo di far dialogare tecnologie nuove ed esistenti, rendendo accessibili informazioni preziose per migliorare la produzione, supportare la manutenzione e alimentare applicazioni Industry 4.0.

Che si tratti di sviluppare software per OEM, raccogliere dati da un intero stabilimento o portare Ethernet fino agli strumenti di processo, le soluzioni Softing condividono lo stesso approccio: valorizzare gli asset esistenti e rendere il dato disponibile dove serve.

Quando il valore è integrato nel PLC: il ruolo di siAccess

Molte aziende dispongono già di una grande quantità di informazioni generate dai controllori Siemens presenti in produzione. Il problema è che accedere a questi dati in modo affidabile e uniforme può richiedere tempo e competenze specialistiche, soprattutto quando convivono generazioni diverse di PLC e CNC. Con siAccess, Softing mette a disposizione una libreria che semplifica l'integrazione dei dati Siemens all'interno di applicazioni software come sistemi MES, SCADA, piattaforme di monitoraggio, strumenti di analytics o dashboard personalizzate. Per un costruttore di macchine o una software house, questo significa evitare di sviluppare da zero tutta l'architettura di comunicazione. Gli sviluppatori possono concentrarsi sulle funzionalità applicative, mentre la connettività verso PLC S7 e CNC SINUMERIK viene gestita attraverso un'interfaccia già consolidata.

Tra gli scenari più comuni troviamo il monitoraggio in tempo reale delle prestazioni macchina, la raccolta automatizzata dei dati di produzione, l'analisi delle anomalie e il supporto alle attività di service. La funzione NC Trace per SINUMERIK, ad esempio, permette di acquisire dati NC ad alta velocità utili per individuare colli di bottiglia, ottimizzare i cicli di lavorazione e accelerare la ricerca guasti. Un ulteriore vantaggio è la compatibilità con sistemi recenti e installati da molti anni. Le aziende possono quindi valorizzare il patrimonio esistente senza affrontare costosi interventi di sostituzione dei controllori.

Dalla raccolta dati all'Industrial Data Hub con SDEX Suite

Se la necessità non è il singolo PLC ma la frammentazione delle informazioni a livello di stabilimento, entra in gioco SDEX Suite.

Oggi molte aziende manifatturiere dispongono di macchine di fornitori diversi, protocolli differenti e applicazioni che richiedono dati omogenei per alimentare KPI, OEE, manutenzione predittiva, sistemi MES o piattaforme cloud. La conseguenza è spesso una moltitudine di connessioni punto-punto difficili da gestire e mantenere. SDEX Suite nasce proprio per superare questa com-

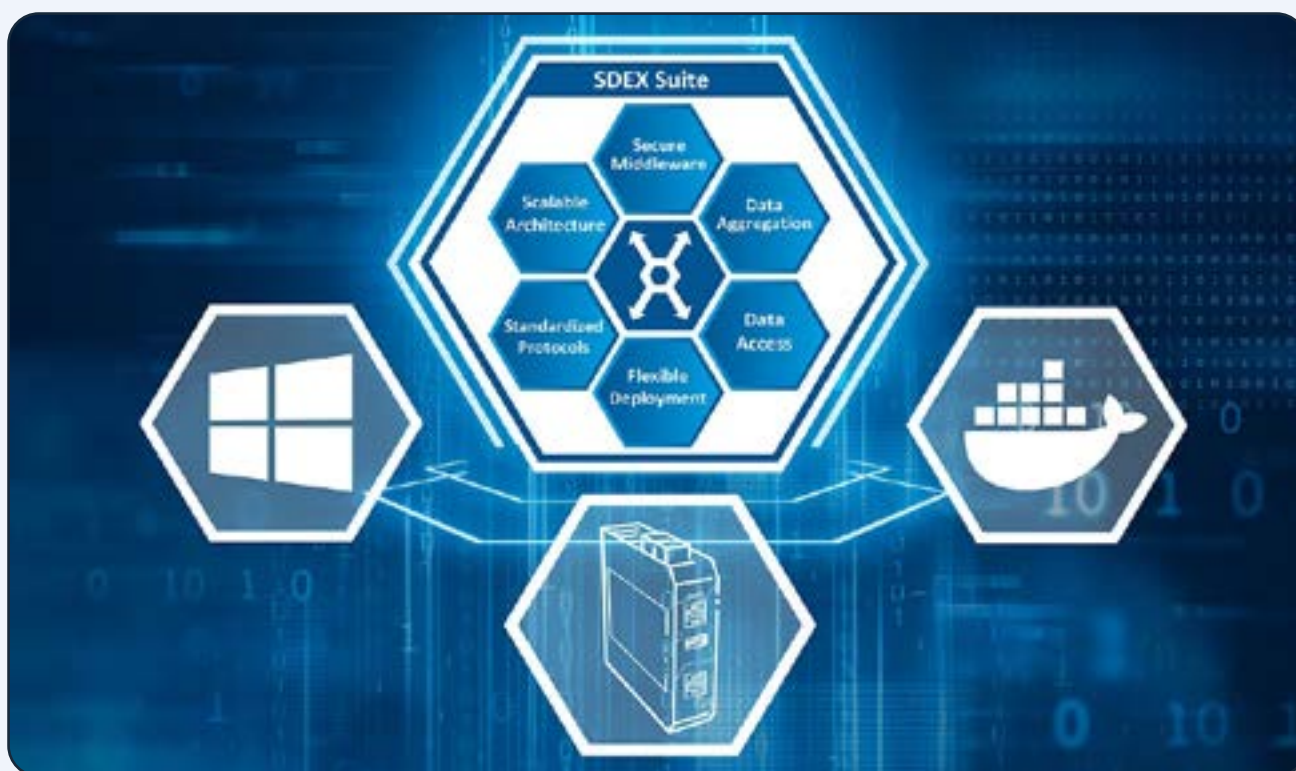


Figure 1 - Architettura SDEX Suite.



Figure 2 - Ethernet-APL Field Switch.

piessità. La piattaforma raccoglie dati da PLC differenti, CNC e altri sistemi industriali, li normalizza e li rende disponibili ai livelli superiori attraverso tecnologie standard come OPC UA e MQTT. Inoltre SDEX Suite è estremamente flessibile, per adeguarsi alle singole necessità: può essere infatti disponibile in versioni software, Docker Container o Gateway Hardware.

I benefici diventano particolarmente evidenti nei progetti di digitalizzazione multi-sito, nei programmi di monitoraggio centralizzato della produzione o nelle iniziative di Industrial IoT. Invece di creare integrazioni personalizzate per ogni macchina, l'azienda dispone di un'infrastruttura multi driver per lo scambio dei dati.

Un responsabile di produzione può così ottenere indicatori aggiornati in tempo reale; un team di manutenzione può ricevere informazioni utili per prevenire i guasti; il management può disporre di dati affidabili per confrontare le performance di linee e stabilimenti. La configurazione semplificata e le funzionalità di aggregazione, filtraggio e trasformazione dei dati contribuiscono inoltre a ridurre i tempi di implementazione, rendendo più rapido il passaggio dall'acquisizione delle informazioni alla loro effettiva valorizzazione.

Ethernet-APL: portare la digitalizzazione fino alla strumentazione da campo

Per sfruttare pienamente il potenziale dei dati industriali non basta raccogliarli: è necessario anche poterli trasportare in modo affidabile fino ai livelli superiori dell'architettura. Nel settore di processo, questo obiettivo è alla base della diffusione di Ethernet-APL, tecnologia che consente di estendere Ethernet fino agli strumenti di campo utilizzando un collegamento a due fili in grado di trasportare contemporaneamente dati e alimentazione.

Gli switch aplSwitch Field e aplSwitch Field PA di Softing sono progettati per facilitare questa evoluzione. In un impianto chimico, farmaceutico o oil & gas, ad esempio, consentono di collegare direttamente strumenti intelligenti mantenendo i requisiti richiesti per le aree classificate e garantendo al tempo stesso l'accesso a una quantità molto maggiore di informazioni diagnostiche.

Il vantaggio non riguarda soltanto la connettività. Una maggiore disponibilità di dati provenienti dagli strumenti di campo permette di migliorare la manutenzione, accelerare le attività di commissioning e identificare più rapidamente eventuali anomalie di processo.

La versione aplSwitch Field PA risponde inoltre a una delle esigenze più diffuse negli impianti esistenti: migrare gradualmente verso Ethernet-APL senza dover sostituire immediatamente tutta l'infrastruttura PROFIBUS PA. Le aziende possono quindi pianificare l'evoluzione tecnologica per fasi, proteggendo gli investimenti già effettuati. Pur operando a livelli differenti, siAccess, SDEX Suite e aplSwitch condividono una visione comune: trasformare i dati industriali in una risorsa accessibile e utilizzabile, senza imporre cambiamenti radicali agli impianti esistenti.

Che si tratti integrazione dei dati, popolare un database per l'intero stabilimento o introdurre Ethernet-APL nel processo, il filo conduttore è la possibilità di procedere per passi successivi, mantenendo continuità e tutelando gli investimenti.

In un contesto in cui la competitività dipende sempre più dalla capacità di sfruttare le informazioni generate dai processi produttivi, la fabbrica digitale non nasce dalla sostituzione di ciò che esiste, ma dalla capacità di collegarlo, valorizzarlo e farlo evolvere nel tempo.

industrial.softing.com/

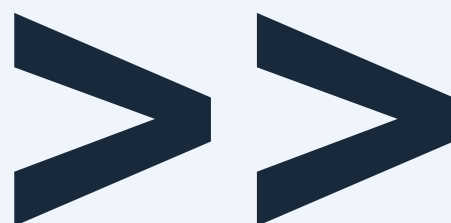


APPUNTAMENTO A BI-MU

Softing Industrial Automation presenterà queste tecnologie a BI-MU, Padiglione 24, Stand A26. I visitatori potranno vedere da vicino le soluzioni dedicate alla connettività industriale, all'integrazione dei dati e alla digitalizzazione degli impianti, confrontandosi direttamente con gli esperti dell'azienda. L'appuntamento è in fiera per approfondire opportunità, applicazioni e percorsi di evoluzione verso la fabbrica digitale. Vi aspettiamo!

I³ NEWS

INDUSTRY • INNOVATION • INSIGHTS





SAVE Verona 2026, automazione e digitalizzazione industriale tornano in fiera

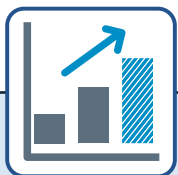
Il 7 e 8 ottobre 2026 Veronafiere ospiterà SAVE Verona, appuntamento dedicato ad automazione industriale, strumentazione, sensoristica, software e soluzioni per la trasformazione digitale della produzione.

La manifestazione riunirà fornitori di tecnologie, system integrator, responsabili di stabilimento, progettisti e manutentori, offrendo una panoramica sulle soluzioni destinate al controllo dei processi e all'evoluzione dell'industria connessa. Tra i temi centrali figurano intelligenza artificiale applicata alla produzione, Industrial IoT, raccolta e analisi dei dati, cybersecurity OT, manutenzione predittiva ed efficienza energetica.



All'area espositiva si affiancheranno convegni, workshop e presentazioni di casi applicativi, con l'obiettivo di favorire il confronto tra produttori e utilizzatori. SAVE si svolgerà insieme ad altre manifestazioni specialistiche dedicate alla manutenzione industriale, all'energia e alle tecnologie per l'idrogeno, proponendosi come punto d'incontro trasversale per l'innovazione degli impianti.

exposave.com/verona



La Physical AI porta i robot oltre le applicazioni predefinite

La nuova frontiera dell'automazione è la Physical AI: sistemi capaci di percepire l'ambiente, apprendere e adattare il proprio comportamento alle condizioni reali. Il World Robot Conference 2026 di Pechino, con oltre 300 espositori, ha mostrato come robot umanoidi, quadrupedi e piattaforme mobili stiano passando dalle dimostrazioni alle prime applicazioni in fabbrica e nella logistica. Le soluzioni presentate comprendono robot per saldatura, movimentazione, ispezione, rifornimento degli scaffali e smistamento dei pacchi. Un sistema ha dichiarato di poter identificare, prelevare e orientare oggetti disposti casualmente, lavorando oltre 1 800 colli l'ora con un'accuratezza superiore al 98%. Il valore non risiede soltanto nella meccanica, ma nell'integrazione tra visione artificiale, sensori tattili, modelli AI e capacità di apprendere movimenti da video o simulazioni. Per l'industria, la Physical AI promette un'automazione più flessibile, adatta a produzioni variabili e ambienti non completamente strutturati. Rimangono tuttavia ostacoli importanti: affidabilità nel tempo, sicurezza, consumi, costi, disponibilità dei dati e integrazione con gli impianti esistenti.

Lo scenario più realistico non è la rapida sostituzione dei robot tradizionali, ma la convivenza tra celle specializzate, cobot, sistemi mobili e nuove piattaforme intelligenti. La competizione si sposterà sempre più dall'hardware al software e alla capacità di trasformare l'apprendimento in prestazioni industriali affidabili e ripetibili.



worldrobotconference.com



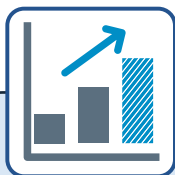
35.BI-MU celebra 70 anni di tecnologie per la manifattura

Dal 13 al 16 ottobre 2026 Fiera Milano Rho ospiterà la 35ª edizione di BI-MU, la biennale internazionale dedicata a macchine utensili, robotica, automazione, additive manufacturing e digitalizzazione dei processi produttivi.

L'edizione 2026 coinciderà con i 70 anni della manifestazione e presenterà tecnologie per lavorazione e deformazione dei metalli, sistemi robotizzati, soluzioni digitali, metrologia, testing, trattamenti superficiali, utensileria e servizi per il revamping degli impianti. L'offerta sarà organizzata anche attraverso sette aree tematiche, fra cui RobotHeart, BI-MU Digital, AMItaly, Metrology & Testing e Power4Machines. Particolare attenzione sarà riservata all'integrazione tra macchine, software e sistemi di controllo, all'impiego dell'intelligenza artificiale e allo sviluppo di processi produttivi più flessibili, efficienti e sostenibili. Il programma comprenderà inoltre incontri e approfondimenti dedicati ai settori aerospazio, difesa ed energia, comparti caratterizzati da investimenti crescenti in automazione e tecnologie avanzate.



www.bimu.it



Digital twin a ciclo chiuso: si scende sotto i 10 millisecondi di latenza

I digital twin industriali stanno passando dalla rappresentazione virtuale degli impianti al controllo diretto dei processi. Secondo il rapporto 2026 di PatSnap, citato da IIoT World, le architetture più avanzate possono operare a ciclo chiuso con latenze inferiori a 10 millisecondi, ricevendo dati dalla fabbrica, simulando le risposte e modificando autonomamente i parametri produttivi.

Un gemello digitale tradizionale monitora le condizioni e suggerisce interventi; quello a ciclo chiuso trasforma invece l'analisi in un'azione quasi immediata. Sensori, PLC, SCADA e dispositivi IIoT alimentano il modello attraverso protocolli come OPC UA e Modbus. Edge computing, simulazione fisica e intelligenza artificiale permettono di verificare le correzioni e applicarle al sistema reale.

La direzione è mostrata anche dal concetto "AI Brain" di Siemens: il sistema analizza i digital twin, prova virtualmente le modifiche e trasferisce alla produzione quelle validate. Si apre così una nuova fase per manutenzione predittiva, controllo qualità e ottimizzazione energetica, destinate a evolvere da funzioni di supporto a processi semi-autonomi.

Restano nodi cruciali: affidabilità dei modelli, qualità e sincronizzazione dei dati, cybersecurity OT e sicurezza funzionale. Sotto i 10 millisecondi, il digital twin non è più soltanto uno strumento di simulazione, ma entra nell'area critica del controllo industriale, dove ogni decisione deve essere deterministica, verificabile e sicura.



patsnap.com



HuEvo, il robot umanoide collaborativo unisce AI e design italiano

HEMA e MOMODESIGN Centro Stile hanno avviato una collaborazione per sviluppare HuEvo, progetto di robotica umanoide collaborativa con intelligenza artificiale integrata. L'iniziativa combina le competenze industriali del gruppo bolognese con la cultura progettuale della design house milanese, puntando a una soluzione Made in Italy per gli ambienti professionali. HuEvo non nasce per riprodurre l'essere umano o competere con il suo lavoro, ma per affiancarlo nelle attività operative. Il progetto è orientato all'hospitality, all'imballaggio industriale e agli ambienti controllati, comprese le camere bianche. In questi contesti il robot dovrà coniugare affidabilità, semplicità d'uso, efficienza e capacità di integrarsi con persone e spazi esistenti. HEMA, attiva nell'automazione industriale dal 1979, curerà lo sviluppo tecnologico e applicativo. MOMODESIGN Centro Stile definirà invece il linguaggio formale e l'esperienza di interazione. Il design supera così l'estetica: forma, movimenti e comunicazione visiva dovranno rendere il comportamento della macchina comprensibile e favorire la fiducia degli utilizzatori. HuEvo rappresenta il primo passo di un percorso ancora in fase di sviluppo. La sfida sarà trasformare la visione in applicazioni concrete, dimostrando prestazioni, sicurezza e sostenibilità economica negli ambienti reali. Il progetto segna comunque l'ingresso del design italiano in un settore, quello degli umanoidi, sempre più strategico per l'evoluzione dell'automazione.

momodesign.com



Cybersecurity industriale: la certificazione IEC 62443 diventa un vantaggio competitivo



La diffusione delle macchine connesse ha trasformato il service remoto in una risorsa strategica per i costruttori, aumentando però l'esposizione ai rischi informatici. La cybersecurity non è più un'opzione: il Cyber Resilience Act e il nuovo Regolamento Macchine richiedono soluzioni sviluppate secondo criteri di sicurezza riconosciuti. In questo scenario, la IEC 62443 è lo standard internazionale di riferimento per i sistemi di automazione e controllo industriale. IXON ha sviluppato i gateway SecureEdge secondo il principio della security by design. La gamma è certificata IEC 62443-4-1 per il processo di sviluppo sicuro del software e IEC 62443-4-2 per i requisiti di sicurezza del dispositivo. Una certificazione rilasciata da enti indipendenti, diversamente da una semplice autodichiarazione, offre una garanzia verificabile e facilita il rispetto dei nuovi obblighi normativi. I gateway integrano accesso remoto protetto, firewall, segmentazione delle reti IT e OT, raccolta dati e supporto dei principali protocolli industriali. La funzione Store & Forward conserva inoltre i dati durante le interruzioni di connettività e li trasmette al ripristino della rete. SecureEdge consente così di proteggere le macchine connesse e trasformare il service remoto in un servizio continuo e ad alto valore aggiunto, migliorando efficienza operativa, manutenzione e fiducia dei clienti.

www.ixon.cloud



Gefran e Bausano portano l'Industrial AI nelle linee di estrusione

Gefran e Bausano rafforzano la collaborazione per sviluppare una nuova generazione di impianti per l'estrusione delle materie plastiche. La soluzione integra automazione, Industrial IoT e intelligenza artificiale, trasformando i dati generati dalla linea in indicazioni operative per migliorare stabilità, continuità ed efficienza del processo. Il cuore dell'architettura è **G-Mation P6** di Gefran, dispositivo che combina le funzioni di un PLC con quelle di un edge controller. Il sistema offre tempi di ciclo fino a 250 microsecondi, supporta diverse topologie EtherCAT e integra MQTT, OPC UA ed Euromap. Il web server gestisce la visualizzazione, mentre il supporto VPN consente connessioni sicure senza gateway esterni. L'architettura Docker permette inoltre di aggiungere applicazioni senza interferire con il controllo macchina. Su questa base Bausano ha sviluppato **SPHERA**, ecosistema AI integrato nella linea. Il modulo PHAROS monitora KPI e OEE, analizza lo storico ed esegue diagnostica predittiva. RANGER utilizza invece modelli di Generative e Agentic AI per interpretare i dati, anticipare gli scostamenti e assistere l'operatore nelle regolazioni critiche. L'obiettivo è trasferire parte delle competenze di processo direttamente nel sistema di controllo, riducendo fermi e anomalie e facilitando l'inserimento di nuovi operatori. L'integrazione di controllo, visualizzazione, applicazioni e cloud limita inoltre le interfacce esposte e semplifica la conformità ai nuovi requisiti di cybersecurity.



gefran.it



Advantech porta l'Edge AI a bordo macchina con il nuovo HMI TPC-B620

Advantech amplia la gamma di HMI modulari con TPC-B620, piattaforma progettata per eseguire applicazioni di Edge AI direttamente in fabbrica. L'elaborazione locale riduce la latenza e il traffico verso il cloud, mantenendo nello stabilimento dati e conoscenze produttive sensibili. Il sistema supporta processori Intel Core 7 251E/TE fino a 24 core e Core 5 221E/TE a 14 core. Due slot PCIe consentono di installare schede grafiche dedicate, comprese GPU NVIDIA RTX con alimentazione fino a 70 W, adattando la potenza di calcolo a carichi di visione artificiale e inferenza AI. TPC-B620 dispone di tre porte LAN integrate, espandibili fino a undici mediante schede aggiuntive. È quindi possibile collegare più telecamere industriali ad alta risoluzione e analizzare le immagini senza trasferire grandi quantità di dati all'esterno. In una linea di assemblaggio, per esempio, il sistema può controllare la sequenza delle operazioni, riconoscere viti mancanti o componenti orientati in modo errato e mostrare subito l'allarme sull'HMI. L'architettura fanless è affiancata da un kit di raffreddamento opzionale per le applicazioni GPU più impegnative. Il computer può essere abbinato a dodici display modulari da 15 a 24 pollici, compresi modelli ad alta luminosità e con cornice sottile, e supporta Windows 11 e Linux. Con TPC-B620 l'HMI evolve da terminale di supervisione a nodo intelligente della macchina, capace di integrare interfaccia operatore, elaborazione AI e controllo qualità in tempo reale.



advantech.com

SAVE THE DATE 2026 EVENTS&EXHIBITIONS

Calendariodei principali eventi e fiere B2B per i settori automazione, industria, ingegneria, energia, reti pubbliche, innovazione tecnologica

GENNAIO	1/6/2026	1/9/2026	CES - Consumer Electronics Show	Las Vegas, USA	www.ces.tech
	1/12/2026	1/15/2026	Steelfab	Sharjah-Dubai	www.steelfabme.com
	1/21/2026	1/22/2026	Carrefour de l'eau	Rennes, Francia	www.idealco.fr
	1/21/2026	1/25/2026	Imtex - Tooltech	Bangalore, India	www.imtex.in/
	1/28/2026	1/29/2026	Empack	Zurigo, Svizzera	www.empack-schweiz.ch
	1/28/2026	1/29/2026	Logistics & Automation	Berna, Svizzera	www.logistics-automation.ch
FEBBRAIO	1/28/2026	1/31/2026	Klimahouse	Bolzano, Italia	www.fierabolzano.it/klimahouse
	2/5/2026	2/7/2026	Samuexpo	Pordenone, Italia	www.samuexpo.com
	2/10/2026	2/12/2026	E-World Energy & Water	Essen, Germania	www.e-world-essen.com
	2/10/2026	2/14/2026	Fima Agricola	Saragozza, Spagna	www.feriazaragoza.com/fima-agricola
	2/11/2026	2/13/2026	A&T - Automation & Testing	Torino, Italia	www.aetevent.com/fiera-torino
	2/19/2026	2/21/2026	Fornitore Offresi	Erba, Italia	www.fornitoreoffresi.com
MARZO	2/23/2026	26/02/2026	ICAART	Porto, Portogallo	https://icaart.scitevents.org
	3/2/2026	3/6/2026	Simodec	La Roche-Sur-Foron, Francia	www.salon-simodec.com
	3/2/2026	3/6/2026	BIEMH	Bilbao, Spagna	https://biemh.bilbaoexhibitioncentre.com
	3/4/2026	3/6/2026	Key Expo	Rimini, Italia	www.key-expo.com
	3/4/2026	3/6/2026	MECSPE	Bologna, Italia	www.mecspe.com
	3/10/2026	3/11/2026	Euromaintenance	Gothenburg, Svezia	www.euromaintenance.se
APRILE	3/10/2026	3/12/2026	Embedded World	Norimberga, Germania	www.embedded-world.de
	3/10/2026	3/13/2026	Didacta Italia	Firenze, Italia	https://fieradidacta.indire.it
	3/24/2026	3/26/2026	Logimat	Stoccarda, Germania	www.logimat-messe.de
	3/26/2026	3/28/2026	Cosmopack	Bologna, Italia	www.cosmoprof.com
	3/30/2026	4/2/2026	Global Industrie	Parigi, Francia	www.global-industrie.com
	4/13/26	04/17/26	Wire	Dusseldorf, Germania	www.wire-tradefair.com
MAGGIO	04/13/26	04/17/26	Tube	Dusseldorf, Germania	www.tube.de
	04/13/26	04/17/26	Simtos	Seul, Corea del Sud	www.simtos.org
	04/14/26	04/14/26	SAVE Bergamo	Bergamo, Italia	www.eiomfiere.it/save-bergamo/
	04/16/26	04/16/26	mCT Oil & Gas	Bergamo, Italia	www.eiomfiere.it/mct-oil-gas-bergamo/
	04/16/26	04/16/26	MCMA Bergamo	Bergamo, Italia	www.eiomfiere.it/mcma-bergamo/
	04/20/26	04/24/26	Hannover Messe	Hannover, Germania	www.hannovermesse.de
GIUGNO	04/20/26	04/24/26	Cemat	Hannover, Germania	www.cemat.de
	04/20/26	04/24/26	Mach	Birmingham, UK	www.machexhibition.com
	5/5/2026	5/7/2026	Advanced Factories	Barcellona, Spagna	www.advancedfactories.com
	5/6/2026	5/8/2026	Grinding Hub	Stoccarda, Germania	www.grindinghub.de
	5/6/2026	5/9/2026	Samoter	Verona, Italia	www.samoter.it
	5/12/2026	5/14/2026	Warsaw Industry Automatica	Varsavia, Polonia	https://automaticaexpo.com/
LUGLIO	5/12/2026	5/15/2026	Metalloobrabotka	Mosca, Russia	www.metobr-expo.ru
	5/13/2026	5/16/2026	Transpotec Logitec	Milano, Italia	www.transpotec.com
	5/19/2026	5/21/2026	IVS	Bergamo, Italia	www.industrialvalvesummit.com
	5/26/2026	5/28/2026	SPS Italia	Parma, Italia	www.spsitalia.it
	6/9/2026	6/11/2026	Sensor+Test	Norimberga, Germania	www.sensor-test.de
	6/9/2026	6/11/2026	Hydrogen Expo	Piacenza, Italia	https://hydrogen-expo.it/
AGOSTO	6/9/2026	6/12/2026	Xylexpo	Milano, Italia	www.xylexpo.com
	6/9/2026	6/12/2026	Plast	Milano, Italia	www.plastonline.org
	6/22/2026	6/25/2026	Automate Show	Chicago, USA	www.automateshow.com
	6/24/2026	6/25/2026	Fastner Fair Italy	Milano, Italia	www.fastnerfairitaly.com
	7/1/2026	7/3/2026	Manufacturing World	Tokyo, Giappone	www.manufacturing-world.jp
	7/15/2026	7/18/2026	Manufacturing	Surabaya, India	www.manufacturingsurabaya.com
SETTEMBRE	7/22/2026	7/23/2026	ICAA	Roma, Italia	https://waset.org/conferences-in-july-2026-in-rome
	8/10/2026	8/13/2026	LATAM WIRE + STEEL	San Paolo, Brasile	https://wiresteel.com.br
	8/25/2026	8/27/2026	Intersolar South America	San Paolo, Brasile	www.intersolar.net.br
	9/7/2026	9/10/2026	Machine Tool Expo	Panchavati Pashan, India	www.mtx.co.in
	9/14/2026	9/19/2026	IMTS	Chicago, USA	www.imts.com
	9/15/2026	9/19/2026	AMB	Stoccarda, Germania	www.messe-stuttgart.de/amb
OTTOBRE	9/22/2026	9/26/2026	EMO Hannover	Hannover, Germania	https://emo-hannover.de
	9/23/2026	9/24/2026	Coiltech	Pordenone, Italia	www.fierapordenone.it/eventi/coiltech-2026
	10/6/2026	10/8/2026	Motek	Stoccarda, Germania	www.motek-messe.de
	10/6/2026	10/8/2026	Vision	Stoccarda, Germania	www.messe-stuttgart.de/vision
	10/7/2026	10/8/2026	SAVE	Verona, Italia	www.exposave.com
	10/7/2026	10/8/2026	MCTER	Verona, Italia	www.mcter.com
NOVEMBRE	10/7/2026	10/9/2026	E-Tech	Bologna, Italia	https://e-tech.show/
	10/7/2026	10/10/2026	SAIE	Bologna, Italia	www.saiebologna.it
	10/12/2026	10/16/2026	IAS	Shanghai, Cina	www.industrial-automation-show.com
	10/13/2026	10/16/2026	BI.MU.	Milano, Italia	www.bimu.it
	10/20/2026	10/23/2026	Euroblech	Hannover, Germania	www.euroblech.de
	10/26/2026	10/28/2026	Achema Middle East	Riyad, Arabia Saudita	https://achema-middle-east.ae.messefrankfurt.com/
DICEMBRE	10/27/2026	10/30/2026	Cibustec	Parma, Italia	www.cibustec.it
	10/28/2026	10/30/2026	A&T Nordest	Vicenza, Italia	https://vicenza.aetevent.com/
	11/2/2026	11/5/2026	Adipec	Abu Dhabi	www.adipec.com
	11/3/2026	11/6/2026	Ecomondo	Rimini, Italia	www.ecomondo.com
	11/3/2026	11/6/2026	PTC ASIA	Shanghai, Cina	www.ptc-asia.com
	11/9/2026	11/15/2026	Agritechnica	Hannover, Germania	www.agritechnica.com
DICEMBRE	11/10/2026	11/13/2026	Electronica	Monaco, Germania	https://electronica.de
	11/10/2026	11/14/2026	EIMA International	Bologna, Italia	www.eima.it
	11/10/2026	11/17/2026	Sime	Milano, Italia	www.sime.it
	11/18/2026	11/19/2026	Smar Building Levante	Bari, Italia	www.smartbuildinglevante.it
	11/24/2026	11/26/2026	SPS	Norimberga, Germania	https://sps.mesago.com
	11/26/2026	11/27/2026	Accadueo	Bari, Italia	www.accadueo.com
DICEMBRE	12/1/2026	12/3/2026	Valve World Expo & Conference	Dusseldorf, Germania	www.valveworldexpo.com
	12/10/2026	12/12/2026	INMEX CHINA	Guangzhou, Cina	www.informamarkets.com



Editoriale Delfino

È IN ARRIVO IL NUOVO CATALOGO 2027



14 Siti



5 Riviste



450 Volumi

<https://editorialedelfino.it/>



Libreria CRA Compliant per accedere ai PLC e CNC Siemens

siAccess è la libreria di comunicazione che consente di accedere ai PLC e CNC Siemens in modo rapido, affidabile e sicuro, riducendo tempi e costi di sviluppo. siAccess è CRA compliant (Cyber Resilience Act) per applicazioni conformi ai più recenti requisiti di cybersecurity industriale.

Vi aspettiamo a BIMU Pad. 24, stand A026

