Executive Summary

La trasformazione digitale dell'industria ha cambiato profondamente il modo in cui vengono progettate, utilizzate e gestite le macchine industriali. Oggi le linee produttive sono sempre più composte da **sistemi cyber-fisici connessi**, che integrano software, firmware, sensori e piattaforme digitali.

In questo scenario, una vulnerabilità software non rappresenta più soltanto un rischio informatico. Può compromettere la sicurezza operativa delle macchine, interrompere la produzione e, nei casi più gravi, generare rischi per l'incolumità degli operatori.

Per affrontare queste nuove sfide, l'Unione Europea ha introdotto un quadro normativo articolato che integra sicurezza informatica, sicurezza delle macchine e resilienza operativa delle organizzazioni. Tre normative rappresentano oggi i pilastri di questo ecosistema:

- Regolamento Macchine (UE) 2023/1230
- Direttiva NIS2 (UE) 2022/2555 recepita con D.Lgs 4 settembre 2024, n. 138
- Cyber Resilience Act Regolamento (UE) 2024/2847

Queste normative affrontano il rischio cyber da **prospettive complementari**:

- sicurezza delle macchine e protezione degli operatori
- resilienza delle organizzazioni e delle supply chain
- sicurezza dei prodotti digitali e del software.

Il risultato è un cambiamento significativo per il settore industriale: la cybersecurity diventa un requisito essenziale per l'accesso al mercato europeo.

Questo white paper analizza il nuovo scenario normativo e propone un approccio strutturato per:

- comprendere le responsabilità introdotte dalle normative europee
- gestire i rischi legati al software industriale
- costruire un percorso concreto verso la conformità e la resilienza digitale.

1. Cybersecurity e sicurezza delle macchine: un nuovo paradigma

L'evoluzione verso l'Industria 4.0 ha trasformato profondamente la natura delle macchine industriali.

In passato le macchine erano sistemi prevalentemente meccanici o elettromeccanici. Oggi sono **sistemi cyber-fisici complessi**, in cui software e componenti digitali svolgono un ruolo fondamentale nel controllo e nell'ottimizzazione dei processi produttivi.

Questa trasformazione ha portato con sé nuove vulnerabilità.

Un attacco informatico può infatti:

- alterare la logica di controllo di una macchina
- interrompere processi produttivi critici
- compromettere la sicurezza degli operatori.

La cybersecurity non è più solo una questione IT.
Con il nuovo quadro normativo europeo diventa **un requisito essenziale per la sicurezza delle macchine e l'accesso al mercato**.

Il nuovo **Regolamento Macchine** riconosce esplicitamente questa evoluzione. Per la prima volta, la cybersecurity viene integrata nei **Requisiti Essenziali di Sicurezza e di Tutela della Salute**.

Questo significa che una macchina non può essere considerata sicura se i suoi sistemi digitali sono vulnerabili ad alterazioni che potrebbero compromettere il comportamento previsto della macchina.

Il regolamento diventerà obbligatorio il **20 gennaio 2027**, data entro la quale i costruttori dovranno dimostrare che la sicurezza informatica è stata integrata nei processi di progettazione e sviluppo delle macchine.

2. I 3 Pilastri dell'ecosistema normativo europeo

La resilienza industriale europea si poggia su tre pilastri normativi che affrontano il rischio cyber da angolazioni diverse e complementari. È fondamentale per il management comprendere che il software agisce come tessuto connettivo tra queste regolamentazioni.
Tre normative costituiscono oggi i pilastri di questo sistema.

Confronto tra Regolamenti: Regolamento Macchine, NIS2 e CRA

Caratteristica	Regolamento Macchine (MR)	Direttiva NIS2 (UE 2022/2555)	Cyber Resilience Act (CRA)
Soggetto Responsabile	Costruttore della Macchina	Operatore / Utilizzatore (Fabbrica)	Produttore di Prodotto Digitale
Oggetto della Tutela	La Macchina (Sistema Cyber-Fisico)	L'Organizzazione e la Business Continuity	Il Prodotto Digitale (Software/Hardware)
Natura del Rischio	Rischio per la safety (fisica)	Rischio operativo e di Supply Chain	Vulnerabilità intrinseche del prodotto
Output Richiesto	Marcatura CE / Fascicolo Tecnico	Compliance organizzativa e resilienza	Marcatura CE e Gestione Vulnerabilità

Queste normative non operano in modo indipendente. Al contrario, si integrano tra loro e definiscono un modello multilivello di gestione del rischio cyber.
Il software rappresenta il punto di connessione tra questi livelli.
Una vulnerabilità software può infatti:

- compromettere la sicurezza di una macchina
- interrompere la continuità operativa di un'azienda
- rappresentare un difetto di sicurezza di un prodotto digitale.

Per questo motivo il software sta diventando **uno degli elementi più critici nella gestione del rischio industriale**.

Il software è il punto di connessione tra safety industriale, cybersecurity e resilienza operativa.

Una **singola vulnerabilità** può avere impatti su:

- sicurezza della macchina
- continuità produttiva
- conformità normativa.

3. Un esempio concreto: anatomia di un attacco a una macchina connessa

Per comprendere meglio l'interazione tra queste normative e la convergenza delle responsabilità, consideriamo uno scenario realistico.
Una vulnerabilità nota presente nel firmware di un PLC viene sfruttata da un attaccante per installare un ransomware che blocca una linea produttiva.

- **Prospettiva CRA (Produttore del PLC):** Il produttore è responsabile del monitoraggio continuo delle vulnerabilità. Deve gestire le CVE attraverso il rilascio di patch tempestive e dimostrare un ciclo di sviluppo sicuro (Secure SDLC), pena pesanti sanzioni.

- **Prospettiva NIS2 (Utilizzatore):** l'azienda che utilizza la macchina deve notificare l'incidente alle autorità competenti e dimostrare di aver adottato misure di sicurezza adeguate per proteggere la propria infrastruttura OT e la supply chain tecnologica.

- **Prospettiva Regolamento Macchine (Costruttore):** L'attacco altera la logica di sicurezza, rischiando di causare danni fisici. Il costruttore deve aver documentato nel **Fascicolo**

Tecnico che la cybersecurity è stata progettata per impedire che una compromissione digitale generi un rischio per la salute.

Questo esempio evidenzia come un singolo incidente cyber possa avere **implicazioni tecniche, operative e normative**.

4. Il requisito chiave del Regolamento Macchine

Uno degli elementi più innovativi del nuovo regolamento è il **requisito 1.1.9**, che introduce l'obbligo di proteggere i sistemi digitali delle macchine da alterazioni che possano comprometterne la sicurezza.

Per soddisfare questo requisito è necessario adottare un insieme di misure tecniche e organizzative, tra cui:

- controllo e autenticazione degli accessi ai sistemi di controllo
- protezione dell'integrità del software e dei dati di sicurezza
- tracciabilità delle modifiche attraverso sistemi di logging
- procedure di aggiornamento sicuro del software
- indicazioni chiare sui requisiti di sicurezza informatica nel manuale d'uso.

Questi elementi devono essere documentati nel **Fascicolo Tecnico della macchina**, diventando parte integrante del processo di marcatura CE.

Il requisito 1.1.9 del Regolamento Macchine introduce l'obbligo di proteggere i sistemi digitali da alterazioni che possano compromettere la sicurezza.

La cybersecurity diventa quindi parte integrante del **Fascicolo Tecnico per la marcatura CE**.

5. Il ruolo strategico del software

La crescente centralità del software nei sistemi industriali richiede strumenti affidabili per valutarne la qualità e la sicurezza.

Lo standard **ISO 5055** consente di misurare in modo oggettivo la qualità strutturale del software, analizzando dimensioni fondamentali come:

- sicurezza
- robustezza
- efficienza
- manutenibilità

Utilizzare metriche ISO 5055 trasforma la cybersecurity da costo a vantaggio competitivo, garantendo che il software sia:

- **Privo di vulnerabilità:** Attraverso analisi rigorose (SCA e SAST) su codice custom e open source.
- **Resiliente:** Capace di mantenere un comportamento prevedibile anche in presenza di anomalie operative.

- **Efficiente e Strutturato:** Allineato agli standard di sviluppo IoT (IEEE 2700-2017) per assicurare interoperabilità tra domini diversi.

Attraverso l'analisi automatizzata del codice è possibile identificare vulnerabilità, dipendenze software rischiose e difetti strutturali che potrebbero compromettere l'affidabilità dei sistemi. Questo approccio consente alle organizzazioni di trasformare la cybersecurity da semplice requisito di conformità a **fattore strategico di qualità e affidabilità del prodotto**.

6. Software Intelligence per la gestione del rischio

La **Software Intelligence** permette di analizzare in modo sistematico il software industriale e produrre evidenze tecniche utili per audit, certificazioni e attività di gestione del rischio.
Le piattaforme di analisi del software consentono, ad esempio, di:

- identificare componenti open source e relative vulnerabilità
- generare la **Software Bill of Materials (SBOM)** richiesta dalle nuove normative
- ricostruire l'architettura reale delle applicazioni
- individuare punti critici e superfici di attacco.

La **Software Bill of Materials (SBOM)** diventa uno strumento fondamentale per:

- identificare vulnerabilità
- gestire la supply chain software
- supportare audit e certificazioni.

Queste informazioni sono fondamentali per supportare i processi di **cyber risk assessment**, migliorare la sicurezza del software e dimostrare la conformità ai requisiti normativi.

CAST Highlight: SCA & Cyber Risk Assessment

Esegue la **Software Composition Analysis (SCA)** identificando componenti *third-party* e relative CVE. Genera automaticamente la **SBOM (Software Bill of Materials)** in formati standard (SPDX/CycloneDX), mappa le vulnerabilità secondo gli standard **CWE, OWASP e CERT**, e supporta la conformità agli Art. 10 e 13 del CRA.

CAST Imaging: Architettura e Threat Modeling

Fornisce una "risonanza magnetica" del software, ricostruendo i flussi dati reali e i *trust boundaries* tra IT e OT. È lo strumento principe per identificare i **Single Points of Failure** e supportare il **Threat Modeling** (metodologia STRIDE), facilitando la valutazione dell'impatto architetturale richiesta dall'Allegato III del Regolamento Macchine.

CAST Gatekeeper: Continuous Compliance

Agisce come sentinella nelle pipeline CI/CD, applicando **Quality Gates** basati su **ISO 5055**. Blocca automaticamente rilasci non conformi, garantendo un **Secure SDLC** verificabile che produce documentazione tecnica oggettiva per autorità e organismi notificati.

7. Il Percorso in 6 fasi verso la conformità e la resilienza

Le organizzazioni che adottano strumenti di analisi del software e processi di Secure SDLC possono trasformare la cybersecurity da obbligo normativo a **vantaggio competitivo**.

Per affrontare la crescente complessità normativa e tecnologica, è utile adottare un approccio strutturato alla cybersecurity del software industriale.
Euranet propone un percorso strutturato "Cybersecurity Analysis del Software OT" per governare la complessità normativa integrando la Software Intelligence di CAST per fornire evidenze audit-ready, indispensabili per la Marcatura CE e la gestione del rischio.

- **Fase 0 – Preparazione e Perimetrazione**
    - *Attività:* Identificazione dei sistemi (PLC, SCADA, firmware, applicazioni di supporto), definizione del perimetro di assessment, classificazione di criticità e impatto su safety e continuità operativa.
    - *Deliverable*: Documento di perimetro, inventory degli asset e mappa dei sistemi OT a rischio (zone/conduit preliminari).
- **Fase 1 – Software Cybersecurity Assessment & SBOM (CAST Highlight)**
    - *Attività:* Analisi automatizzata del portafoglio applicativo, identificazione componenti open source, generazione SBOM e valutazione dei rischi (open source, obsolescenza, esposizione), inclusa l'identificazione di vulnerabilità note **CVE** sui componenti utilizzati.
    - *Deliverable:* **Software Cyber Risk Assessment Report**, SBOM dettagliata e Heatmap dei rischi.
- **Fase 2 – Analisi Architetturale (CAST Imaging)**
    - *Attività:* Ricostruzione automatica di componenti e dipendenze, analisi dei flussi dati e supporto al threat modeling (IEC 62443 / STRIDE), inclusa l'identificazione dei trust boundary IT/OT.
    - *Deliverable:* **Diagrammi architetturali reali** e mappa delle superfici di attacco/ potenziali single point of failure.

- **Fase 3 – Analisi Statica del Codice e Definizione del Secure SDLC (Governance)**
    - *Attività:* Analisi statica approfondita del codice con **CAST Imaging** per identificazione delle debolezze strutturali **CWE**, e allineamento dei processi di sviluppo e manutenzione ai requisiti normativi (CRA, NIS2, Machinery Regulation).
    - *Deliverable*: Elenco vulnerabilità classificate CWE con root cause, **modello di Secure SDLC**, standard e linee guida di sicurezza per sviluppatori e fornitori, integrazione con processi aziendali.
- **Fase 4 – Enforcement e Quality Gate (CAST Gatekeeper)**
    - *Attività:* Integrazione dei controlli di sicurezza e qualità nelle pipeline di rilascio (CI/CD), monitoraggio delle vulnerabilità (CVE/CWE), definizione di KPI, metriche e quality gate automatici.
    - *Deliverable:* Policy operative, **dashboard di conformità continua**, KPI (es. Technical Debt, Security Risk Index, qualità codice) e regole di blocco rilascio basate su soglie.
- **Fase 5 – Remediation e Miglioramento**
    - *Attività:* Prioritizzazione e gestione delle vulnerabilità (sia **CVE** legate a componenti sia **CWE** nel codice) e delle debolezze architetturali, definizione delle azioni correttive e ottimizzazione continua.
    - *Deliverable:* Piano di remediation strutturato (risk-based), backlog di interventi e roadmap di maturità.
- **Fase 6 – Monitoraggio Continuo e Audit**
    - *Attività:* Aggiornamento continuo della SBOM, correlazione periodica con nuove **CVE**, monitoraggio dei KPI e verifica nel tempo delle vulnerabilità **CWE** risolte o persistenti, supporto agli audit (interni/esterni, OEM, autorità).
    - *Deliverable:* Repository SBOM aggiornato, reportistica per audit per clienti OEM e autorità ed evidenze di conformità nel tempo.

Questo approccio consente alle organizzazioni di passare da una gestione reattiva degli incidenti a una **cybersecurity progettata e verificabile**.

Conclusioni

Il nuovo quadro normativo europeo rappresenta un cambiamento significativo per l'industria.
Le normative non devono essere interpretate come obblighi indipendenti, ma come elementi di una strategia coerente per rafforzare la sicurezza e la resilienza del sistema industriale.

- Il **Regolamento Macchine** protegge la sicurezza fisica degli operatori.
- Il **Cyber Resilience Act** garantisce la sicurezza dei prodotti digitali.
- La **NIS2** rafforza la resilienza delle organizzazioni e delle infrastrutture critiche.

Le aziende che adotteranno un approccio integrato alla sicurezza del software saranno meglio preparate ad affrontare le nuove sfide normative e tecnologiche.
In questo contesto, la capacità di **misurare, analizzare e migliorare la qualità del software industriale** diventa un elemento fondamentale per garantire sicurezza, conformità e competitività nel mercato globale.
Adottare questa visione sistemica, supportata dalle analisi oggettive di CAST e dalla consulenza strategica di Euranet, permette ai costruttori di trasformare l'obbligo normativo in un pilastro di affidabilità e responsabilità, garantendo una resilienza duratura nel mercato globale.

About CAST

CAST è leader mondiale nella Software Intelligence che analizza automaticamente il software per identificare vulnerabilità, componenti critici e rischi di conformità. Le soluzioni di CAST supportano tutti i produttori di macchine intelligenti nel rispettare fornendo evidenze oggettive sulla sicurezza del software. Grazie all'integrazione con GenAI, CAST potenzia l'analisi dei dati applicativi, facilitando la generazione automatica di SBOM, l'individuazione di vulnerabilità e il miglioramento della cyber-resilienza lungo l'intero ciclo di vita del prodotto.

About Euranet

Euranet è una società specializzata in Compliance Management con esperienza ultraventennale e internazionale in oltre 10 Paesi, che si rivolge prevalentemente ad aziende di medie e di grandi dimensioni. L'azienda svolge attività di consulenza anche sull'Information Security, Business Continuity, Asset Protection e Cybersecurity e assiste i clienti nella gestione e controllo dei processi organizzativi, nell'incremento di valore degli assets e supporto per il raggiungimento della conformità a leggi, regolamenti e standard internazionali.