IEC 62443 e Nuovo Regolamento Macchine (UE) 2023/1230

come prepararsi

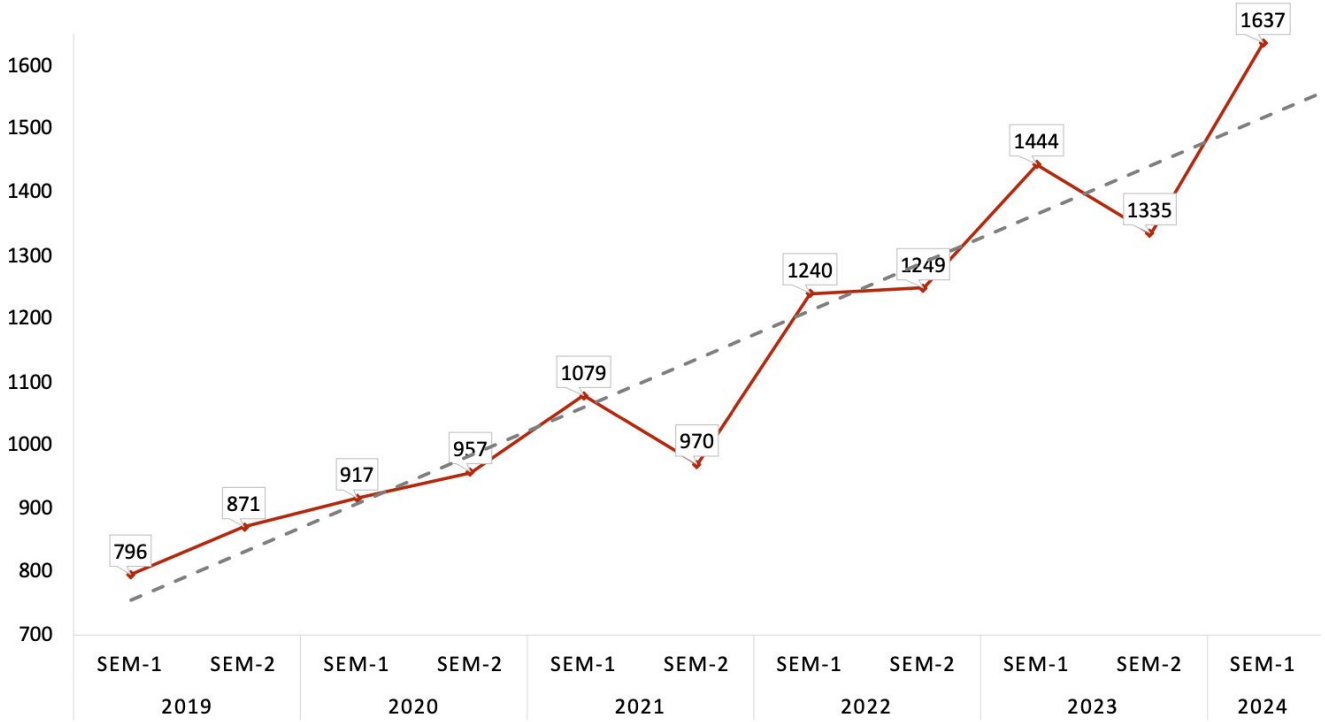
Agenda

- Rapporto Clusit 2024
- Regolamento UE 2023/1230
- IEC 62443

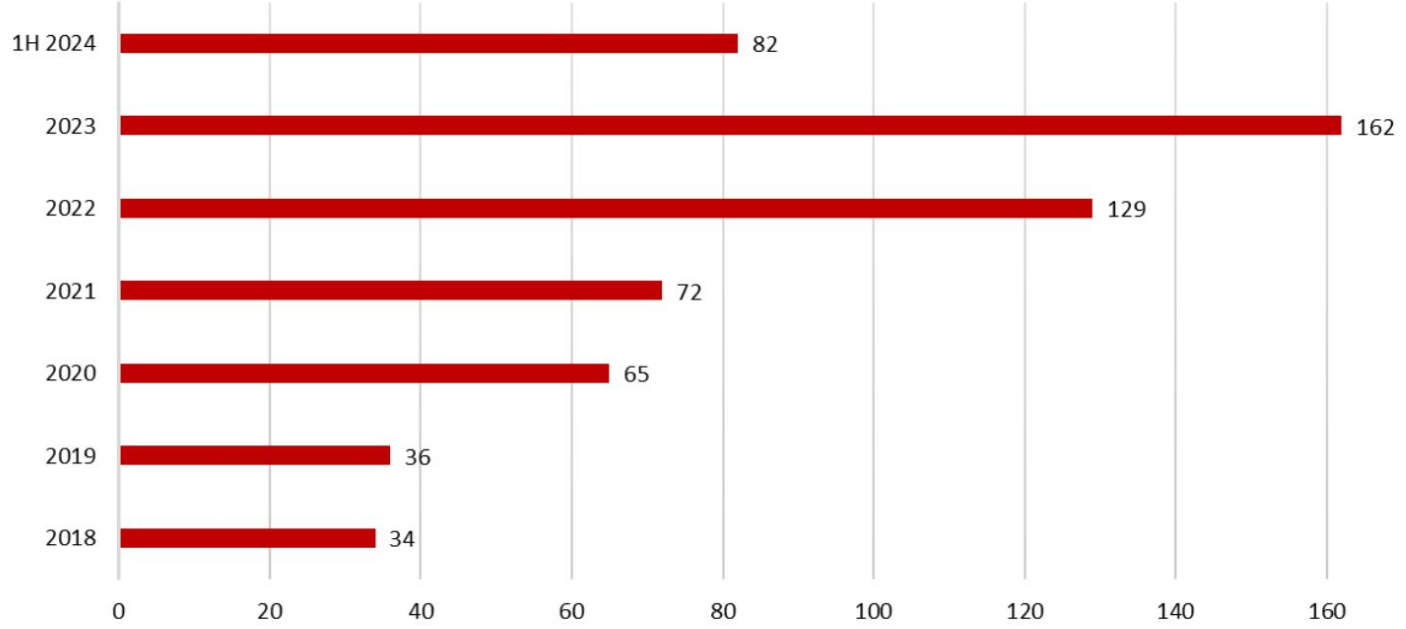
IXON

Rapporto Clusit 2024

Incidenti per semestre H1 2019 - H1 2024

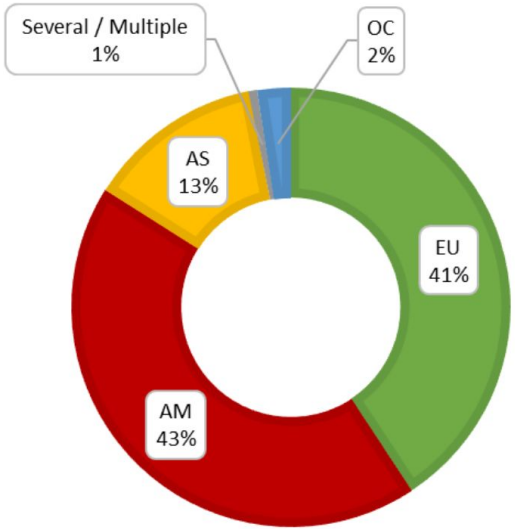


Manufacturing per anno

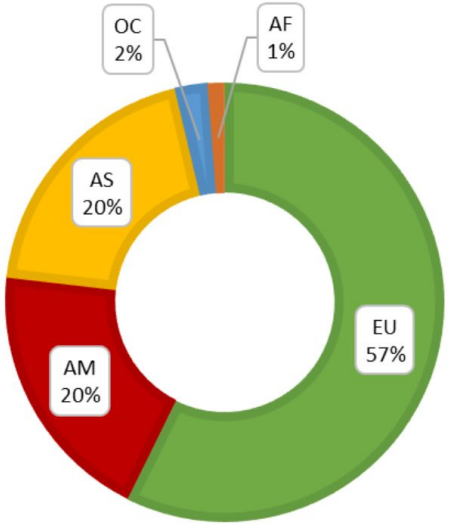


MANUFACTURING PER GEOGRAFIA

2023



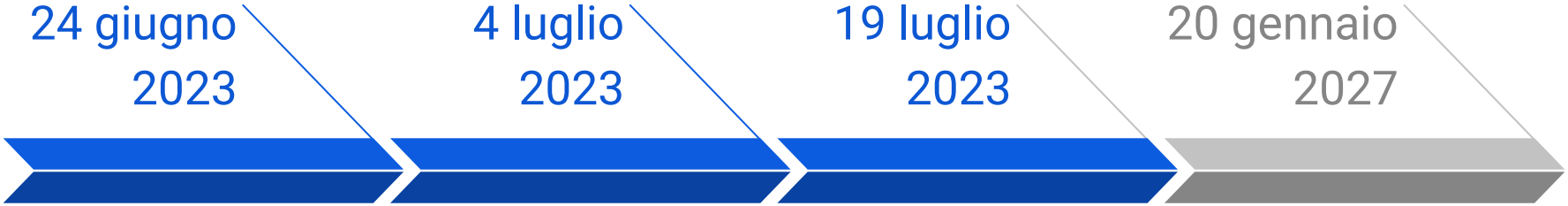
1H 2024



IXON

Regolamento UE 2023/1230

Roadmap



Pubblicazione su Gazzetta Ufficiale

Pubblicazione della rettifica

Entrata in vigore

Applicazione definitiva e abrogazione della direttiva 2006/42/CE

Roadmap


24 giugno 2023
4 luglio 2023
19 luglio 2023
20 gennaio 2027
Pubblicazione su Gazzetta Ufficiale
Pubblicazione della rettifica
Entrata in vigore
Applicazione definitiva e abrogazione della direttiva 2006/42/CE
Articoli da 26 a 42
dal **14 Gennaio 2024**

Articolo 26

“[...] Le macchine o i prodotti correlati devono essere conformi ai requisiti essenziali di sicurezza e di tutela della salute quando vengono immessi sul mercato o messi in servizio. [...]”

ALLEGATO III
REQUISITI ESSENZIALI DI SICUREZZA E DI TUTELA DELLA SALUTE
[...]

Protezione dall'alterazione &
Sicurezza ed affidabilità dei sistemi di comando

“I componenti hardware che trasmettono segnali o dati [...] devono essere progettati in modo tale da essere adeguatamente protetti da un'alterazione accidentale o intenzionale.”
(Allegato III, 1.1.9)

“Software e dati critici [...] devono essere adeguatamente protetti da un'alterazione accidentale o intenzionale.”
(Allegato III, 1.1.9)

Protezione dall'alterazione &
Sicurezza ed affidabilità dei sistemi di comando

“La macchina o il prodotto correlato devono raccogliere prove di un intervento legittimo o illegittimo sul software o di una modifica del software installato sulla macchina o sul prodotto correlato o della sua configurazione.”
(Allegato III, 1.1.9)

“la registrazione di tracciamento dei dati generati in relazione a un intervento e delle versioni del software di sicurezza caricato dopo l'immissione sul mercato o la messa in servizio della macchina o del prodotto correlato sia consentita per cinque anni dopo tale caricamento [...].”
(Allegato III, 1.2.1)

Protezione dall'alterazione &
Sicurezza ed affidabilità dei sistemi di comando

“[...] non siano consentite modifiche alle impostazioni o alle norme generate dalla macchina o dal prodotto correlato o dagli operatori [...] qualora tali modifiche possano determinare situazioni pericolose;”
(Allegato III, 1.2.1)

“La macchina o il prodotto correlato devono individuare il software installato sullo stesso [...] e devono essere in grado di fornire tali informazioni in qualsiasi momento in un formato facilmente accessibile.”
(Allegato III, 1.1.9)

Protezione dall'alterazione &
Sicurezza ed affidabilità dei sistemi di comando

“riescano a resistere, se del caso, a circostanze e rischi [...] compresi tentativi deliberati ragionevolmente prevedibili da parte di terzi che conducono a una situazione pericolosa;”
(Allegato III, 1.2.1)

“consentire in qualsiasi momento la correzione della macchina o del prodotto correlato al fine di preservarne la sicurezza intrinseca.”
(Allegato III, 1.2.1)

Requisiti di cybersecurity

Protezione dell'integrità

Tracciabilità

Controllo degli accessi

Risposta agli eventi

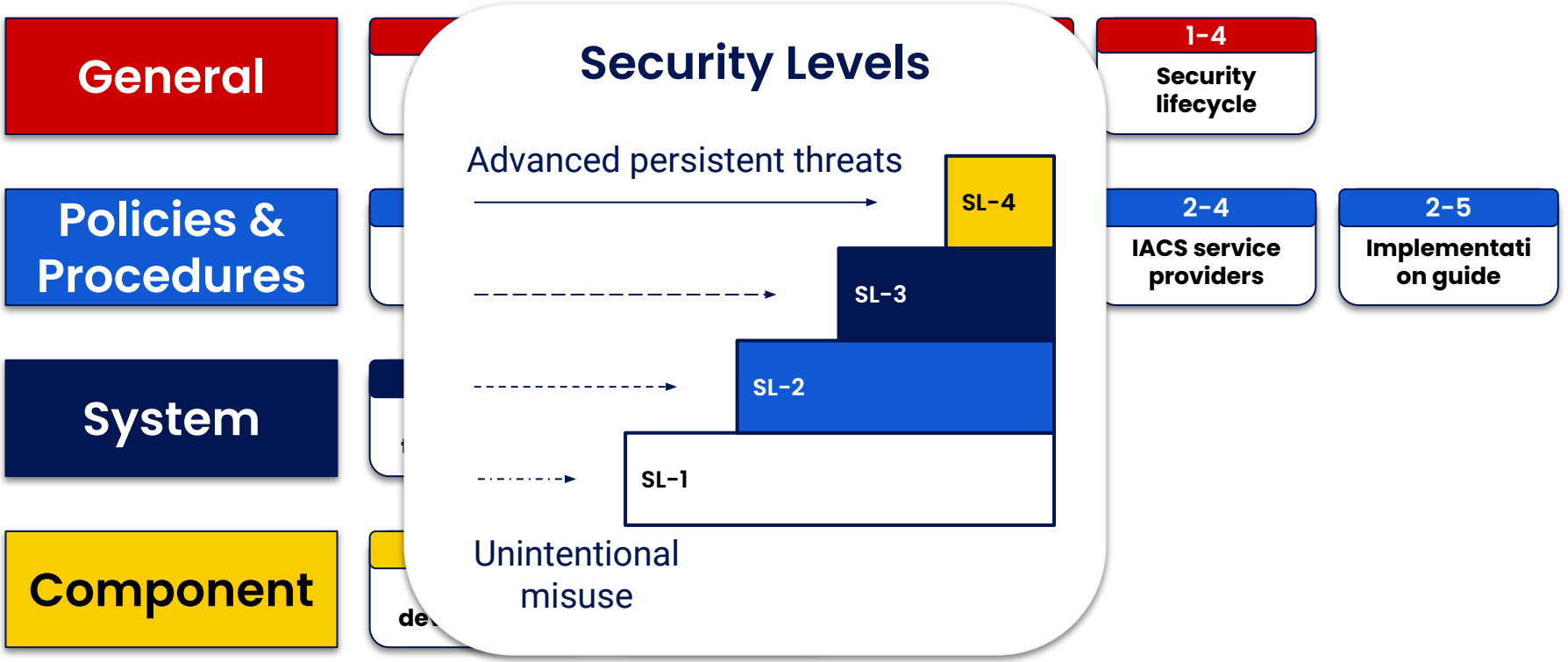
E quindi?


IEC
62443

Cos'è la IEC 62443?

General	1-1 Concepts & models	1-2 Glossary of terms	1-3 Security metrics	1-4 Security lifecycle	
Policies & Procedures	2-1 Security program	2-2 Protection levels	2-3 Patch management	2-4 IACS service providers	2-5 Implementation guide
System	3-1 Security technologies	3-2 Risk assessment	3-3 Secure systems		
Component	4-1 Product development	4-2 Secure components			

Cos'è la IEC 62443?



Cos'è la IEC 62443?

General	1-1 Concepts & models	1-2 Glossary of terms	1-3 Security metrics	1-4 Security lifecycle	
Policies & Procedures	2-1 Security program	2-2 Protection levels	2-3 Patch management	2-4 IACS service providers	2-5 Implementation guide
System	3-1 Security technologies	3-2 Risk assessment	**3-3 Secure systems**		
Component	4-1 Product development	**4-2 Secure components**			

IEC 62443

Protezione dell'integrità

IEC 62443-3-3 SR 3.4
IEC 62443-4-2 EDR 3.2
IEC 62443-4-2 EDR 3.14

Tracciabilità

IEC 62443-3-3 SR 2.8
IEC 62443-3-3 SR 2.9

Controllo degli accessi

IEC 62443-3-3 SR 1
IEC 62443-3-3 SR 2.1
IEC 62443-3-3 SR 5

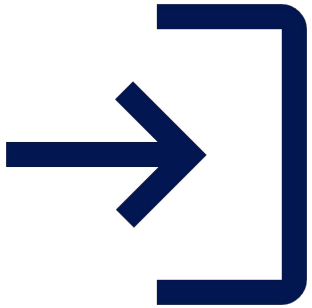
Risposta agli eventi

IEC 62443-3-3 SR 3.7
IEC 62443-3-3 SR 7
IEC 62443-4-2 CR 1.11

Protezione dell'integrità

- Verifica integrità software di boot e runtime
- Verifica integrità dati e software
- Firma digitale del software
- Whitelist applicazioni autorizzate
- Sandboxing

Controllo degli accessi



- Username univoco e password complesse
- Autenticazione a due fattori
- Gestione utenti basata su ruoli
- Doppia autorizzazione per operazioni critiche
- Crittografia
- Segmentazione di rete

Tracciabilità

- Logging estensivo
- Logging dettagliati
- Storage adeguato alla normativa applicabile
- Monitoraggio dello storage
- Log accessibili in sola lettura

IXON

Risposta agli eventi

- Protezione dagli attacchi DoS
- Protezione da attacchi Brute-force
- Limitazione delle risorse in uso
- Sistemi di backup
- Ripristino del sistema
- Least functionality

IXON

Fine?

IXON

IXON

GRAZIE