Advanced

CONFINDUSTRIA VENETO EST
Area Metropolitana
Venezia Padova Rovigo Treviso

ac&e

OBIETTIVO EXPORT

Webinar "Esportare macchine e impianti in Nord America. Focus sul nuovo regolamento NEC2023 e la cybersecurity applicata alle macchine e agli impianti industriali",

giovedì 14 settembre 2023

Relatore : Matteo Marconi AC&E SRL

CONFINDUSTRIA VENETO EST
Area Metropolitana
Venezia Padova Rovigo Treviso

Disclaimer of liability

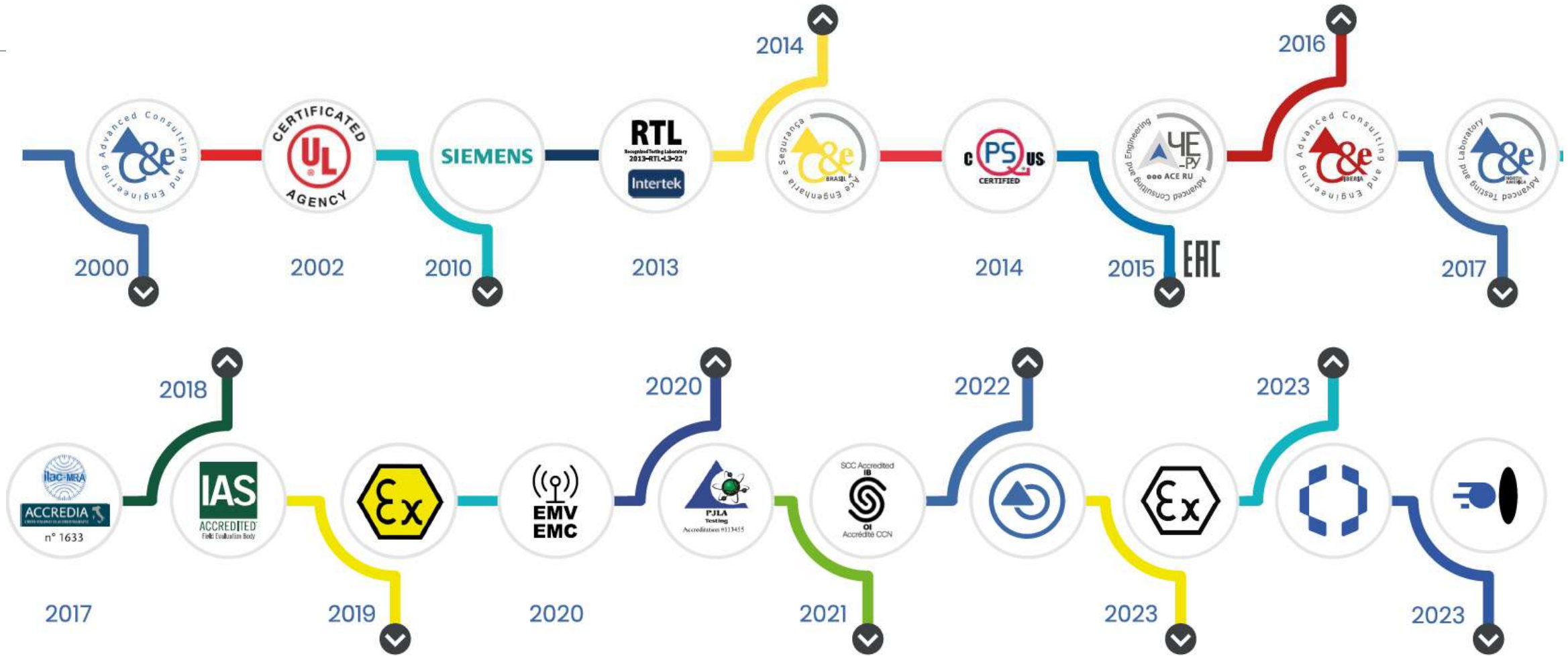
Tutti i contenuti del presente documento (immagini, testi, loghi e marchi) sono proprietà letteraria ed esclusiva di A.C.&E. s.r.l.
Si fa espressamente divieto di usare dati, immagini, informazioni, rappresentazioni fotografiche, PDF, contenuti in questa presentazione.

L'utilizzo di materiale appartenente ad A.C.&E. s.r.l. deve essere soggetto a richiesta e ad approvazione.
Ogni utilizzazione diversa dalla mera consultazione o dagli usi consentiti dalla legge nel rispetto della paternità del documento e/o delle informazioni senza il consenso scritto di A.C.&.E. è sanzionabile civilmente e penalmente.

Loghi di altre Aziende e Istituzioni, link ad altri siti e altro materiale pubblicizzato appartengono ai legittimi proprietari.

Le informazioni contenute nella presentazione, ideata e realizzata dal relatore, non costituiscono una consulenza tecnica sui temi trattati. I contenuti espressi sono frutto di interpretazione e opinione di A.C. & E. Srl, da non considerare quindi come ufficiali e/o univoci.
Gli esempi e le informazioni illustrate nella presentazione sono riportate in modo parziale ed hanno una mera valenza indicativa e non devono pertanto essere intese come esaustive o complete. Il materiale è propedeutico all'attività di consulenza e/o assistenza tecnica di A.C.&E.

La nostra storia

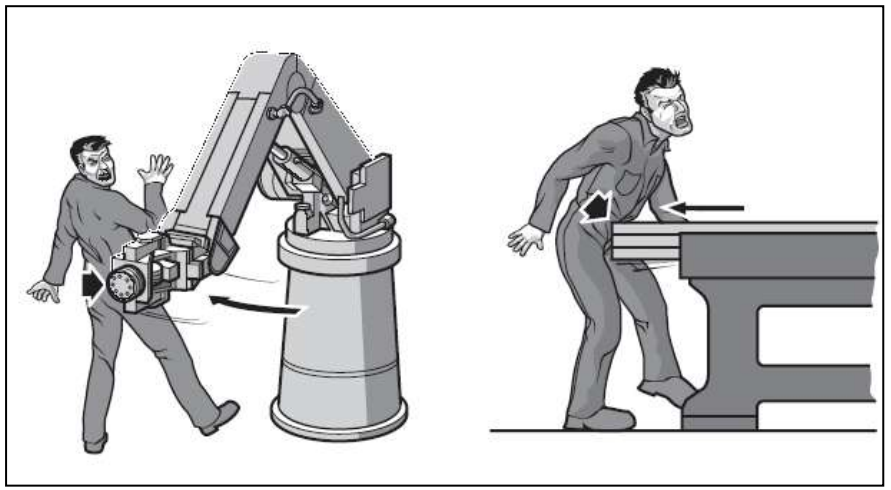


MACHINE SAFETY

Sicurezza Elettrica e sicurezza operatore

- 29 CFR (Code of Federal Regulation) 1910 and Osha applicable standards
- Electrical safety

≠

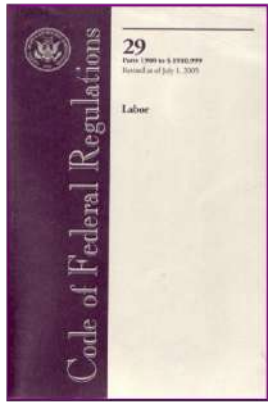



O
S
H
A
OCCUPATIONAL
SAFETY
HEALTH
ADMINISTRATION

29 CFR 1910

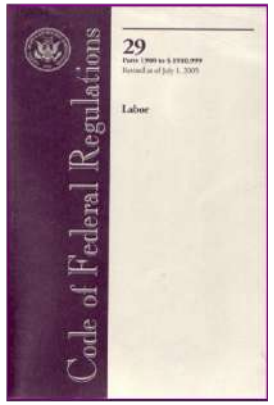

REGLOGIC
PREMIUM
January 2020
29 CFR
1910 OSHA
GENERAL INDUSTRY REGULATIONS & STANDARDS
As required by the U.S. Department of Labor, Occupational Safety and Health Administration
regs2go.com
Regulations on the go from any smartphone!
See inside for details.

29 CFR 1910



- 1910 - Table of Contents
- 1910 Subpart A – General
- 1910 Subpart B - Adoption and Extension of Established Federal Standards
- 1910 Subpart C – Reserved
- 1910 Subpart D - Walking-Working Surfaces
- 1910 Subpart E - Exit Routes and Emergency Planning
- 1910 Subpart F - Powered Platforms, Manlifts, and Vehicle-Mounted Work Platforms
- 1910 Subpart G - Occupational Health and Environmental Control
- 1910 Subpart H - Hazardous Materials
- 1910 Subpart I - Personal Protective Equipment
- 1910 Subpart J - General Environmental Controls

29 CFR 1910

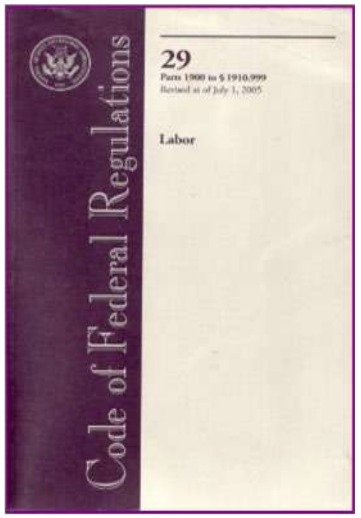


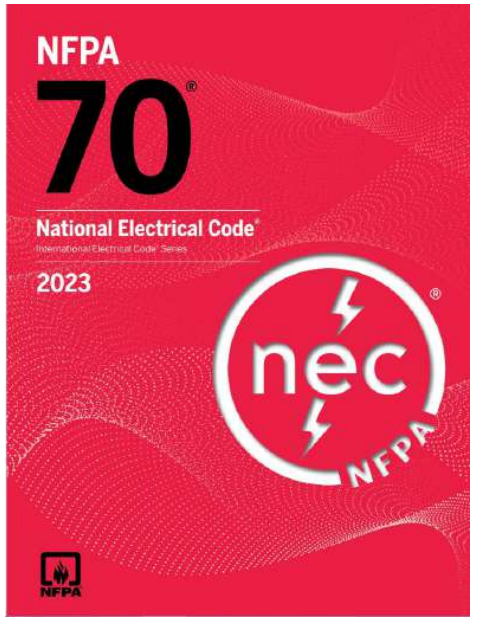
- 1910 Subpart K - Medical and First Aid
- 1910 Subpart L - Fire Protection
- 1910 Subpart M - Compressed Gas and Compressed Air Equipment
- 1910 Subpart N - Materials Handling and Storage
- 1910 Subpart O - Machinery and Machine Guarding
- 1910 Subpart P - Hand and Portable Powered Tools and Other Hand-Held Equipment
- 1910 Subpart Q - Welding, Cutting and Brazing
- 1910 Subpart R - Special Industries
- 1910 Subpart S – Electrical
- 1910 Subpart Z - Toxic and Hazardous Substances

29 CFR 1910

OSHA

- 1910 Subpart S – Electrical





NFPA70 / NEC (National Electrical Code)

NIOSH

NFPA70 / NEC (National Electrical Code)

NFPA70: SCOPE

*"… minimizing the risk of electricity as a source of electric shock and as a **potential ignition source** of **fires** and **explosions**;*

*minimizing the propagation of **fire** and **explosions** due to electrical's installations.»*

Art. 90.1 NFPA70HB (comm. text)

(C) Installations Covered.

This *Code* covers the installation and removal of electrical conductors, equipment, and raceways; signaling and communications conductors, equipment, and raceways; and optical fiber cables for the following:

(1) Public and private premises, including buildings, structures, mobile homes, recreational vehicles, and floating buildings

(2) Yards, lots, parking lots, carnivals, and industrial substations

(3) Installations of conductors and equipment that connect to the supply of electricity

(4) Installations used by the electric utility, such as office buildings, warehouses, garages, machine shops, and recreational buildings, that are not an integral part of a generating plant, substation, or control center

(5) Installations supplying shore power to ships and watercraft in marinas and boatyards, including monitoring of leakage current

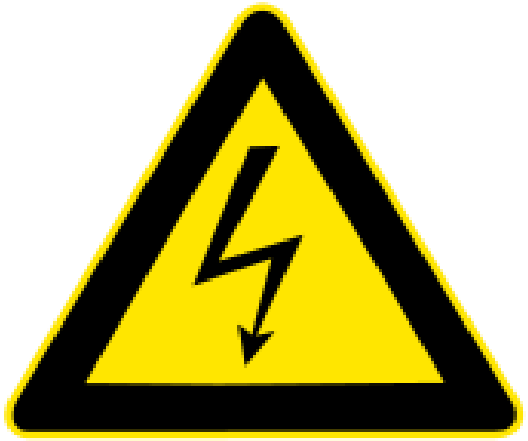
(6) Installations used to export electric power from vehicles to premises wiring or for bidirectional current flow

NFPA70 / NEC (National Electrical Code)

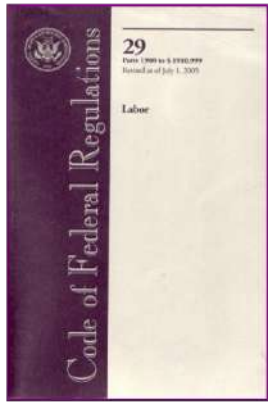
Il sistema ispettivo

Authority Having Jurisdiction (**AHJ**)

Fire and electrical shock



OSHA®



National Institute for Occupational Safety and Health
NIOSH®

L'AHJ
Authority Having Jurisdiction

«Generally they are local building inspectors, mechanical inspectors, fire marshals, and

the like who are ultimely responsible for the compliance of products, devises, or

systems being installed in buildings in accordance with he the governing Codes.»

NFPA70 / NEC (National Electrical Code)

AHJ: NEC art. 90.4

90.4 Enforcement.

(A) Application.

This *Code* is intended to be suitable for mandatory application by governmental bodies that exercise legal jurisdiction over electrical installations, including signaling and communications systems, and for use by insurance inspectors.

(B) Interpretations.

The authority having jurisdiction for enforcement of the Code has the responsibility for making interpretations of the rules, for deciding on the approval of equipment and materials, and for granting the special permission contemplated in a number of the rules.

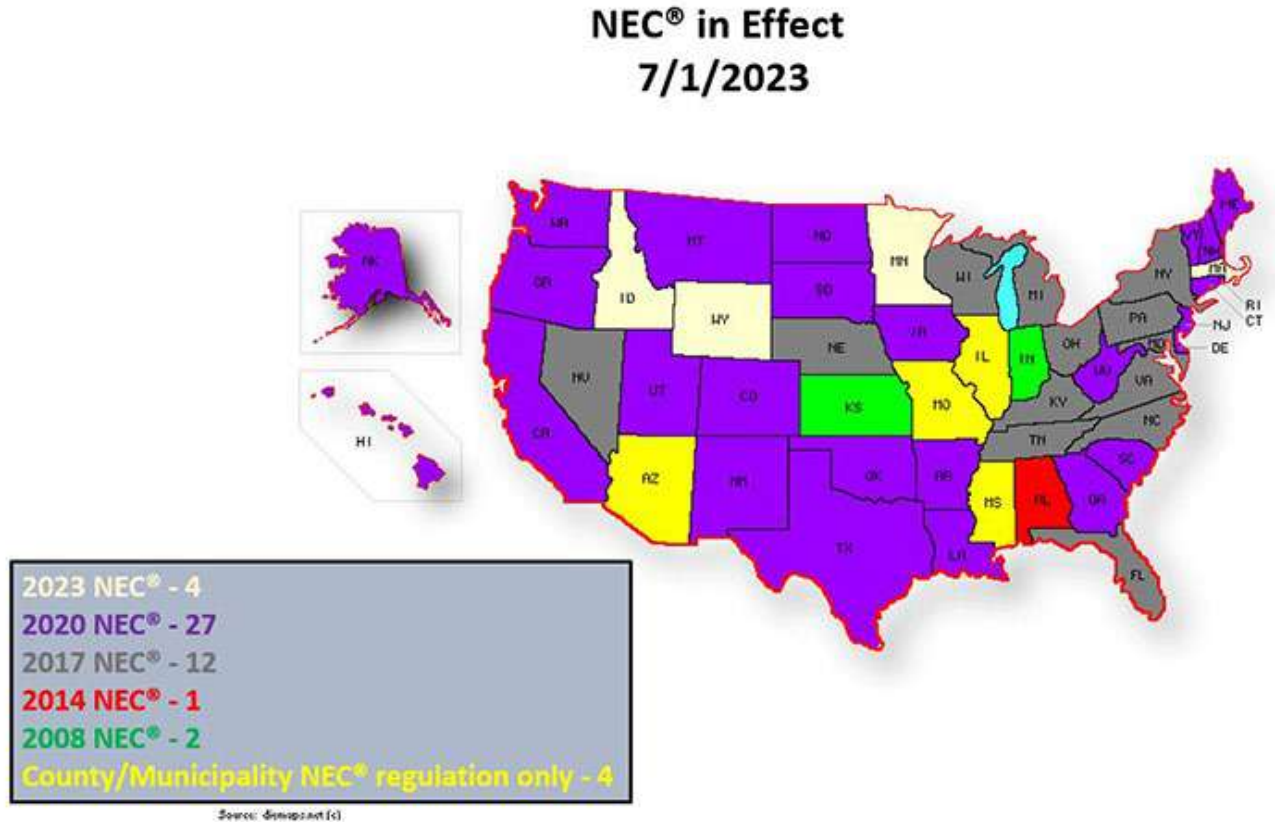
NFPA70 / NEC (National Electrical Code)

Recepimento

al **01 Luglio 2023**:

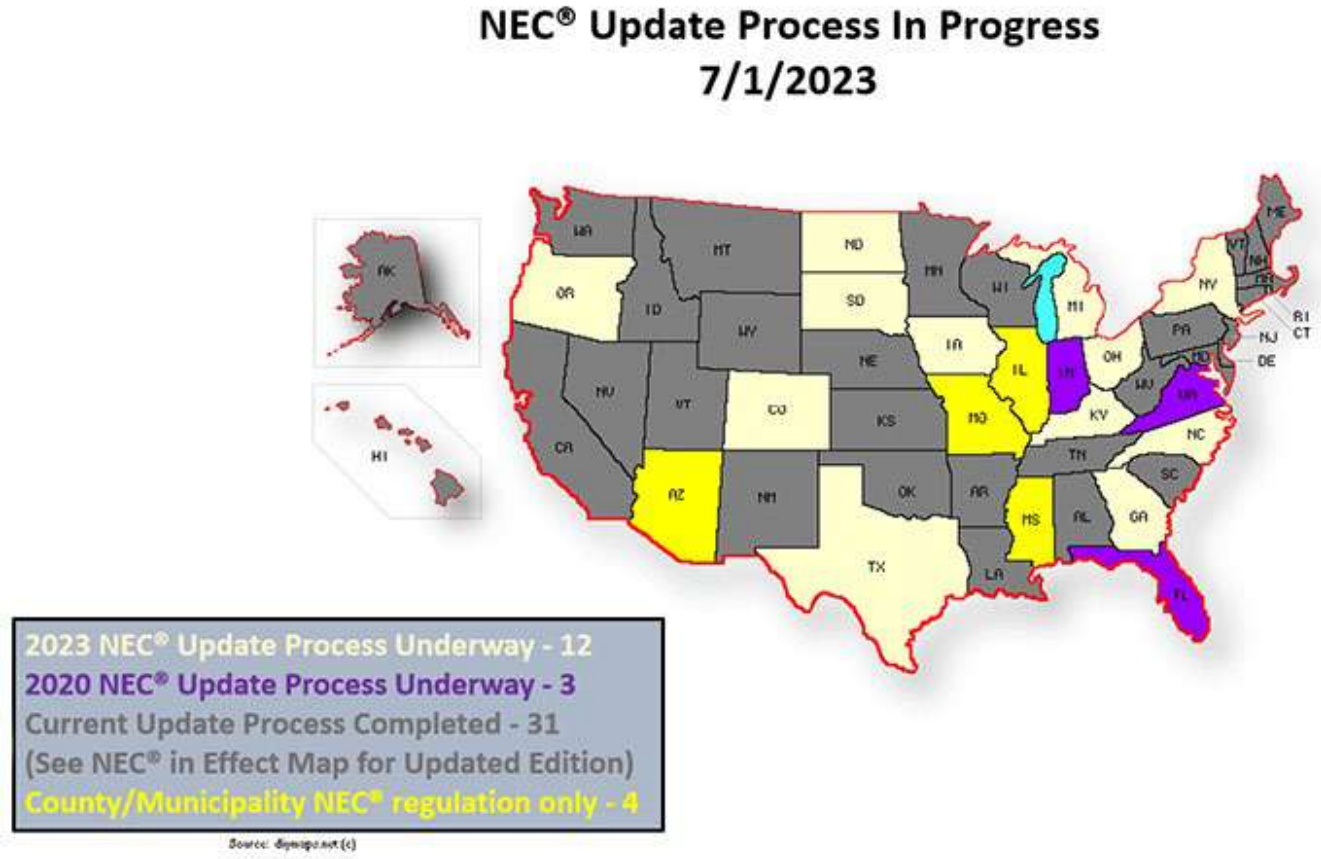
4 Stati con il 2023

27 stati hanno completato il recepimento del NEC2020



Learn where the National Electrical Code® (NEC®) is enforced. | NFPA www.nfpa.org

NFPA70 / NEC (National Electrical Code)



Learn where the National Electrical Code® (NEC®) is enforced. | NFPA www.nfpa.org

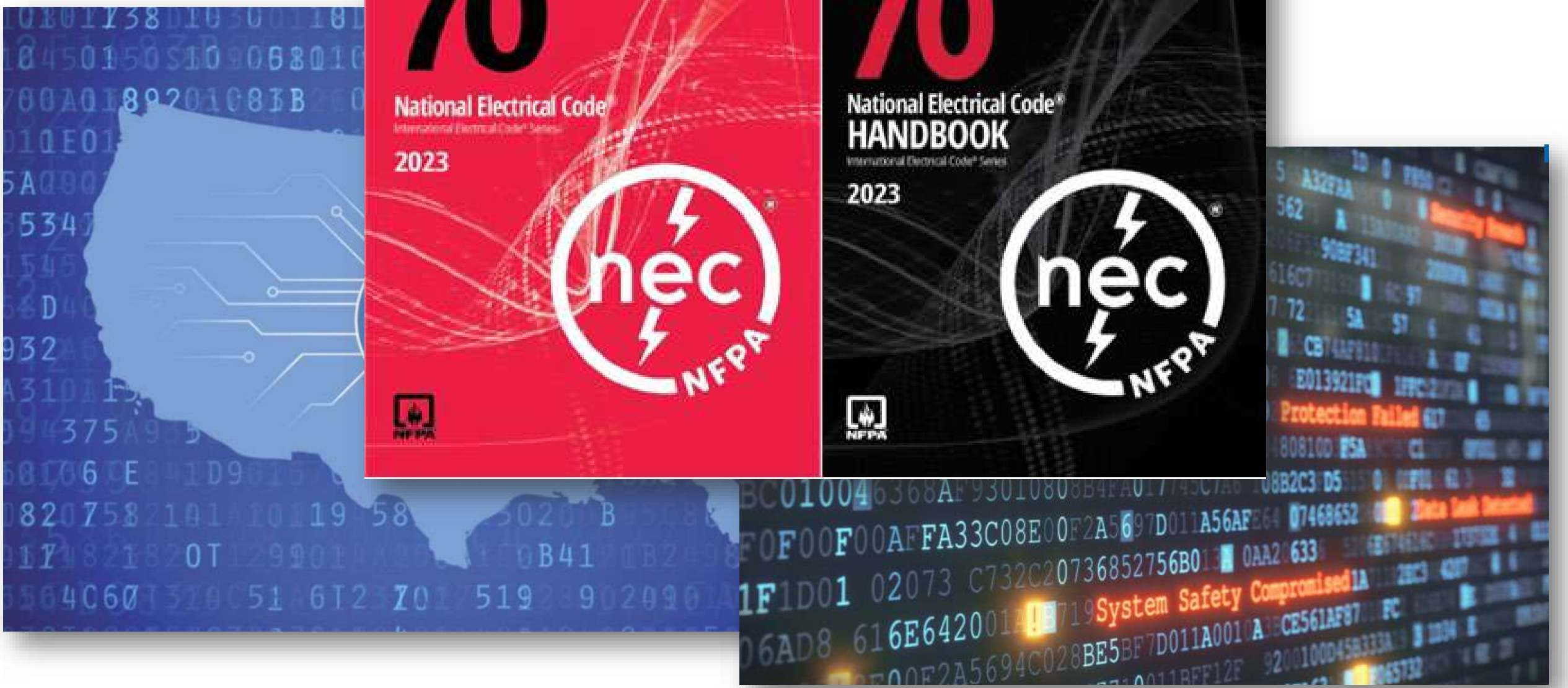
Obbligatorio nei seguenti stati:

1	Georgia	2020 with GA amendments (1/1/2021)	2023 update process underway (Projected 1/1/2025)
2	Iowa	2020 with IA amendments (4/1/2021)	2023 update process underway (projected 1/1/2024)
3	Massachusetts	2023 with MA amendments (2/17/2023)	
4	Michigan	2017 Commercial (1/4/2019) One- and two-family dwellings (2/8/2016)	2023 update process underway (effective date not established)
5	Minnesota	2023 (7/1/2023)	
6	New York	2017 (5/12/2020)	2023 update process underway (Effective date not established)
7	North Carolina	2020 with NC amendments for other than one- and two-family dwellings (11/1/21)	2023 update process underway (Projected 7/1/2024)
8	North Dakota	2020 (1/1/2021)	2023 update process underway (effective date not established)
9	Ohio	Commercial (11/1/2017) 2017, with Ohio amendments One-, two- and three-family dwellings (7/1/2019)	2023 update process underway for commercial & one-, two-, and three-family dwellings (Effective date projected first quarter of 2024)
10	Oregon	2020 with OR amendments (4/1/2021)	2023 update process underway (Projected 10/1/2023)
11	Texas	2020 (11/1/2020)	2023 update process underway (Projected 9/1/2023)
12	Wyoming	2023 (7/1/2023)	

Advanced

CONFINDUSTRIA VENETO EST
Area Metropolitana
Venezia Padova Rovigo Treviso

ac&e



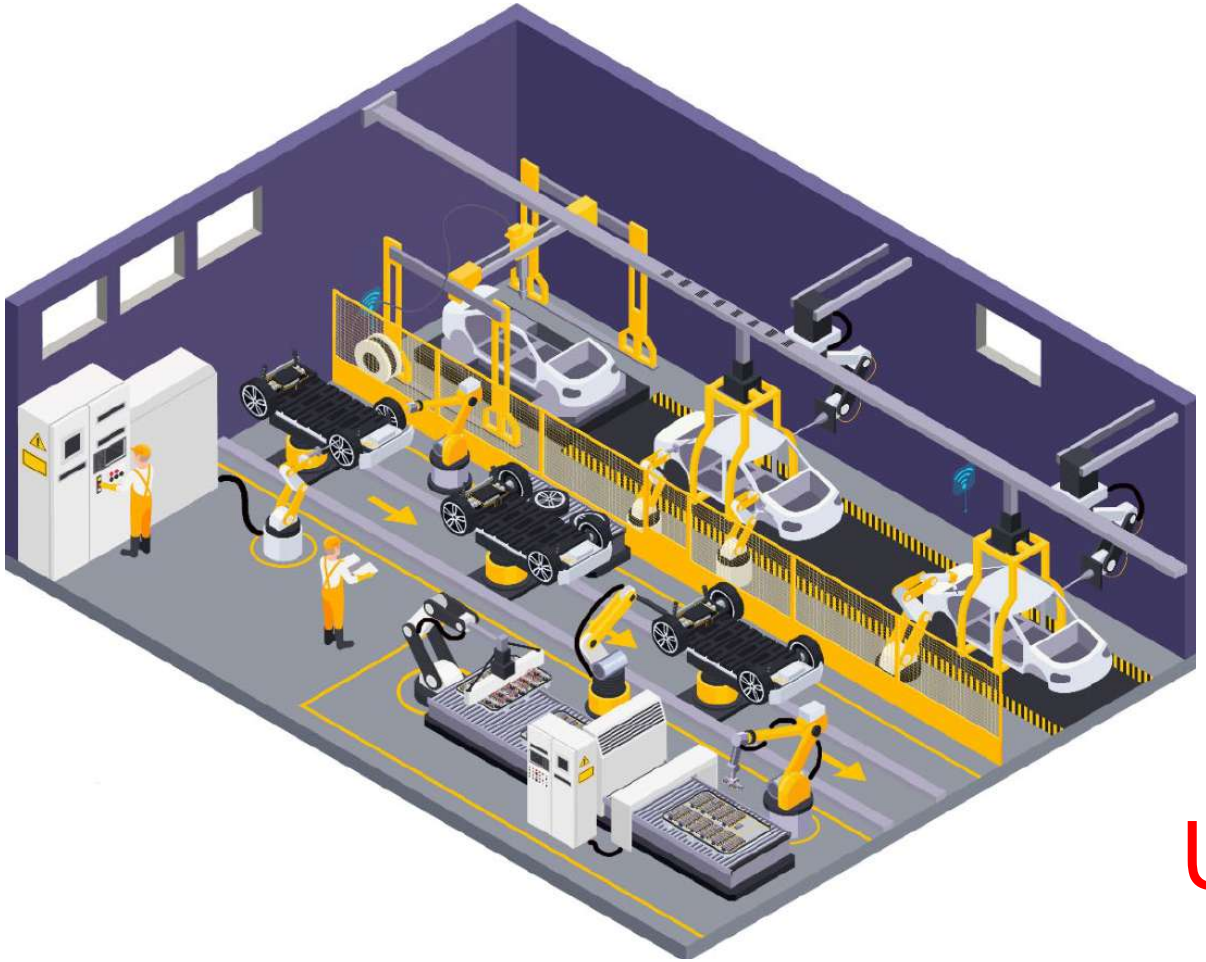
NEC 2023 Non solo UL508A

Advanced

CONFINDUSTRIA VENETO EST
Area Metropolitana
Venezia Padova Rovigo Treviso

NEC 2023 Non solo UL508A

ac&e



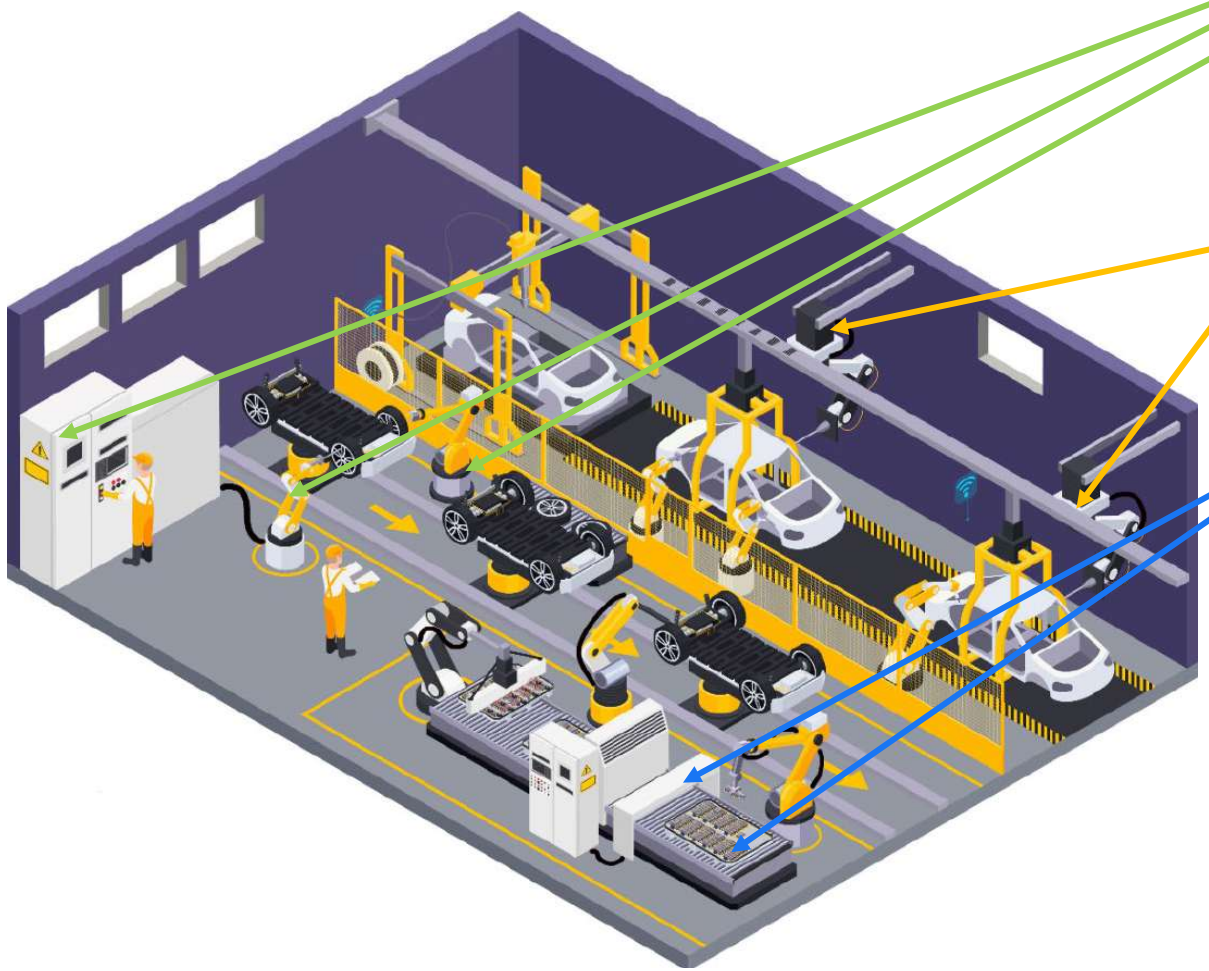
Cosa significa essere

«NEC compliant»?

NON ESISTE SOLO LA
UL 508A Industrial Control
Panels

NEC 2023 Non solo UL508A

Definitions

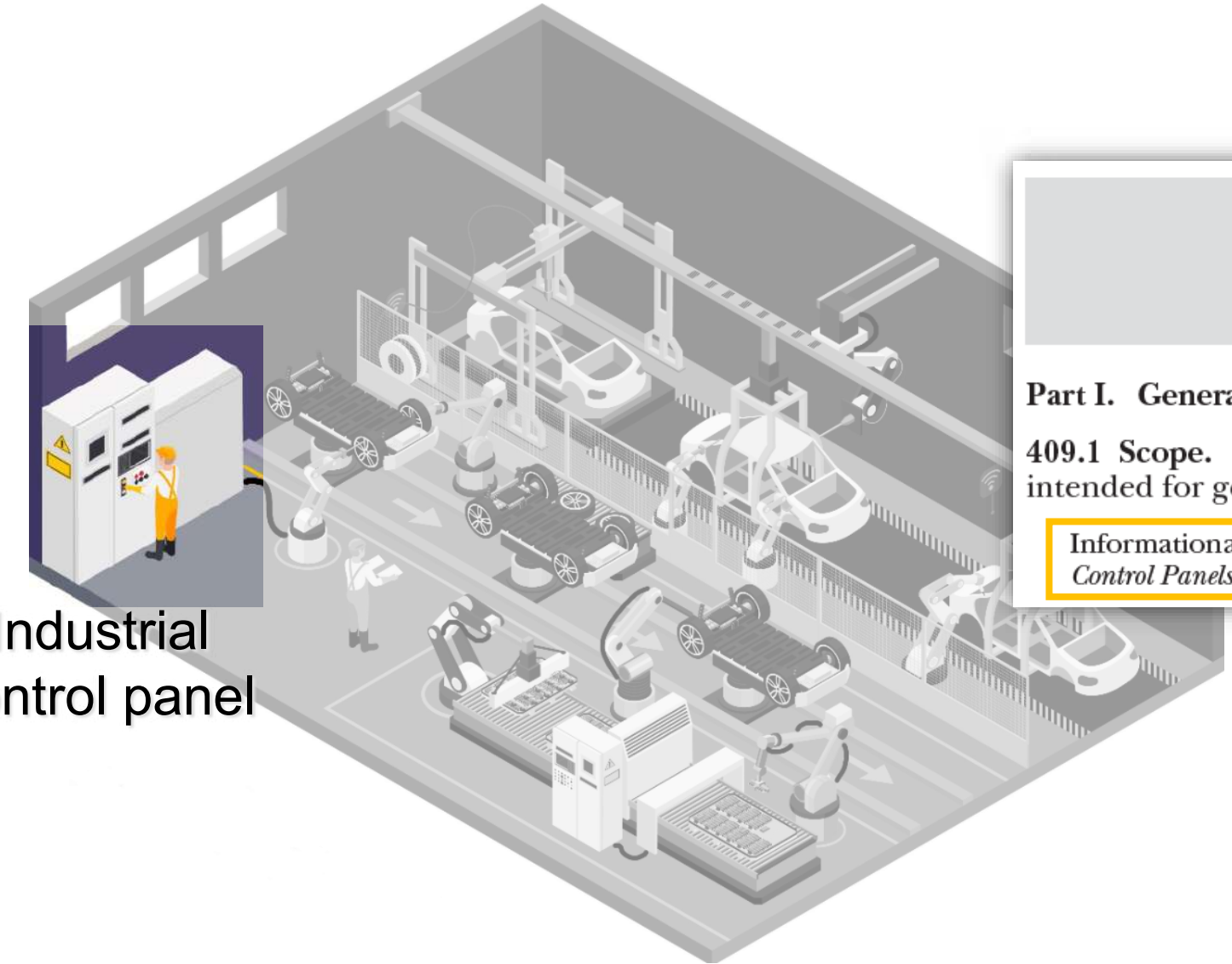


Equipment. A general term, including fittings, devices, appliances, luminaires, apparatus, machinery, and the like used as a part of, or in connection with, an electrical installation. (CMP-1)

Building. A structure that stands alone or that is separated from adjoining structures by fire walls. (CMP-1)

Structure. That which is built or constructed, other than equipment. (CMP-1)

NEC 2023 Non solo UL508A



Industrial control panel

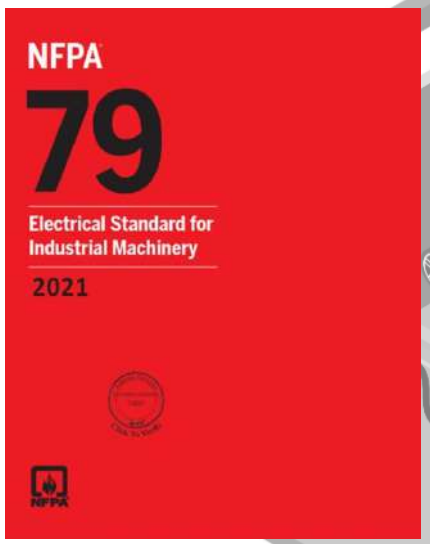
ARTICLE 409
Industrial Control Panels

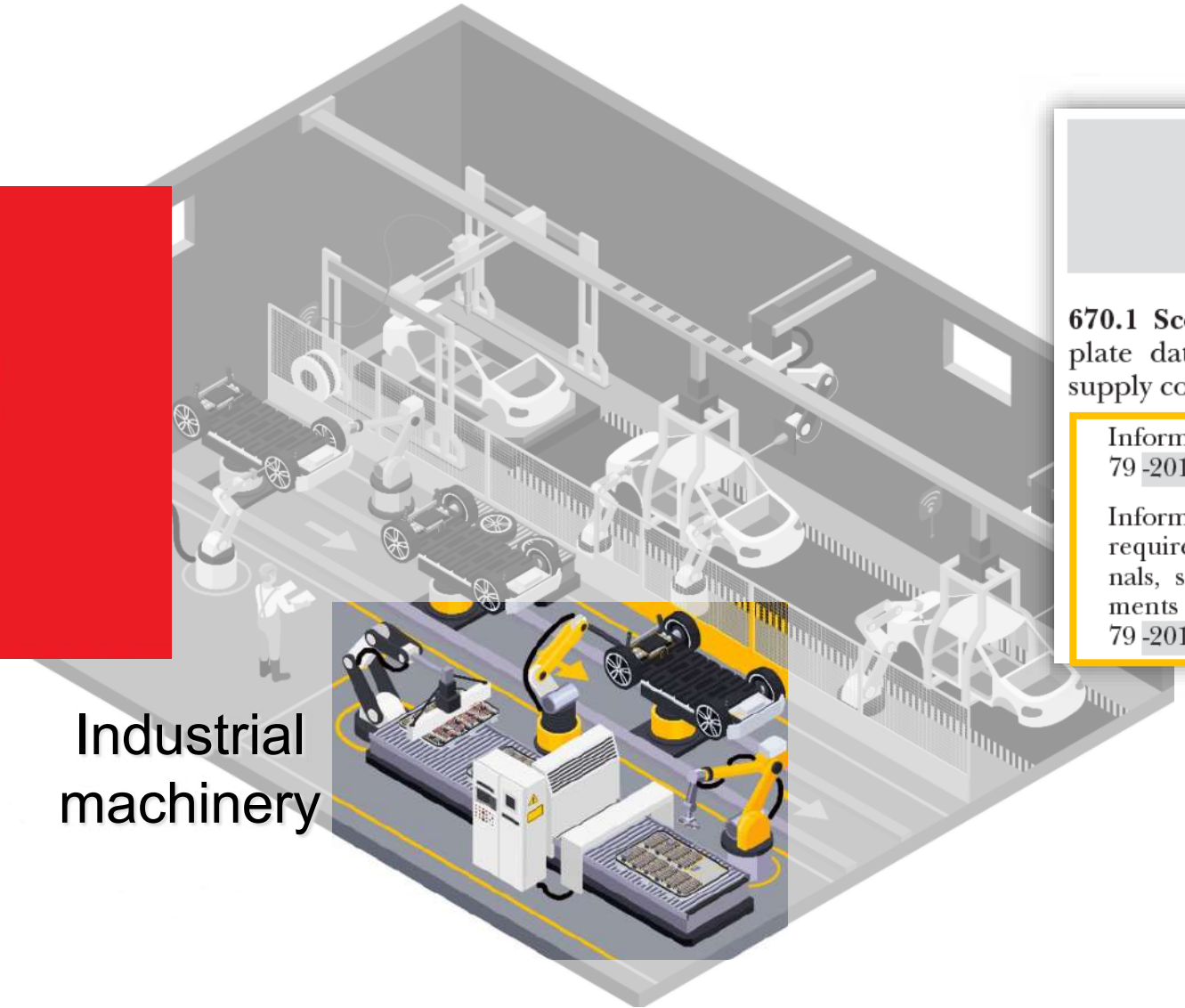
Part I. General

409.1 Scope. This article covers industrial control panels intended for general use and operating at 1000 volts or less.

Informational Note: ANSI/UL 508A, *Standard for Industrial Control Panels*, is a safety standard for industrial control panels.

NEC 2023 Non solo UL508A





Industrial machinery

ARTICLE 670
Industrial Machinery

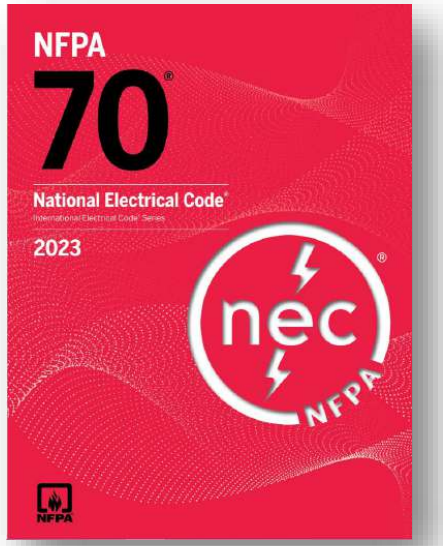
670.1 Scope. This article covers the definition of, the name-plate data for, and the size and overcurrent protection of supply conductors to industrial machinery.

Informational Note No. 1: For further information, see NFPA 79 -2015, *Electrical Standard for Industrial Machinery.*

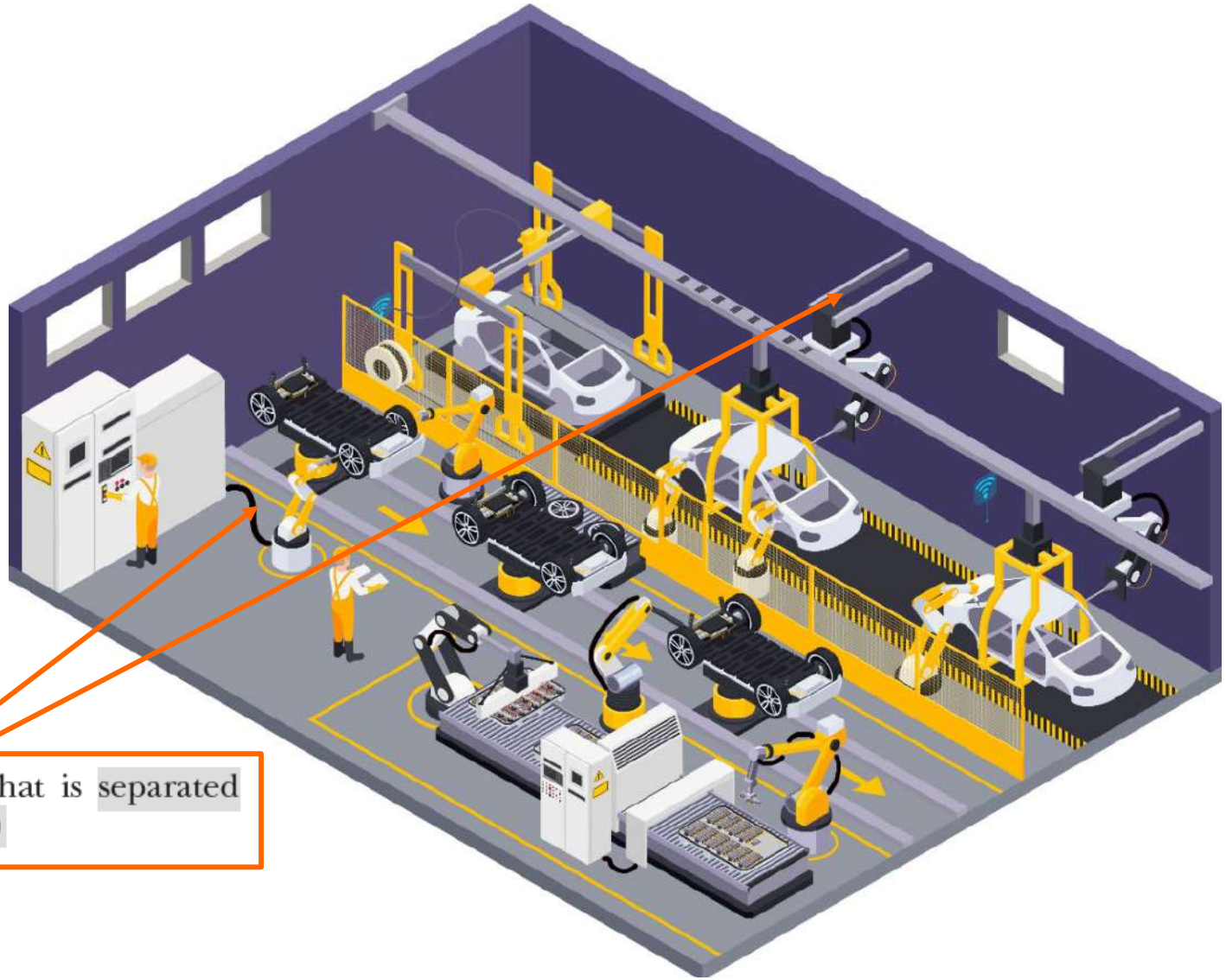
Informational Note No. 2: For information on the workspace requirements for equipment containing supply conductor terminals, see 110.26. For information on the workspace requirements for machine power and control equipment, see NFPA 79 -2015, *Electrical Standard for Industrial Machinery.*

NEC 2023 Non solo UL508A

Interconnecting wiring
Building
But not only…



Building. A structure that stands alone or that is separated from adjoining structures by fire walls. (CMP-1)




NFPA
70
National Electrical Code
2023
nec
NFPA
AI
ac&e

NEC 2023 Non solo UL508A

Art. 110.3

Nuovo scopo

Cyber security

110.3 Examination, Identification, Installation, Use, and Listing (Product Certification) of Equipment.

(A) Examination.

In judging equipment, considerations such as the following shall be evaluated:

(8) Cybersecurity for network-connected life safety equipment to address its ability to withstand unauthorized updates and malicious attacks while continuing to perform its intended safety functionality

Informational Note No. 3: See the ANSI/ISA 62443 series of standards for industrial automation and control systems, the UL 2900 series of standards for software cybersecurity for network-connectable products, and UL 5500, *Standard for Remote Software Updates*, which are standards that provide frameworks to mitigate current and future security cybersecurity vulnerabilities and address software integrity in systems of electrical equipment.

Art. 110.3

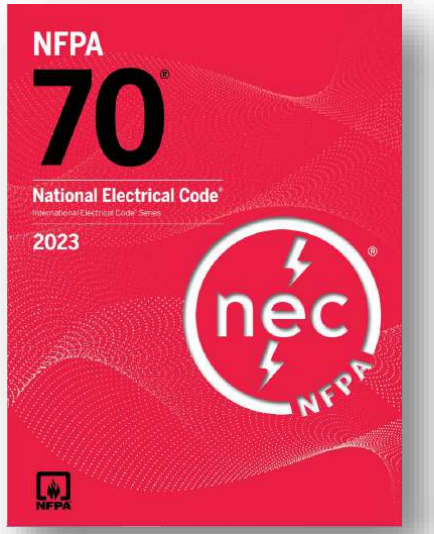
Formato della documentazione

(B) Installation and Use.

Equipment that is listed, labeled, or both, or identified for a use shall be installed and used in accordance with any instructions included in the listing, labeling, or identification.

Informational Note: The installation and use instructions may be provided in the form of printed material, quick response (QR) code, or the address on the internet where users can download the required instructions.

NEC 2023 Cyber Security



(8) Cybersecurity for network-connected life safety equipment to address its ability to withstand unauthorized updates and malicious attacks while continuing to perform its intended safety functionality

Informational Note No. 3: See the ANSI/ISA 62443 series of standards for industrial automation and control systems, the UL 2900 series of standards for software cybersecurity for network-connectable products, and UL 5500, *Standard for Remote Software Updates*, which are standards that provide frameworks to mitigate current and future security cybersecurity vulnerabilities and address software integrity in systems of electrical equipment.

Rapporto Clusit 2023: le aziende manifatturiere italiane nel mirino dei criminali informatici

Cresce ancora l'allarme Cyber Security.

La pressione degli attacchi è più alta nelle realtà industriali, nei servizi professionali e nel comparto tecnico-scientifico.

In 8 casi su 10 conseguenze molto gravi per il business.

Tutti i dati nel report annuale dell'associazione

Nel periodo che prenderemo in esame, tra gennaio 2018 e dicembre 2022 si sono verificati un totale di 9.633 cyber attacchi, così suddivisi:

Fig. 1: *Andamento dei cyber attacchi nel periodo 2018 - 22*

OT Security Scenario Italia

Rapporto sullo stato della cybersecurity

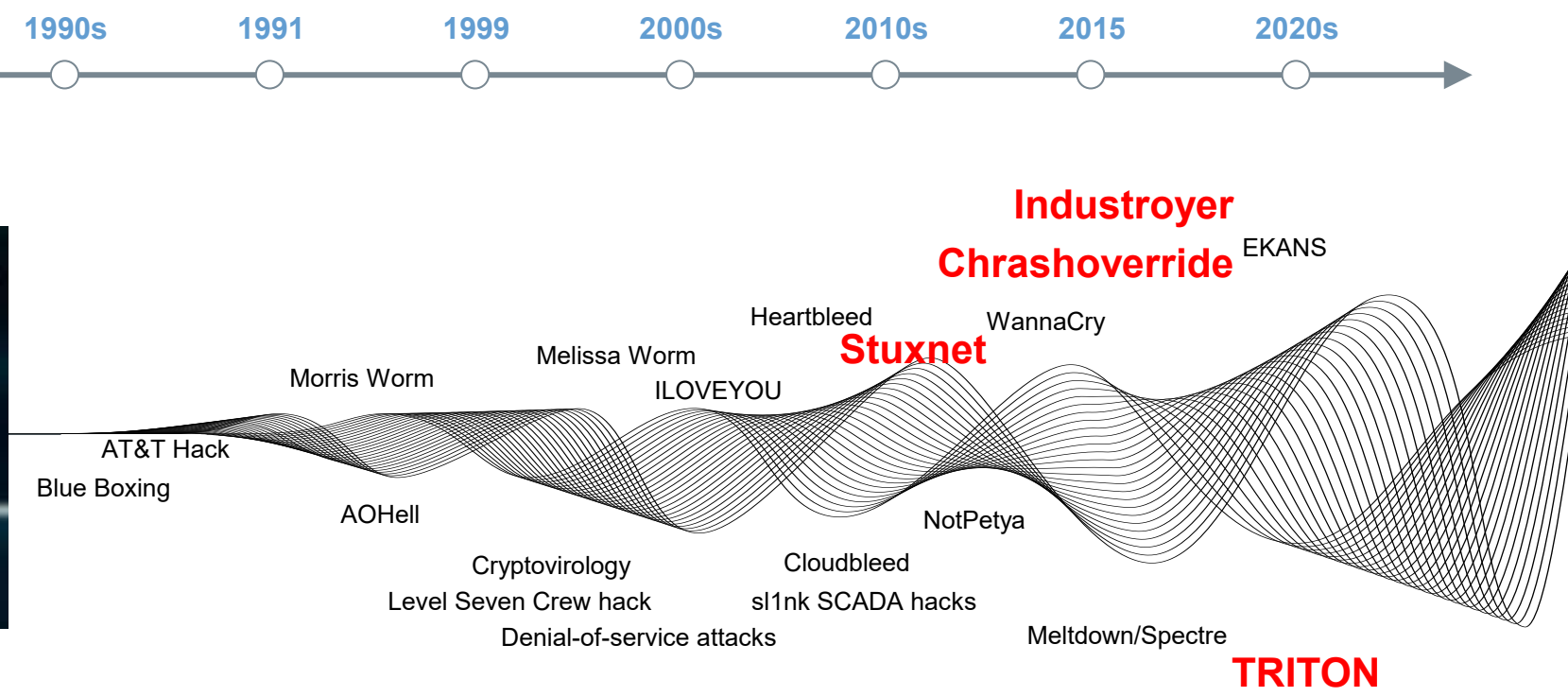
…gli ultimi anni sono stati caratterizzati da un intensificarsi degli attacchi informatici a livello globale. Ma se nel mondo la crescita è del 20%, ***per quanto riguarda l'Italia il numero di incidenti informatici cresce a tripla cifra: +169%.*** *E questo nonostante un significativo aumento dei budget destinati alla sicurezza. Per dare un'idea delle dimensioni del fenomeno, basti sapere che il 7,6% di tutti gli attacchi informatici registrati a livello globale vedeva come vittime enti o aziende italiane.*

Non parliamo tra l'altro di incidenti di poca entità: ***nell'83% dei casi si tratta di attacchi di gravità elevata o critica*** *(la media globale è dell'80%).*

Link:

https://edge9.hwupgrade.it/news/security/clusit-l-italia-sotto-attacco_114719.html

IL PANORAMA DEGLI ATTACCHI AL MONDO INDUSTRIALE

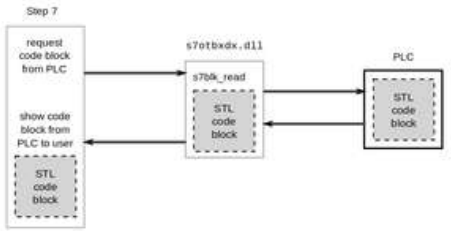


Stuxnet: il malware che fece conoscere al mondo la guerra cibernetica

Cosa è Stuxnet

Il worm Stuxnet è apparso per la prima volta durante l'estate del 2010. Si tratta di un worm informatico dal peso di soli 500 kilobyte che si è infiltrato in numerosi sistemi informatici. Questo worm ha operato in tre fasi. Innanzitutto, ha analizzato e preso di mira reti Windows e sistemi informatici e successivamente si è diffuso all'interno della rete informatica per poi colpire i sistemi per il quale era stato progettato. Le centrifughe di arricchimento dell'Uranio, gestite dai **Programmable logic controller (PLC).**

Il worm, una volta infiltrato in queste macchine, ha iniziato a replicarsi infiltrandosi all'interno del software **Siemens Step7 basato su Windows.** Questo sistema software della **Siemens e**ra e continua ad essere **un software diffuso all'interno delle reti informatiche industriali,** come ad esempio gli impianti di arricchimento dell'uranio.



Schema logico del software Step7 di Siemens

Compromettendo il software Step7, il worm ha avuto accesso ai **Programmable logic controller (PLC)** e questo **p**assaggio finale ha permesso al worm di manipolare informazioni industriali cruciali, oltre ad acquisire la capacità di utilizzare diversi macchinari nei singoli siti industriali.

Il processo di replica è ciò che ha reso il worm così diffuso. Era così invasivo che se una chiavetta USB fosse stata collegata ad un sistema informatico dove era presente al suo interno, il worm si sarebbe spostato dal dispositivo USB e avrebbe iniziato a diffondersi su tutti i successivi sistemi informatici a cui l'USB era stata collegata, come all'interno delle reti Air Gap, ovvero quelle reti isolate che non possono essere raggiunte da internet.

> Valutare

SIMATIC WinCC / SIMATIC PCS 7: Informazioni su malware / virus / cavalli di Troia

Iscrizione | Prodotti associati)

Qui forniamo informazioni sugli ultimi sviluppi e sulle misure consigliate da Siemens per la gestione di Stuxnet. ...

Qui forniamo informazioni sugli ultimi sviluppi e sulle misure consigliate da Siemens per la gestione di Stuxnet.

Contenuti

- Stato attuale dei computer infetti
- Procedura consigliata per identificare e rimuovere un'infezione da Stuxnet
- Ulteriori informazioni tecniche
  - Nota importante sull'uso di programmi antivirus per i file compressi
  - Informazioni sui controllori SIMATIC CPU 315-2 e CPU 417
  - Compatibilità degli aggiornamenti Microsoft con le applicazioni SIMATIC
- Download
  - Strumento per identificare e rimuovere Stuxnet
  - Strumento di aggiornamento della sicurezza SIMATIC
  - Aggiornamenti Microsoft

Aggiornato Stato attuale dei computer infetti

11.03.2011 Ad oggi un totale di 24 clienti Siemens nel settore industriale in tutto il mondo hanno riferito di essere stati infettati dal cavallo di Troia. Il malware è stato in grado di essere rimosso in tutti i casi. In nessuno di questi casi l'infezione ha avuto un impatto negativo sulla soluzione di automazione.

Procedura consigliata per identificare e rimuovere un'infezione da Stuxnet

Si consiglia di esaminare i seguenti tipi di computer:

A. Sistemi embedded (es. Microbox)

B. Altri computer

- Computer dell'infrastruttura (file server, controller di dominio, altri server...)
- Computer con e senza installazione di WinCC
- Macchine virtuali (es. installazioni VMWARE)

Procedere come di seguito per attuare le varie misure.

Triton è un malware scoperto per la prima volta in un impianto petrolchimico dell'Arabia Saudita nel 2017. [1] [2] Può disabilitare i sistemi strumentali di sicurezza, che possono quindi contribuire a un disastro dell'impianto. È stato definito "il malware più micidiale del mondo".

Nel dicembre 2017, è stato riferito che i sistemi di sicurezza di una centrale elettrica non identificata, che si ritiene si trovasse in Arabia Saudita , sono stati compromessi quando la tecnologia di sicurezza industriale Triconex prodotta da Schneider Electric SE è stata presa di mira in quello che si ritiene sia stato un attacco sponsorizzato dallo stato .

La società di sicurezza informatica Symantec ha affermato che il malware , noto come "Triton", ha sfruttato una vulnerabilità nei computer che eseguono il sistema operativo Microsoft Windows .

Nel 2018, FireEye, una società che si occupa di ricerca sulla sicurezza informatica, ha riferito che il malware molto probabilmente proveniva dal Central Scientific Research Institute of Chemistry and Mechanics (CNIIHM), un'entità di ricerca in Russia.

Malware Industroyer

(conosciuto anche con il nome di *CrashOverRide*) che, a cavallo dell'inverno 2016, ha messo in ginocchio la rete elettrica ucraina, provocando un blackout e lasciando al buio (e al freddo) milioni di persone.

Secondo gli esperti di sicurezza di ESET e di Dragos, due delle maggiori società attive nel settore della *cybersecurity*,

Industroyer è la minaccia più rilevante per grandi sistemi industriali dai tempi di **Stuxnet**, il malware ideato dall'i*ntelligence* statunitense e israeliana per sabotare il piano di sviluppo nucleare dell'Iran.

CONTENUTO PER GLI ABBONATI PREMIUM

Le scarpe di Ganna sotto attacco hacker. Northwave paralizzata, lavoratori a casa

L'azienda trevigiana ferma da lunedì, si cerca di ripartire con i server di backup. In attesa, smaltimento ferie per i dipendenti

FABIO POLONI

31 Agosto 2023 alle 06:53 | 2 minuti di lettura

La sede della Northwave a Pederobba e a destra Filippo Ganna, ciclista testimonial di punta dell'azienda, con le scarpe Northwave ai piedi

La scoperta lunedì mattina, come spesso accade in questi casi: **computer fuori uso, rete paralizzata, attività bloccata**. **La Northwave è sotto attacco hacker**, pesante, come negli ultimi mesi è successo a nomi del calibro di Benetton, Geox, Luxottica solo per citare la vistosissima punta dell'iceberg.

Al **quartier generale di Pederobba** sono ore, giorni di lavoro febbrile per cercare di rimettere in piedi l'infrastruttura digitale che sorregge l'attività: **si punta a salvare il salvabile grazie ai server di backup mantenuti provvidenzialmente offline**, al di fuori della portata dei pirati informatici.

Nel frattempo, in attesa di risolvere la situazione – potrebbero volerci ancora un paio di giorni, nell'ipotesi più ottimistica – **tutti a casa: lavoratori in smaltimento ferie**, «siamo solamente io e il tecnico informatico», dice cortesemente la centralinista al telefono, «gli altri, una trentina, sono tutti a casa».

Attacco e ripristino

L'obiettivo dei cyber-criminali non è l'attacco frontale, bensì l'accesso a qualche "porta esterna", più vulnerabile. **Difendersi è molto difficile, quasi impossibile**: prima o poi verrai colpito, è praticamente un dato di fatto. Detto ciò, devi essere in grado di tornare online prima possibile: il tempo di reazione misura la tua impreparazione e quanto gli hacker sono riusciti a colpirti a fondo. Non si resetta tutto in due ore, in media per tornare online ne servono almeno 72.

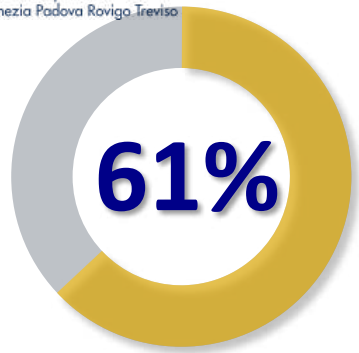
Precauzioni? Zero trust, non fidarsi di nessuno, e poi tecnologia e formazione del personale, perché **l'errore o l'imprudenza umana possono fare più danni di un "baco"**. Dopo l'attacco, è necessario ripulire l'organismo digitale dal virus, ma non è semplice: vanno ricreati tutti i server e i pc dopo aver verificato che il cryptolocker non sia ancora in rete. Gli attacchi spesso rimangono silenti per mesi: tra il momento dell'intrusione del virus e quello in cui fa danni passano in media duecento giorni, è quella che in gergo si chiama finestra di compromissione.

31 Agosto

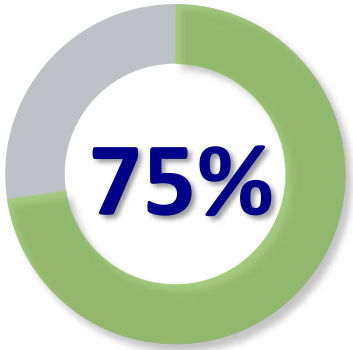
Onigo di Pederobba (TV)

https://tribunatreviso.gelocal.it/regione/2023/08/31/news/ciclismo_ganna_northwave_hacker-13019483/?ref=pay_amp

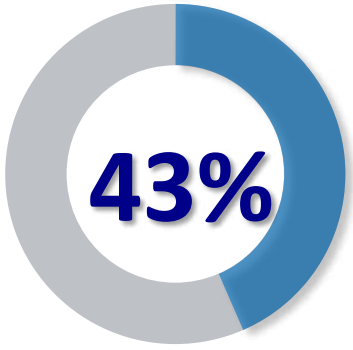
Many manufacturing companies have experienced critical cyber breaches



of Manufacturers have come across cybersecurity incidents

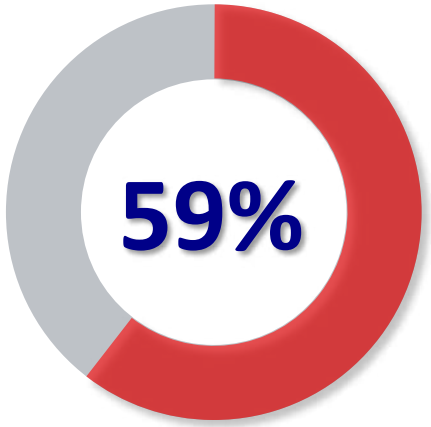


of cyber incidents have blocked production



of cyber incidents have blocked production

for more than 4 days



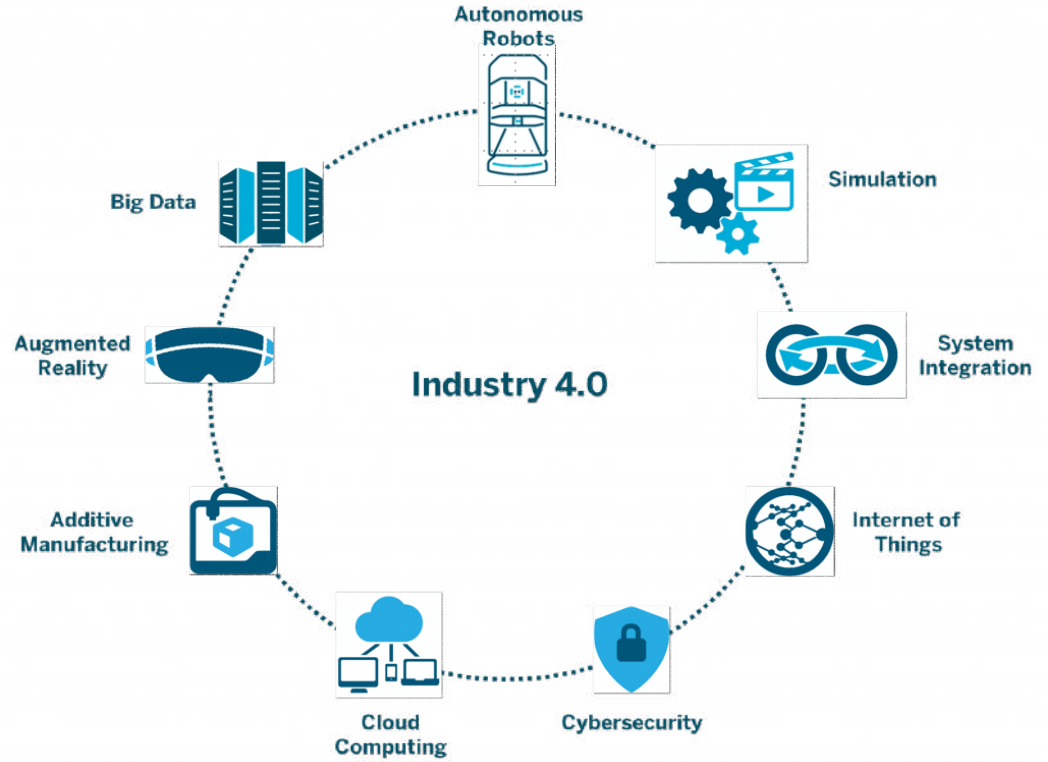
of respondents said the biggest challenge in OT Cybersecurity is the lack of ICS Cybersecurity solutions designed for industrial systems and devices.

Source: https://resources.trendmicro.com/Industrial-Cybersecurity-WP.html

Trend Micro 2021 OT security survey, 500 respondents in US (200), Germany (150), and Japan (150)

Quindi … adesso ….
Cyber security….

industry 4.0


Autonomous Robots
Simulation
System Integration
Internet of Things
Cybersecurity
Cloud Computing
Additive Manufacturing
Augmented Reality
Big Data
Industry 4.0


Cybersecurity
admin

DIFFERENZA TRA SAFETY e SECURITY

SAFETY

Con il termine “safety” si definiscono le misure che permettono di essere protetti o di proteggere da ciò che può causare danno o provocare la perdita di vite umane.

SECURITY

Con il termine “security” si definisce la protezione di individui, organizzazioni o asset da minace esterne ovvero da un possibile attacco.

IEC TR 63074:2019

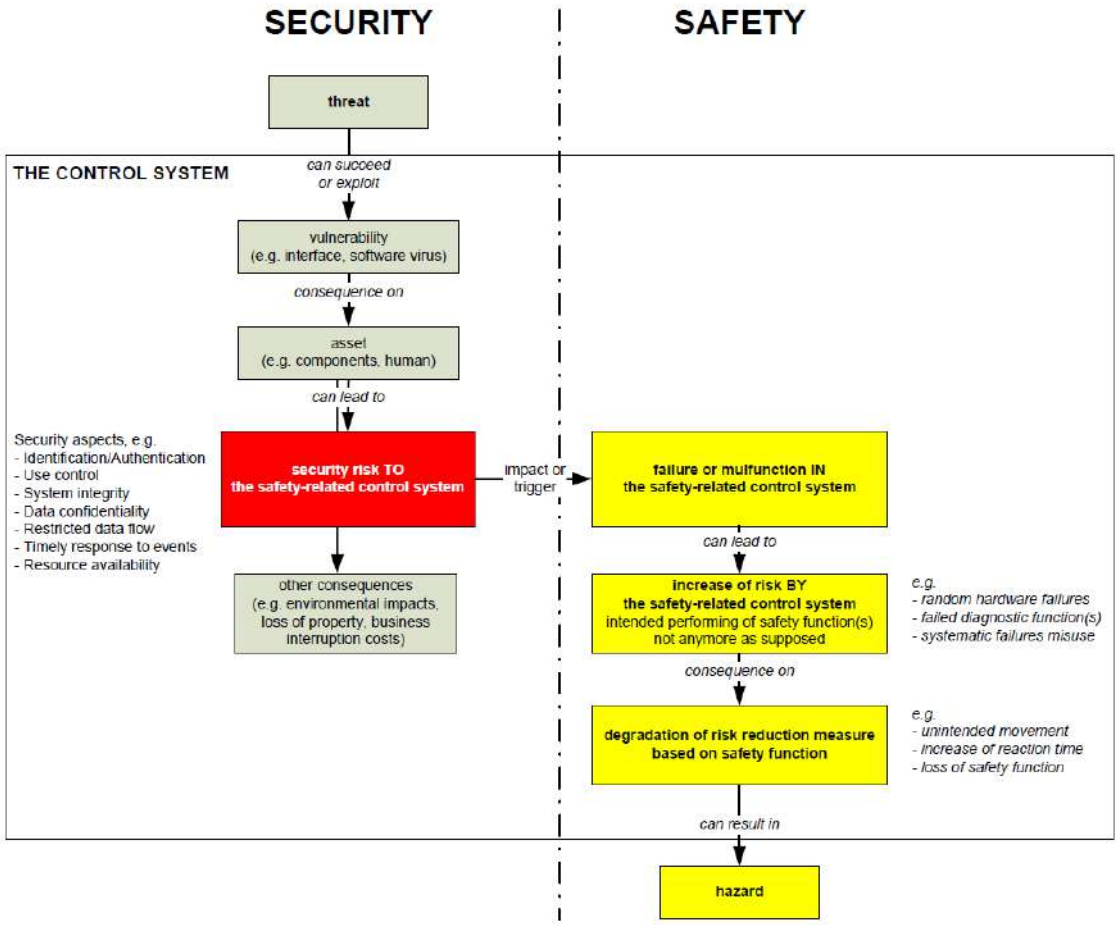
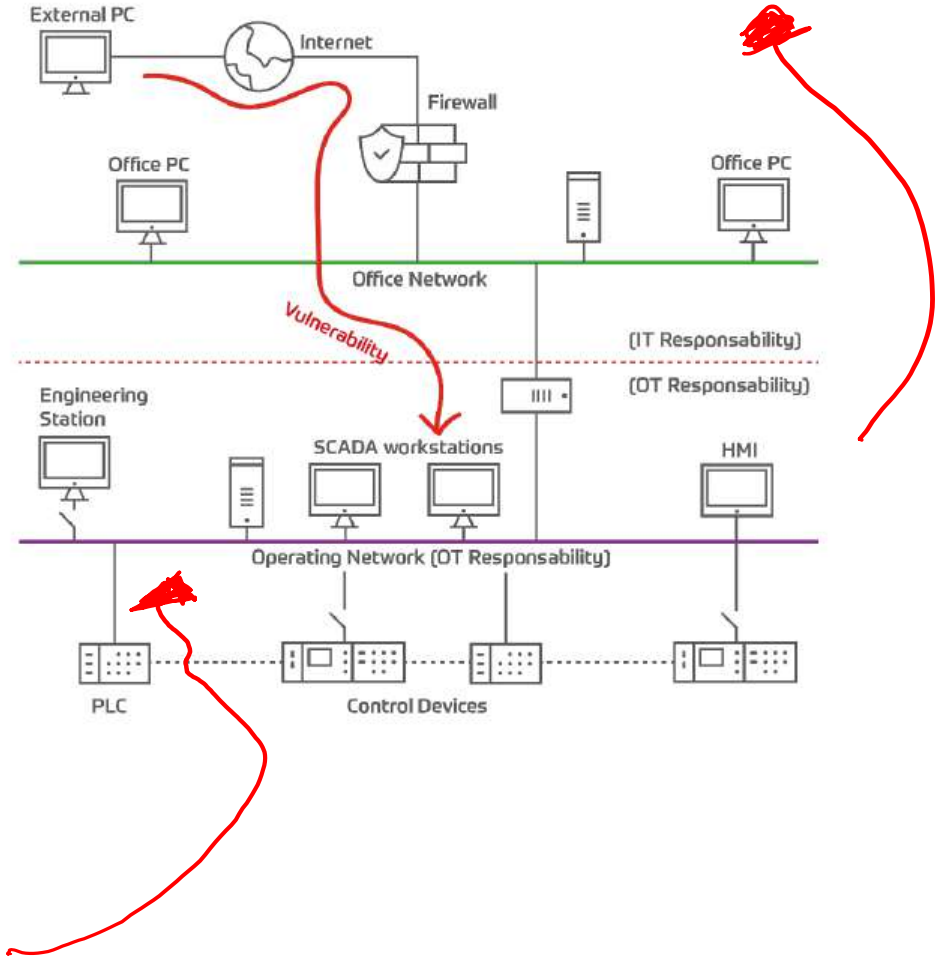


Figure 2 – Possible effects of security risk(s) to a safety-related control system

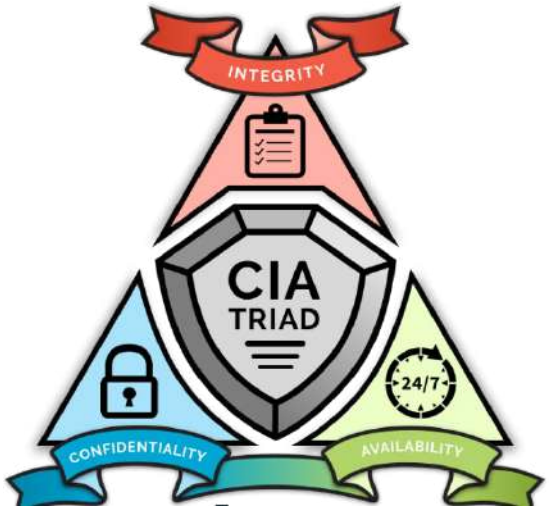


DIFFERENZA TRA IT e OT

IT

L'IT (**Information Technology**) si occupa dei sistemi principalmente computer e telecomunicazioni per eseguire varie operazioni come fornire input, archiviare, recuperare, trasmettere, manipolare e proteggere dati o informazioni.

La rete IT comprende, software e apparecchiature periferiche. Invece di eseguire un insieme statico di funzioni, l'IT può essere regolato e riprogrammato in tanti modi diversi per soddisfare le applicazioni in continua evoluzione, i requisiti aziendali e le esigenze degli utenti. La rete IT in qualsiasi settore viene utilizzata per gestire i sistemi informatici ei dati delle aziende in modo più sicuro.



OT

L'OT (**Operational Technology**) è una categoria di un sistema informatico e viene utilizzata per monitorare i industriali e apportare modifiche se necessario in un settore o in un'impresa.

L'OT utilizza la combinazione di software e hardware per eseguire operazioni in tempo reale e per rilevare se si sono verificati cambiamenti durante l'intero processo.

I sistemi OT garantiscono la sicurezza delle operazioni industriali monitorandole continuamente e supportando la produzione.

La rete OT opera a livello industriale per elaborare i dati operativi di qualsiasi organizzazione

OT Security Scenario Italia

Coinvolte 698 imprese italiane, tra le quali 180 Grandi Organizzazione con oltre 249 addetti

- Fermo della Produzione 54%
- Safety 20%
- Alterazione/modifica della produzione 16%
- Furto o perdita di dati confidenziali 10%

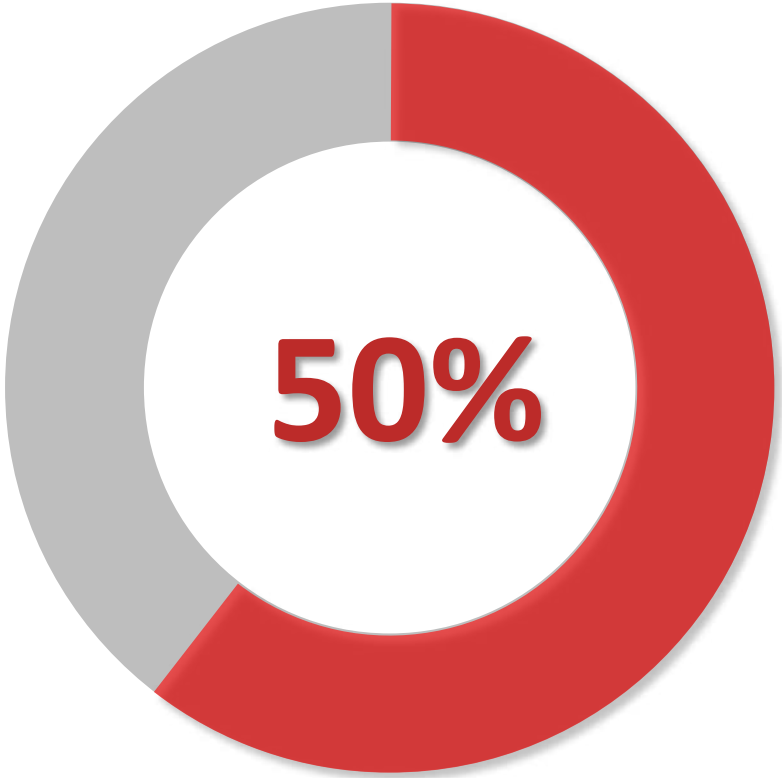
Negli ambienti industriali vengono sempre più interconnessi e integrati sistemi che non sono stati originariamente progettati con lo scopo di essere connessi in rete o, per lo meno, non in reti che non fossero segregate

Ricerca dell'Osservatorio di Information Security & Privacy della School of Management del Politecnico di Milano Giugno 2020

OT/ICS 2022 Threat Landscape

Insufficient ICS endpoint security installations

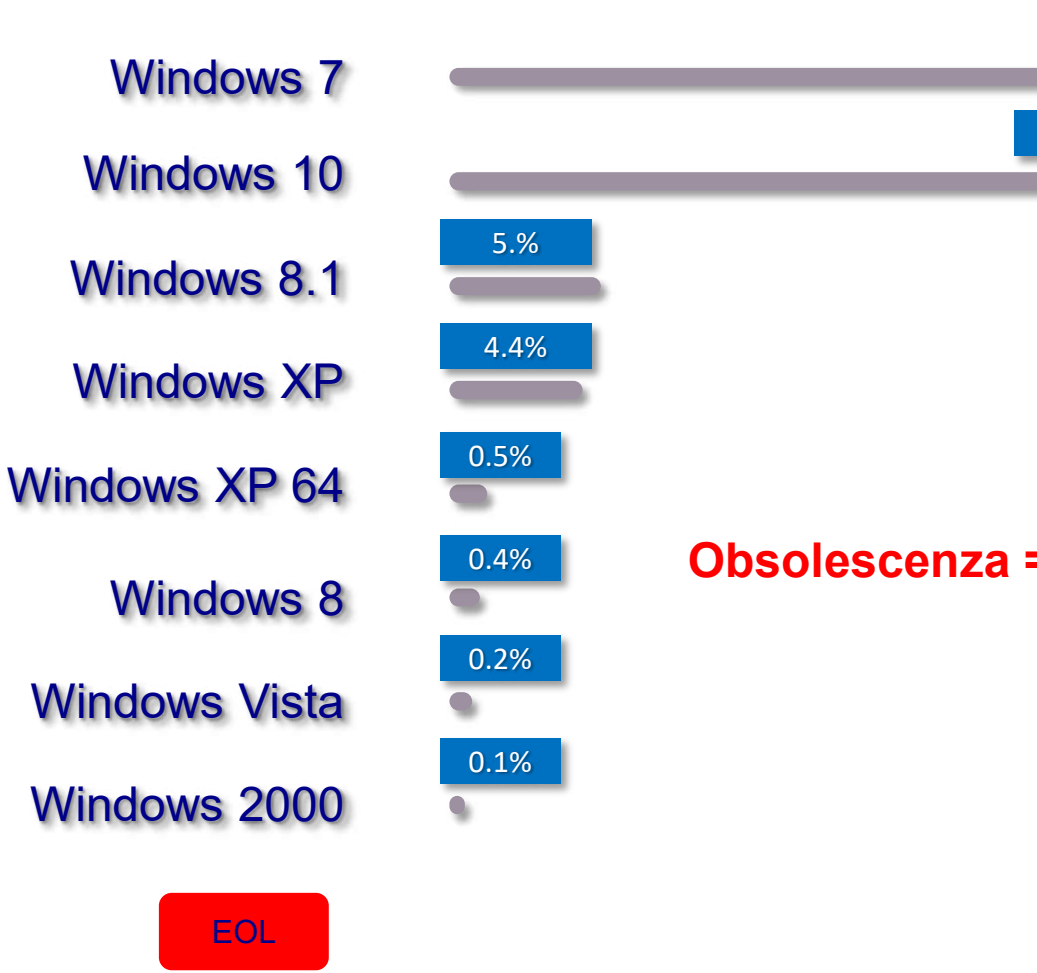
Trend Micro 2021 OT Security survey, 500 respondents in US (200), Germany (150), and Japan (150)



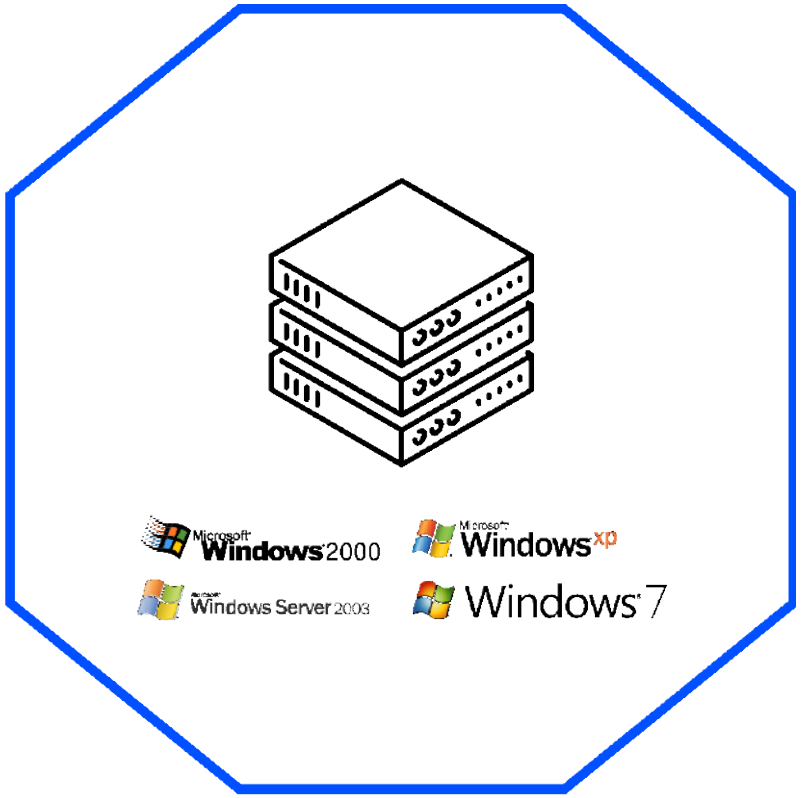
Less than 50% of plant managers install antivirus for ICS endpoints

Source: https://resources.trendmicro.com/Industrial-Cybersecurity-WP.html

Most frequently used Operating Systems in Manufacturing



Obsolescenza = Vulnerabilità

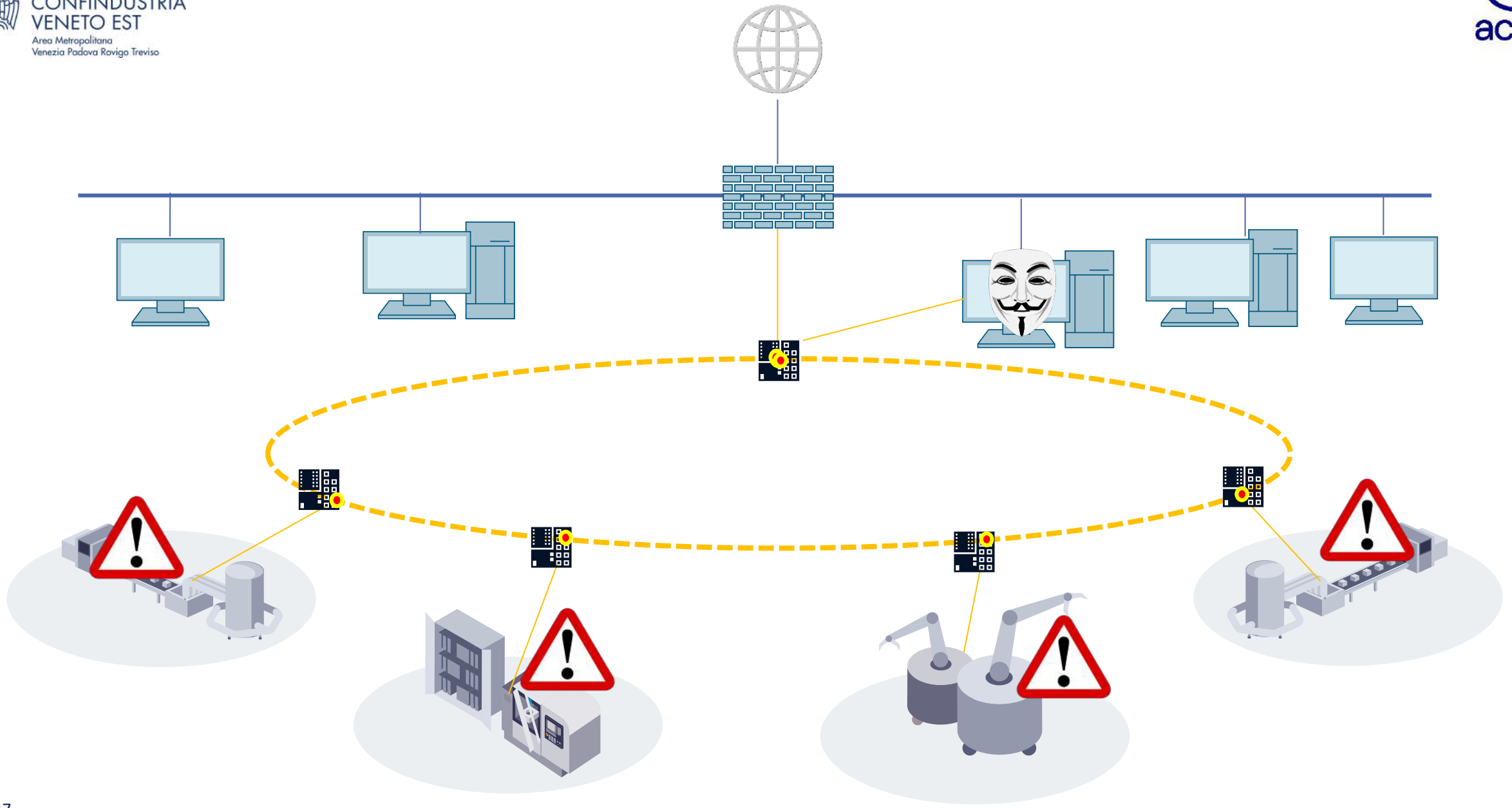


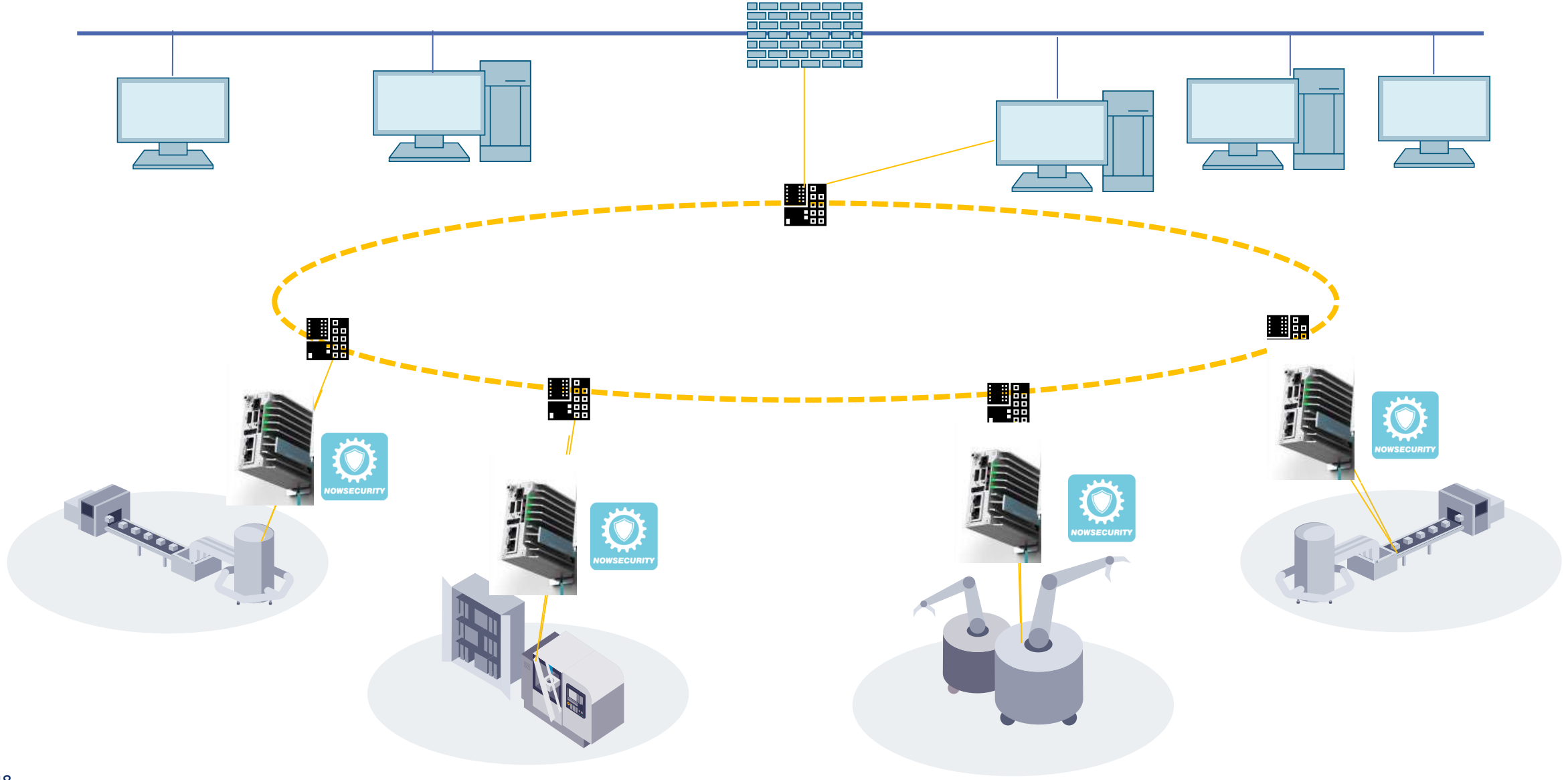
Source: Trend Micro Securing Smart Factories Threats to Manufacturing Environments in the Era of Industry 4.0

I sistemi **ICS** (Industrial Control System)

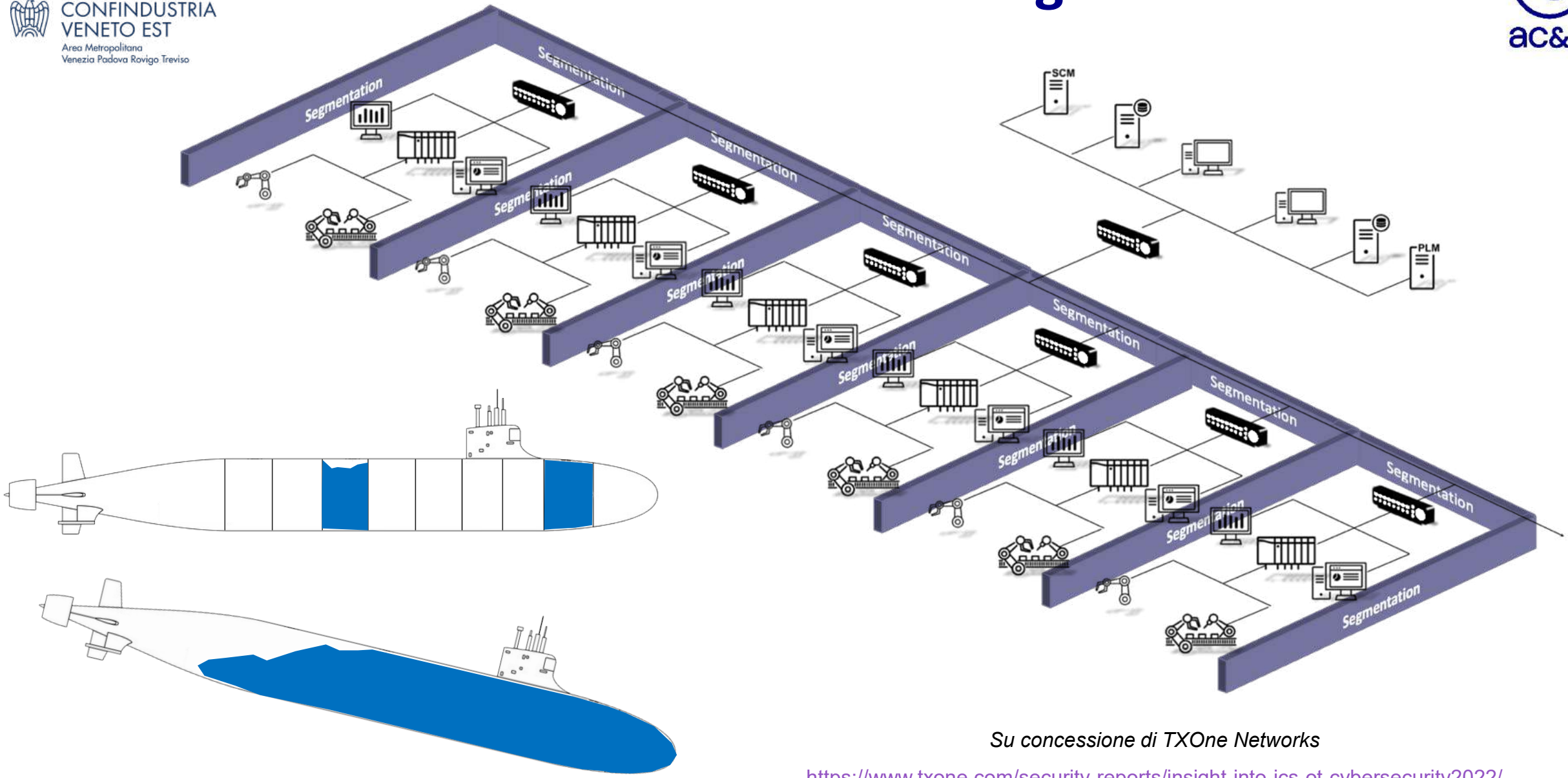
I protagonisti delle cyber-minacce	Molti ambienti ICS usano credenziali condivise e hanno una debole separazione delle funzioni.
Fuga di informazioni	I sistemi possono essere esposti a Internet senza controlli adeguati, per errore o per ignoranza.
Accesso Remoto	Le VPN possono permettere l'uso di applicazioni e dati presenti su macchine esterne all'interno di reti ICS.
Connettività business-to-ICS	Gli attacchi possono migrare da Internet attraverso la rete ICS.
Reti ICS	La maggior parte dei protocolli ICS è suscettibile di attacchi "man-in-the-middle" e di spoofing basati sulla rete.
Social engineering	Gli autori degli attacchi possono utilizzare nomi utenti di default, password deboli o meccanismi di autenticazione obsoleti.
Supply chain	Le infrastrutture ICS possono essere attaccate attraverso fornitori, appaltatori o integratori compromessi.
Governance	I cyber-attacchi spesso non sono considerati nelle procedure di risposta agli incidenti ICS.
Sicurezza fisica	Gli autori degli attacchi che riescono ad accedere al sito possono rubare o alterare facilmente i dispositivi ICS.

Generic OT network – simple but…




NOWSECURITY
NOWSECURITY
NOWSECURITY
NOWSECURITY

Network Segmentation

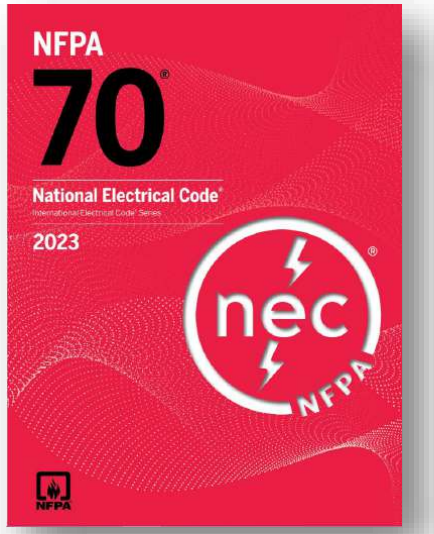


No Network Segmentation

Su concessione di TXOne Networks

https://www.txone.com/security-reports/insight-into-ics-ot-cybersecurity2022/

NEC 2023 Cyber Security



(8) Cybersecurity for network-connected life safety equipment to address its ability to withstand unauthorized updates and malicious attacks while continuing to perform its intended safety functionality

Informational Note No. 3: See the ANSI/ISA 62443 series of standards for industrial automation and control systems, the UL 2900 series of standards for software cybersecurity for network-connectable products, and UL 5500, *Standard for Remote Software Updates*, which are standards that provide frameworks to mitigate current and future security cybersecurity vulnerabilities and address software integrity in systems of electrical equipment.

La norma nasce quasi venti anni fa ad opera di un gruppo di volontari dell'industria facenti parte del comitato SP99, istituito da ISA, *International Society Automation & Control*. È stata in seguito revisionata e adottata da IEC, la *Commissione Elettrotecnica Internazionale*; da qui la **denominazione originale ISA 99/IEC 62443**.

- **ISA**

- Int. Society of Automation
- Organo riconosciuto a livello internazionale
- All'interno di ISA il commitee ISA99 è formato da più di 500 volontari di tutto il mondo. ISA99 ha creato e mantiene lo standard 62443.
- Collabora continuamente con altri organi quali IEC ed ISO

- **ISA/IEC 62443**

- «Standards to secure your Control Systems»
- E' uno standard riconosciuto a livello internazionale, adottato da diversi paesi, e da diversi produttori di automazione.
- Descrive tutto il processo di gestione della cybersecurity degli impianti industriali; dal prodotto all'impianto completo.

ISA 99 e la famiglia delle norme IEC 62443

La Commissione Economica delle Nazioni Unite per l'Europa, Nord America e Asia centrale (UNECE, con sede a Ginevra), ha reso noto che utilizzerà lo standard ISA 99 / IEC 62443 all'interno del Common Regulatory Framework on Cybersecurity (CRF) che rappresenterà la sua "posizione ufficiale" in tema di sicurezza informatica.

L'IEC62443 è senza dubbio lo standard più diffuso a livello internazionale per la protezione da rischi informatici di reti e sistemi di controllo e telecontrollo nell'industria come nelle utility: l'adozione di questo standard da parte dell'UNECE contribuirà ulteriormente alla sua diffusione ed adozione ove ci siano sistemi industriali critici.

Il suo sviluppo è iniziato una ventina di anni fa grazie al lavoro svolto da volontari dell'industria all'interno del comitato SP99 promosso da ISA, International Society Automation & Control, e ha poi visto la revisione e adozione da parte della IEC, la Commissione Elettrotecnica Internazionale con sede a Ginevra.

ISA99 si basa infatti sul contributo di esperti internazionali di cybersecurity che hanno deciso di sviluppare standard applicabili in tutti i settori industriali e infrastrutture critiche, fornendo un quadro flessibile e completo per affrontare e mitigare le vulnerabilità di sicurezza attuali e future nei sistemi di automazione e controllo industriale.

Cybersecurity Risk Assessment According to ISA/IEC 62443-3-2

- PHA Hazards
- Device Inventory
- Risk Criteria

Document the Worst-case Scenario for each Device

Determine SL Target for each Device assuming a Likelihood of 1

Group Devices with similar SL Targets into segmented *Zones*

Document Initial Response to Cybersecurity Incidents

Scope/ Input for:
- Detailed Risk Assessment
- SL verification

Initial Risk Assessment

IL RISCHIO SECONDO LA ISA IEC 62443

La valutazione del rischio cyber in ambito OT deve tenere conto di più aspetti rispetto all'ambiente IT.

- Danni fisici alle persone.
- Danni all'ambiente.
- Danni economici.
- Danni all'immagine.
- Interruzione del business.
- Perdita di dati confidenziali e proprietà intellettuale.
- Violazioni dei regolamenti pubblici.
- Impatto sulla sicurezza nazionale.

General	**IEC 62443-1-1** Terminology, Concepts and Models	**IEC TR-62443-1-2** Master Glossary of Teams and Abbreviations	**IEC TR-62443-1-3** System Security Conformance Metrics	**IEC TR-62443-1-3** IACS Security Lifecycle and Use-Cases	
Policies & Procedures	**IEC 62443-2-1** Establishing an Industrial Automation and Control System Security Program	**IEC TR-62443-2-2** IACS Protection Levels	**IEC TR-62443-2-3** Patch Management in the IACS Environment	**IEC TR-62443-2-4** Requirement for IACS Service Providers	**IEC TR-62443-2-5** Implementation Guidance for IACS Asset Owners
System	**IEC TR 62443-3-1** Security Technologies for IACS	**IEC TR-62443-3-2** Security Risk Assessment and System Design	**IEC TR-62443-3-3** System Security Requirments and Security Levels		
Component	**IEC 62443-4-1** Product Development Requirements	**IEC 62443-4-2** Technical Security Requirments for IACS Components			

SYSTEM INTEGRATOR SERVICE PROVIDER	Chi si occupa della realizzazione della rete o di una sua parte. Nel mondo industriale sono: - il softwarista di una macchina - Chi si occupa dell'immissione in rete della macchina	**IEC 62443-2-4** **IEC 62443-3-3**
DEVICE MANUFACTURER PRODUCT SUPPLIER	Costruttore del dispositivo. Nel mondo industriale: - Costruttore di dispositivi (firewall, PLC, SCADA…) - Costruttore di macchinari	**IEC 62443-4-1** **IEC 62443-4-2**
ASSET OWNER	Colui che è proprietario della rete. Nel mondo industriale: - l'utilizzatore finale della macchina	**IEC 62443-2-1** **IEC 62443-3-2** **IEC 62443-3-3**

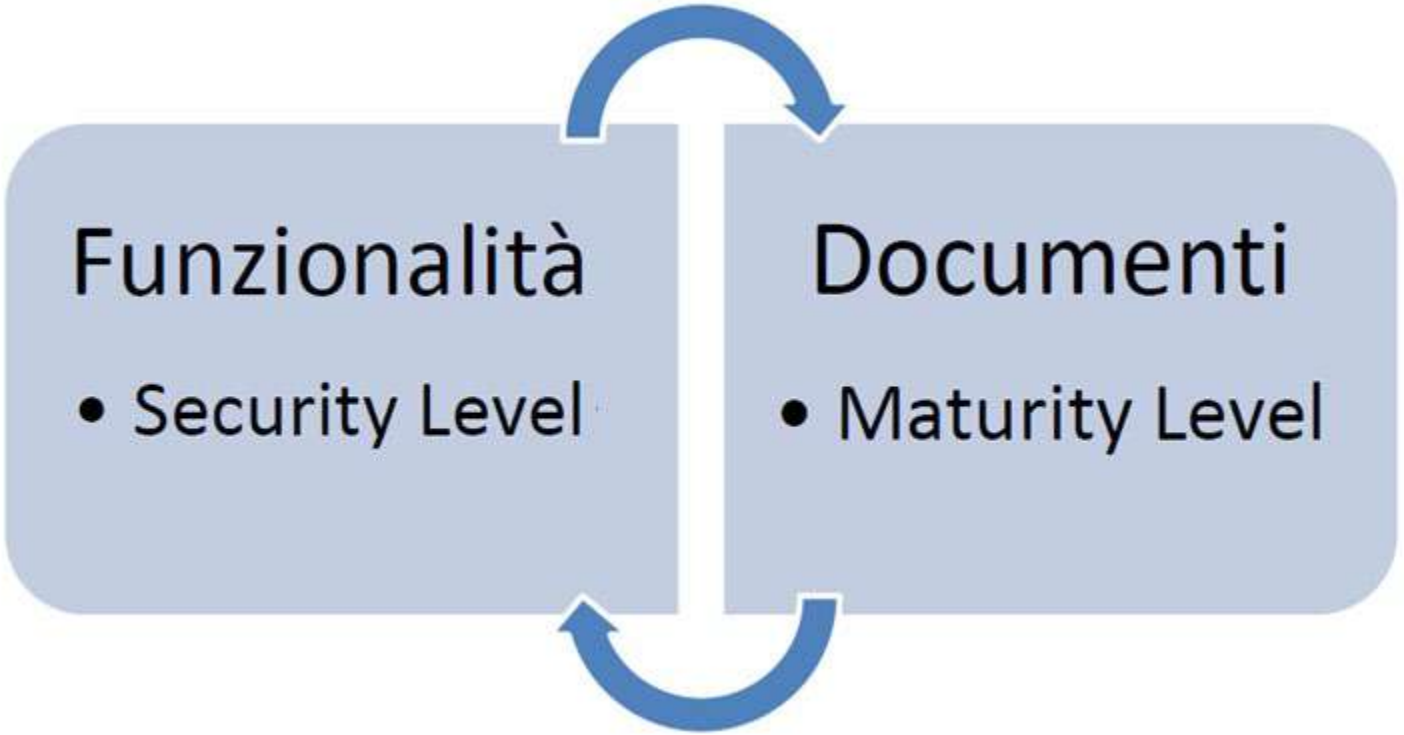
Il processo della security

I termini classici e nuovi:

PL = Protection Level

SL = Security level

MT = Maturity Level



SECURITY LEVEL

3 tipi di Security Level SL:

Target SL (SL-T): SL di riferimento che l'ambiente di destinazione prevede (Risk assessment)

Achieved SL (SL-A): SL raggiunto con la soluzione implementata compresi metodi di compensazione

Capability SL (SL-C): effettivo livello di sicurezza che il dispositivo è capace di fornire grazie alle funzionalità di sicurezza di cui dispone

MINACCE e SECURITY LEVEL

Vengono definiti 5 livelli di sicurezza (**Security Level**) equivalenti a 5 livelli di **Minaccia:**

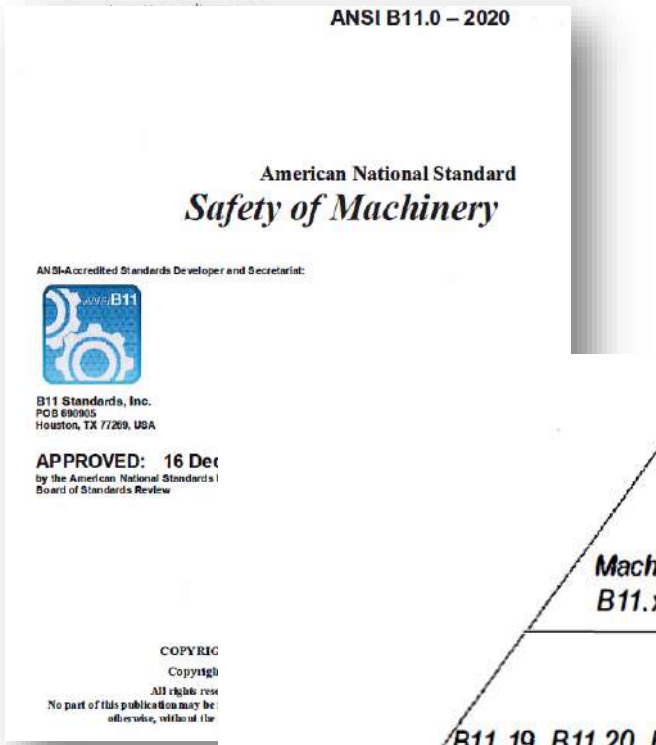
- **Livello 0** non sono necessari né specifici requisiti né protezioni di sicurezza
- **Livello 1** necessaria protezione contro errori accidentali (componente umana)
- **Livello 2** necessaria protezione contro azioni volontarie compiute da soggetti con mezzi comuni, poche risorse, skills generiche riguardo I sistemi di controllo e bassa motivazione (Hacker amatoriali)
- **Livello 3** necessaria protezione contro azioni volontarie compiute da soggetti con mezzi sofisticati, risorse moderate , skill specifiche riguardo I sistemi di controllo e moderata motivazione (Hacker professionisti, hacktivisti)
- **Livello 4** necessaria protezione contro azioni volontarie compiute da soggetti con mezzi sofisticati, risorse estese , skill specifiche riguardo I sistemi di controllo e alta motivazione (nazioni e terroristi)

MATURITY LEVEL

I livelli di Maturità si riferiscono alla parte documentale, che le tre figure dovranno integrare nei loro processi produttivi come processi di security Sono definiti 4 livelli:

- **Livello Iniziale**: il sistema è definito ma in modo non documentato
- **Livello definito**: il sistema è definito, sono state scritte procedure e policies e vi è evidenza scritta del sistema
- **Livello gestito**: oltre a quanto si ha nel livello definito, il sistema è anche messo in pratica e si hanno evidenze
- **Livello misurabile**: come il livello precedente ed in più è in atto un sistema di misura delle performance ed è possibile attuare il miglioramento continuo

ANSI B11.0-2020, Safety of Machinery


ANSI B11.0 – 2020

American National Standard

Safety of Machinery

ANSI-Accredited Standards Developer and Secretariat:

B11 Standards, Inc.
POB 690905
Houston, TX 77269, USA

APPROVED: 16 Dec
by the American National Standards
Board of Standards Review

COPYRIG
Copyrigh
All rights res
No part of this publication may be
otherwise, without the

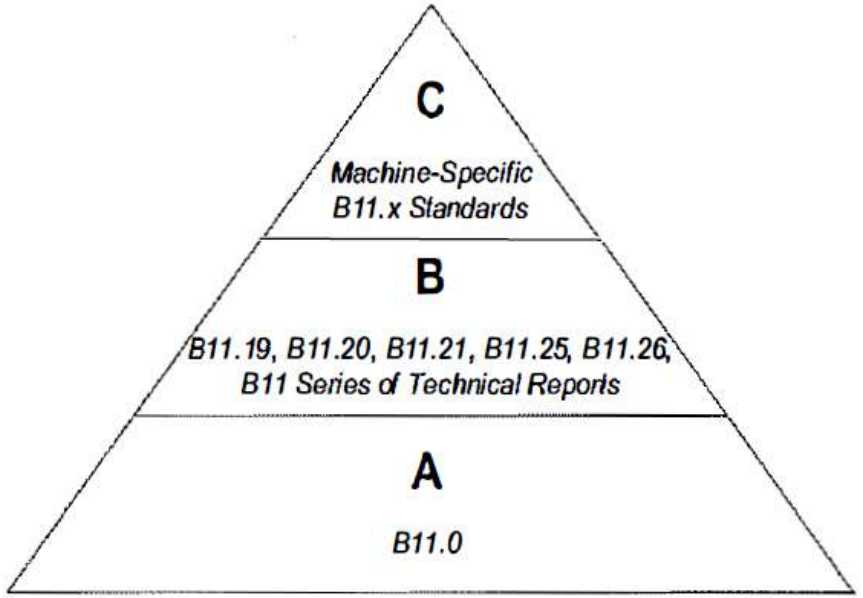
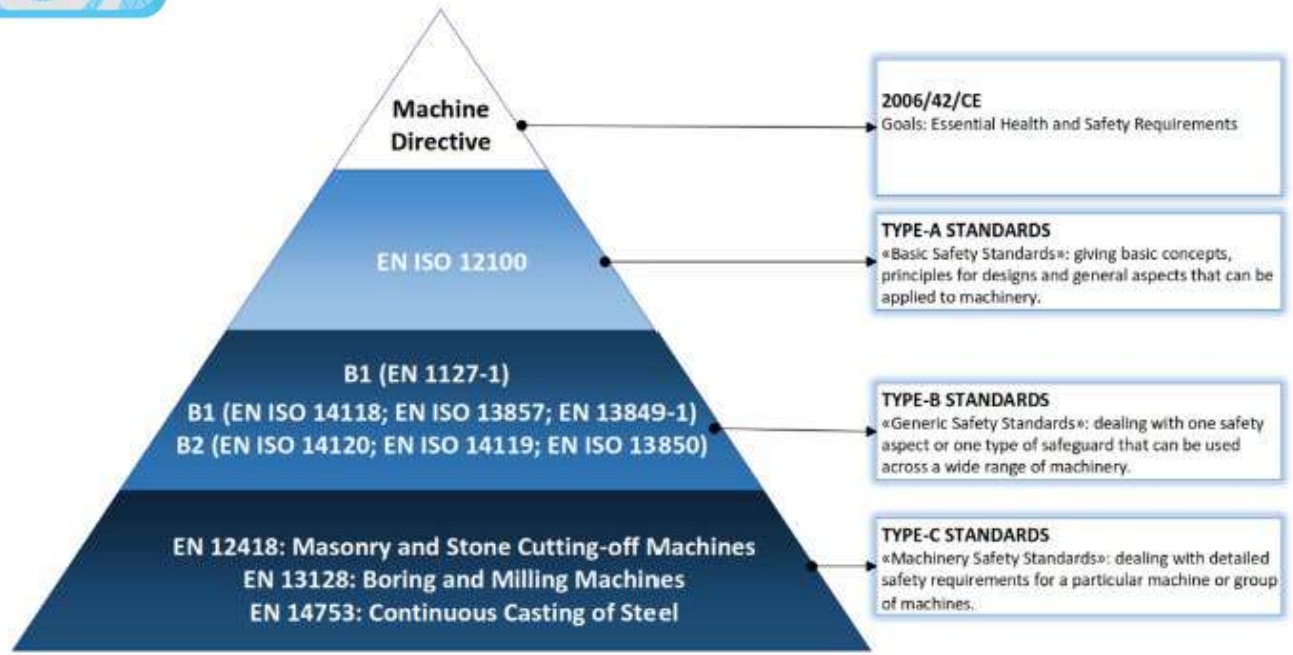


Figure 2 — Organization of the B11 Series of Documents



B11.TR9–2019

Guidance to Machinery Manufacturers for Consideration of Related IT-Security (Cyber Security) Aspects

This document gives machine manufacturers guidance on potential security aspects in relation to safety of machinery when putting a machine into service or placing it on the market for the first time. It provides essential information to identify and address IT-security threats which can influence the safety of machinery.

This document gives guidance but does not provide detailed specifications on how to address IT-security aspects which can influence the safety of machinery. This document does not address the bypass or defeat of risk reduction measures through physical manipulation.

B11.TR10–2020

Functional Safety of Artificial Intelligence for Machinery Applications

This technical report provides guidance for the implementation of functional safety principles in artificial intelligence (AI) programming when used as a means for machinery safety applications. These principles may include internal diagnostics such as component/system integrity during operation and external diagnostics such as environmental effects and communication networks.

This technical report is not a replacement for embedded and application functional safety software requirements.

B11.TR9-2019 (ISO/TR 22100-4:2018 *IDT*)

Guidance to Machinery Manufacturers for Consideration of Related IT-Security (Cyber Security) Aspects

ANSI-Accredited Standards Developer and Secretariat:

A Technical Report prepared by
B11 Standards, Inc.
POB 890905
Houston, TX 77269
www.b11standards.org
and

Registered with ANSI: 07 APRIL 2019

Bibliography

[1] ISO/IEC Guide 51:2014, *Safety aspects — Guidelines for their inclusion in standards*

[2] ISO 11161:2007, *Safety of machinery — Integrated manufacturing systems — Basic requirements*

[3] ISO 13849-1:2015, *Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design*

[4] ISO/IEC 20924[2], *Information technology — Internet of Things (IoT) — Definition and vocabulary*

[5] IEC/TS 62443-1-1, *Industrial communication networks – Network and system security — Part 1: Terminology, concepts and models*

[6] IEC 62443-3-2:—[3], *Security for industrial automation and control systems — Part 3-2: Security risk assessment and system design*

[7] IEC 62443-3-3, *Industrial communication networks — Network and system security — Part 3-3: System security requirements and security levels*

[8] IEC 62443-4-2, *Industrial communication networks — Security for industrial automation and control systems — Part 4-2: Technical security requirements for IACS components*

[9] CENELEC Guide 32: *Guidelines for Safety Related Risk Assessment and Risk Reduction for Low Voltage Equipment*

[10] *Capabilities Assessment for Securing Manufacturing Industrial Control Systems,* Draft Nov 2016, https://nccoe.nist.gov/sites/default/files/library/project-descriptions/mf-ics-1-project-description-draft.pdf

[11] CNSSI-4009, Committee on National Security Systems (CNSS) Glossary, April 2015, USA https://cryptosmith.files.wordpress.com/2015/08/glossary-2015-cnss.pdf

[12] FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems,* Federal Information Processing Standards Publication, March 2006, USA http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf

[13] NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations,* Revision 4, April 2013 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

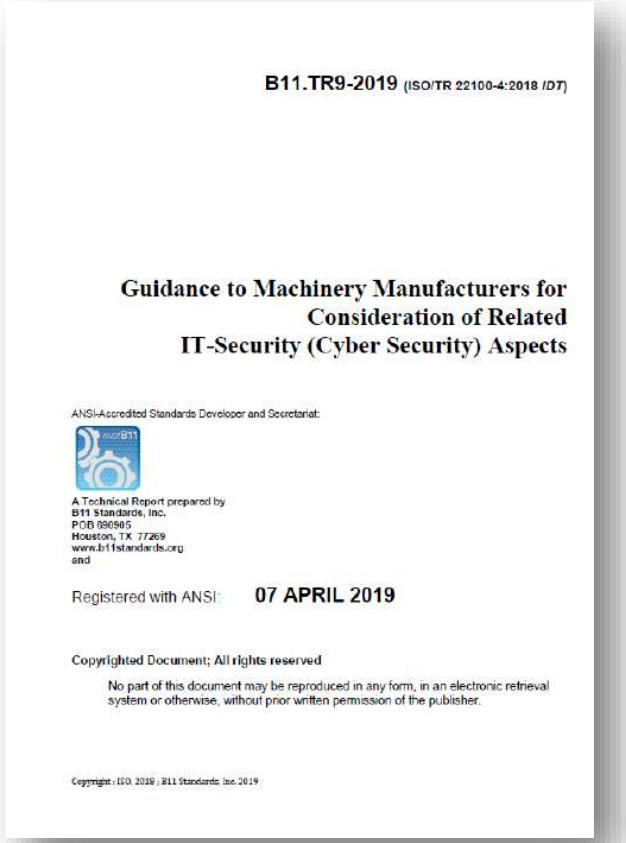
[14] NIST SP 800-61, *Computer Security Incident Handling Guide,* Revision 2, August 2012 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

[15] NIST SP 800-82, *Guide to Industrial Control Systems (ICS) Security,* Revision 2, May 2015. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-109 82r2.pdf

[16] RFC 4949, *Internet Security Glossary*, Version 2, August 2007

B11.TR9-2019

Guidance To Machinery Manufacturers For Consideration Of Related IT-Security (Cyber Security) Aspects



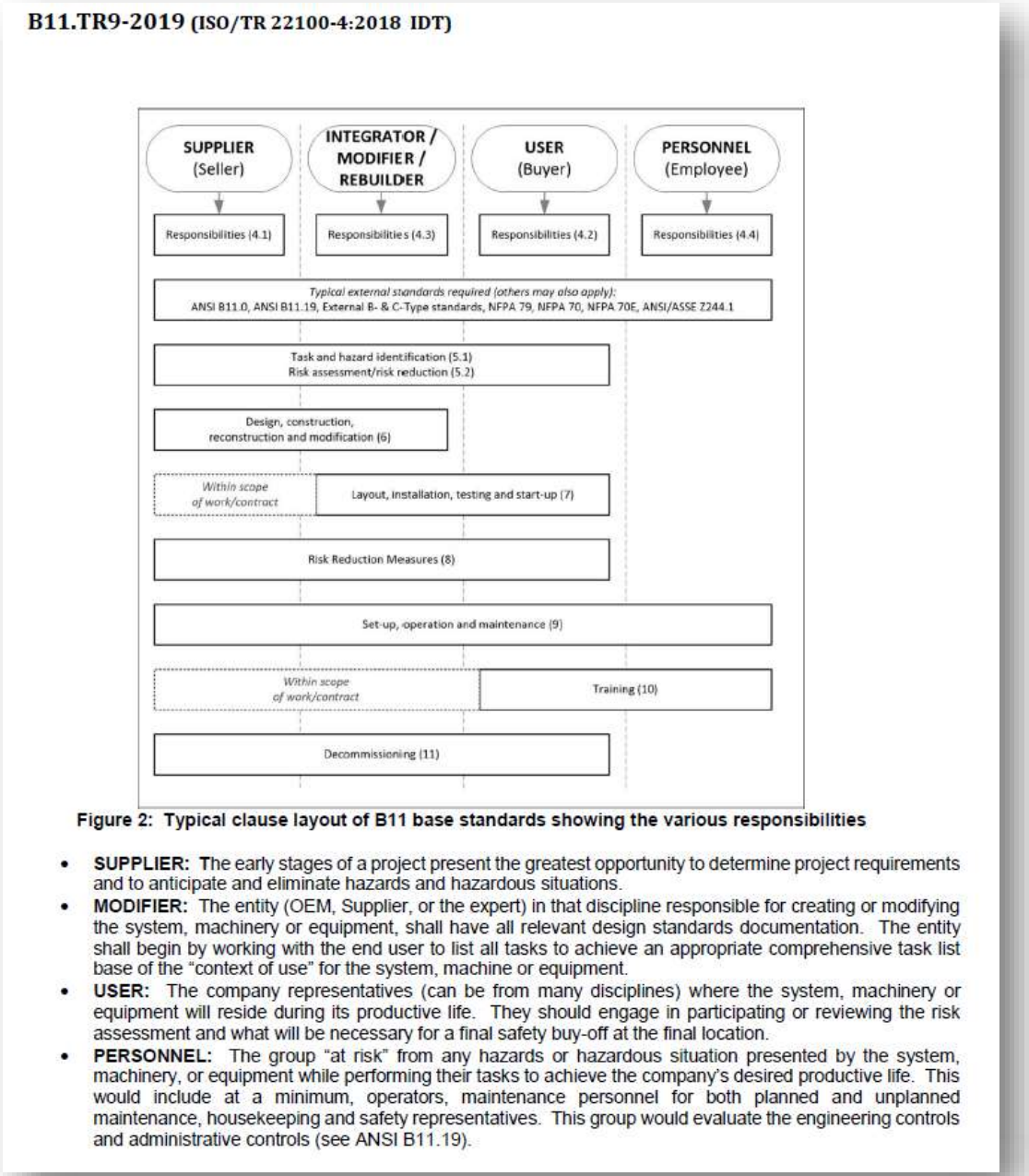
B11.TR9-2019 (ISO/TR 22100-4:2018 IDT)

Guidance to Machinery Manufacturers for Consideration of Related IT-Security (Cyber Security) Aspects

ANSI-Accredited Standards Developer and Secretariat:

A Technical Report prepared by
B11 standards, Inc.
POB 690965
Houston, TX 77269
www.b11standards.org
and

Registered with ANSI: 07 APRIL 2019



B11.TR9-2019 (ISO/TR 22100-4:2018 IDT)

Figure 2: Typical clause layout of B11 base standards showing the various responsibilities

- **SUPPLIER:** The early stages of a project present the greatest opportunity to determine project requirements and to anticipate and eliminate hazards and hazardous situations.
- **MODIFIER:** The entity (OEM, Supplier, or the expert) in that discipline responsible for creating or modifying the system, machinery or equipment, shall have all relevant design standards documentation. The entity shall begin by working with the end user to list all tasks to achieve an appropriate comprehensive task list base of the "context of use" for the system, machine or equipment.
- **USER:** The company representatives (can be from many disciplines) where the system, machinery or equipment will reside during its productive life. They should engage in participating or reviewing the risk assessment and what will be necessary for a final safety buy-off at the final location.
- **PERSONNEL:** The group "at risk" from any hazards or hazardous situation presented by the system, machinery, or equipment while performing their tasks to achieve the company's desired productive life. This would include at a minimum, operators, maintenance personnel for both planned and unplanned maintenance, housekeeping and safety representatives. This group would evaluate the engineering controls and administrative controls (see ANSI B11.19).

Cybersecurity
Regulatory compliance application

- ✓ ANSI B11.TR9-19

B11.TR9-2019 (ISO/TR 22100-4:2018 *IDT*)

Guidance to Machinery Manufacturers for Consideration of Related IT-Security (Cyber Security) Aspects

ANSI-Accredited Standards Developer and Secretariat:

A Technical Report prepared by
B11 Standards, Inc.
POB 690905
Houston, TX 77269
www.b11standards.org
and

Registered with ANSI: 07 APRIL 2019

TECHNICAL REPORT

ISO/TR 22100-4

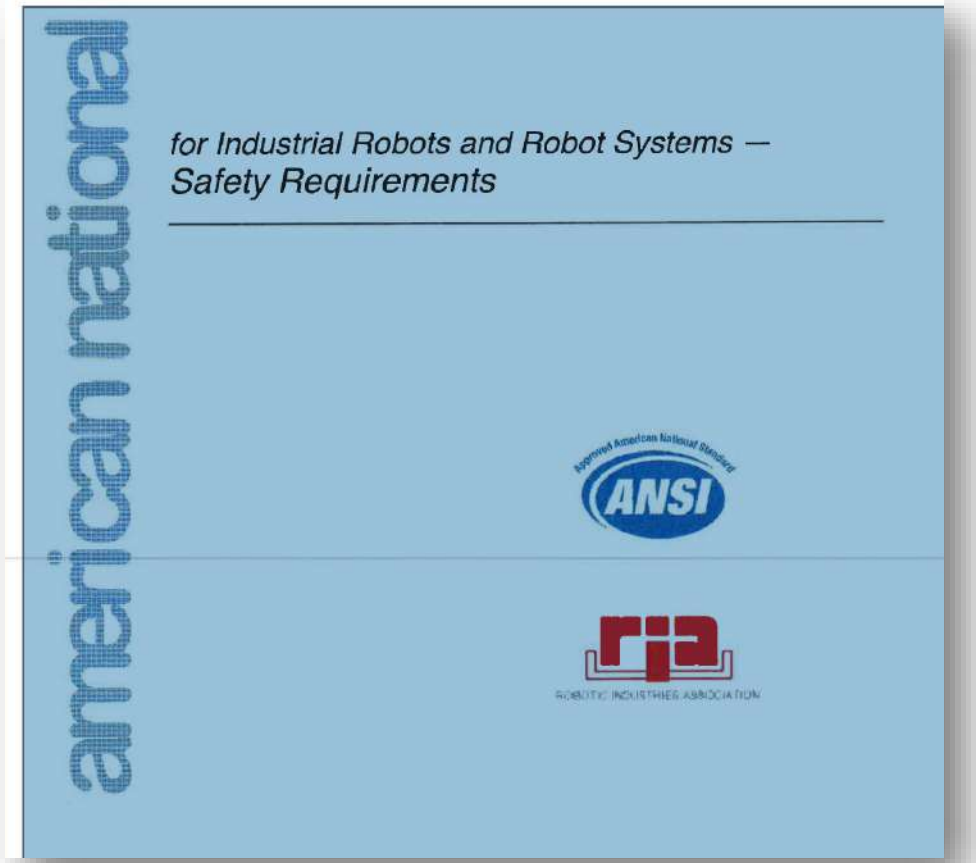
First edition
2018-12

Safety of machinery — Relationship with ISO 12100 —

Part 4:
Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects

ISO

Reference number
ISO/TR 22100-4:2018(E)



5.6.5 Remote access for manual intervention

A robot system may be network enabled (e.g. LAN, modem, and internet) which allows remote access for diagnostics, technical consultation and testing, etc.

If a robot system is to be remotely controlled by an operator who is physically away from the robot (e.g. in a distant office), the following shall be required:

a) manual remote control shall only be possible when the robot system is in manual mode;

b) at one time, only one source of control – local or remote – shall be active (single point of control);

c) the type of control listed in b) shall not override local selection and cause any local hazardous situation;

d) activation of the manual remote control function shall be possible only from the local control;

e) all controller functions that may cause a hazard (e.g. motion of robot, forcing outputs that control hazardous equipment, changing values that influence the robot in a hazardous way, acknowledgement of safety functions, hold to run, etc.) shall be possible only from the single selected source of control;

f) it shall not be possible for remote changes to the parameters, related to limiting robot motion by means of safety-rated soft axis and space limiting as described in 5.4.3, to take effect without local action to confirm the acceptability of the change and that it did not create a hazard;

g) an indication at the local control (control panel, teach pendant, etc.) shall show that the robot system is being remotely controlled;

h) attended manual intervention shall only be possible when the robot system is in manual reduced speed;

i) if no-one is in the safeguarded space and safeguards are active, remote functions may be performed without any local activities;

Dalla safety alla security – L' analisi dei rischi

Come per gli aspetti legati alla safety, per definire le azioni mitigatorie da intraprendere al fine di limitare la possibilità degli accessi agli utenti non autorizzati, si dovrà effettuare un'analisi dei rischi del sistema.

Saranno scopo delle valutazioni ad esempio:

- Le procedure di identificazione accesso ed uso
- La configurazione dei componenti
- L'identificazione sistema
- La segmentazione del sistema

IEC 62443-3-2 and IEC 62443-3-3

Documentazione

Architettura di rete

Componenti di rete utilizzati

Protocolli di comunicazione usati

Procedure/Policies ed aspetti implementativi

IEC 62443-3-2

Risk Assessment

Security Level Target (SL-T)

Security Level Achieved (SL-A)

IEC 62443-3-3

Security Level Capability (SL-C)

IEC 62443-3-3

IEC 62443-3-3: Security Requirements

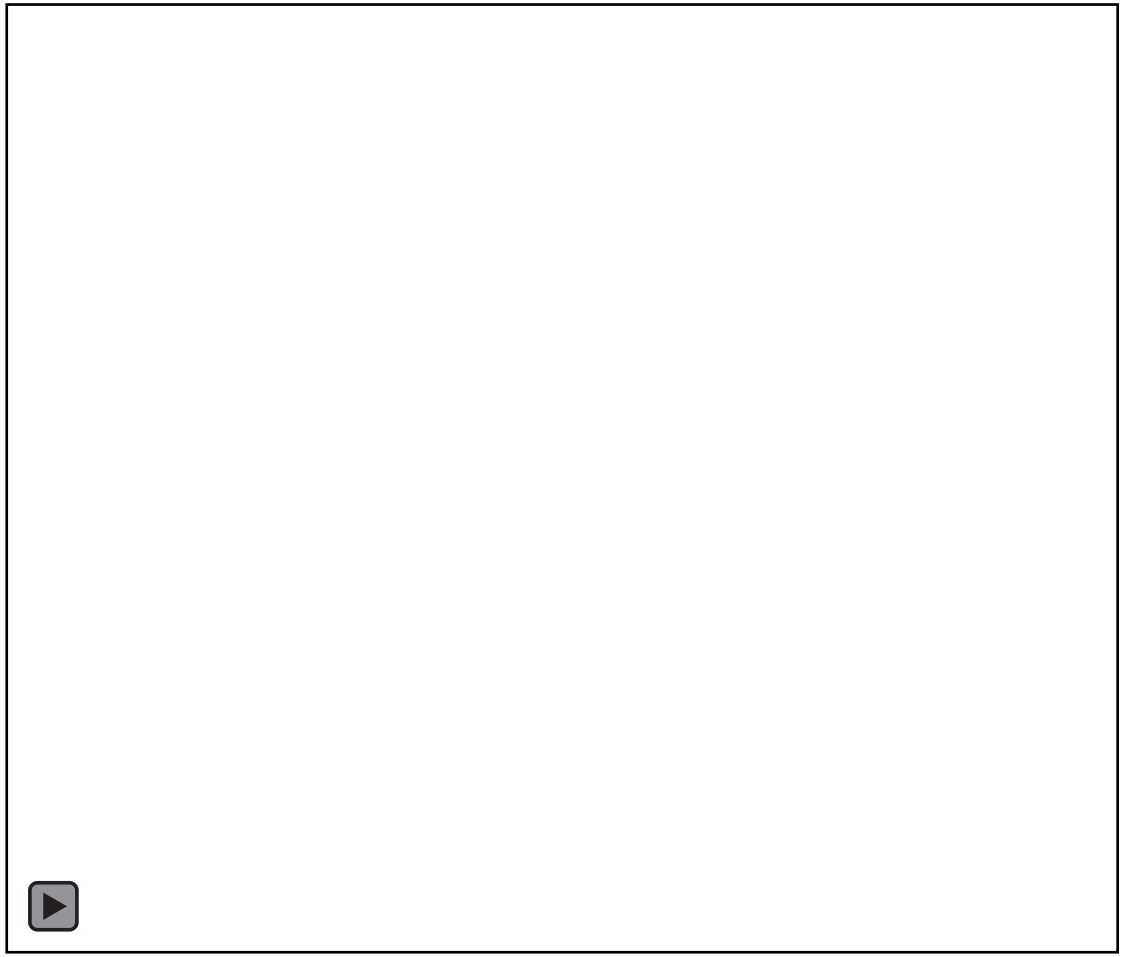
Security Level Targeted	2	Cliente:						
IEC 62443-3-3	SL1	SL2	SL3	SL4	Y/N	Requirement	Rationale	Associated SL
FR 1 – Identification and authentication control								SL 4
SR 1.1 – Human user identification and authentication	x	x	x	x	No	The control system shall provide the capability to identify and authenticate all human users.	passwords, tokens, biometrics, multifactor auth, geographic location may be used. The requirement should be applied to both local and remote access to the control system.	SL 0
RE (1) Unique identification and authentication		x	x	x	No	The control system shall provide the capability to uniquely identify and authenticate all human users		SL 1
RE (2) Multifactor authentication for untrusted networks			x	x	No	The control system shall provide the capability to employ multifactor authentication for human user access to the control system via an untrusted network		SL 2

A..B..C.. per una minima protezione

- Un sistema di VPN Layer 2 per la teleassistenza.
- Segmentazione di rete protetta da firewall per la macchina o linea.
- Log di accesso VPN e log del firewall.
- Possibile configurazione push di notifiche aziendali.
- Tracciamento delle modifiche PLC chiusura software Safety, previa opportuna configurazione
- Acquisizione dati tramite protocolli di automazione industriali (S7, Modbus-TCP, OPC-UA, Ethernet IP, ecc.).

I punti rispettati rispetto alle richieste della IEC 62443 (elenco non esaustivo)

- User Authentication and Identification
- Identification Management
- Authentication Management
- Sending Notifications to Users (via Telegram/e-mail)
- Authentication Feedback (in caso di User o Pwd errati il sistema non dovrà indicare il motivo)
- Unsuccessful Logon Attempts (registro dei tentativi di accesso non autorizzato)
- Implementing Authorizations (possibilità di gestire i privilegi degli accessi)
- Access Session Lock (tempo di inattività e successivo logout impostabile)
- Event Audit (validazione dell'architettura security di macchina e rilascio di report)



I punti rispettati rispetto alle richieste della IEC 62443 (elenco non esaustivo)

- Storage Capacity Control (il sistema controlla e monitora i pacchetti archiviati nel server certificato)
- Communication Integrity (protezione dei pacchetti scambiati)
- Security Function Verification (durante gli audit è possibile monitorare e registrare le anomalie della security)
- Input Validation (il sistema valida e discrimina gli operatori in base alle procedure)
- Information Confidentiality (i dati scambiati con il server sono crittografati)
- Using Cryptography (la crittografia è sempre attiva)
- Historical Data and Audit Accessibility (i dati e le modifiche effettuate sono allocate nel server certificato)
- Emergency Power (obbligo di installazione di UPS per SL 2)

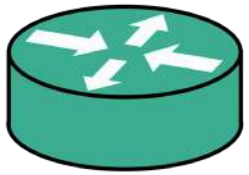
	Security level	IACS component designed to defend against…
	4	intentional cyberthreats posed by motivated, skilled and sophisticated malicious users with access to substantial resources
	3	intentional cyberthreats posed by skilled, sophisticated malicious users with access to moderate resources
	2	intentional cyberthreats posed by malicious users having basic, generic skills with low access to resources
	1	casual or unintentional system violation

Fig. 2: IEC 62443 security levels

L'Hardware e software

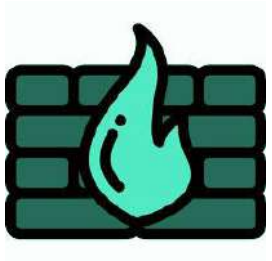
- NEC 2023: si inizia a parlare di cybersecurity
- Da cosa partire? Firewall e Switch Managed

Firewall and Intrusion Prevention System



Router

Reindirizza il traffico tra i client (dalla rete esterna dell'IoT) e i dispositivi (dalla rete interna dell'IoT) come NAT. Può operare su più client interni.



Firewall *

Come la modalità router, con un filtro IPv4 personalizzabile che controlla la connessione a livello di trasporto (Lv4).

Supporta whitelist e blacklist che possono essere definite globalmente o specificatamente per ogni connessione.

IPS *

Come la modalità firewall, con un filtro personalizzabile che controlla la connessione a livello di applicazione (Lv7).

Consente inoltre di controllare i permessi (lettura/scrittura) sulle variabili.
Compatibile con i seguenti protocolli:

S7 COMM, OPC UA, Modbus, HTTP, EtherNet/IP

Firewall and Intrusion Prevention System

	Descrizione	Sintesi	Protocolli esempio
Livello 3	È responsabile del routing: scelta ottimale del percorso di rete da utilizzare per garantire la consegna delle informazioni dal mittente al destinatario.	A questo livello lavorano i router.	IP
Livello 4	Si occupa di: stabilire, mantenere e terminare una connessione, garantendo il corretto e ottimale funzionamento della sottorete di comunicazione. (es. controllo della congestione).	Il livello di trasporto associa a ciascuna porta utilizzata un punto di contatto utilizzato da uno o più processi applicativi per trasmettere e/o ricevere dati.	TCP - UDP
Livello 7	Fornisce un insieme di protocolli che operano a stretto contatto con le applicazioni.	Funziona da interfaccia tra utente e macchina.	S7Comm, OPC-UA


RITTAL

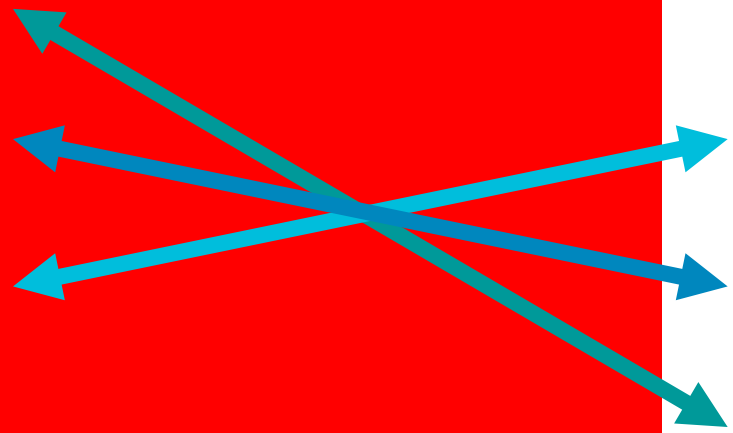

LINDY

L'Hardware e software

- Teleassistenza: regole scritte e registrazione accessi (è un di cui …)
- Versioning del software

Principi fondamentali della protezione dei sistemi IT

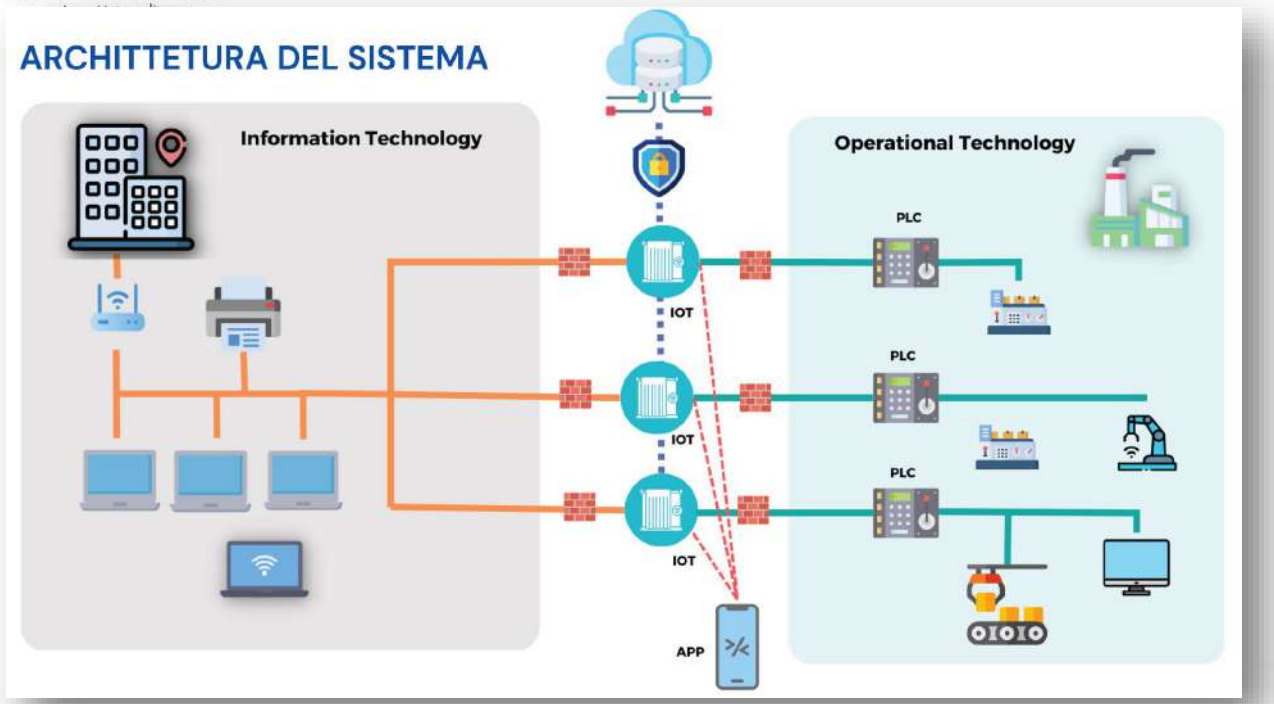
1. Riservatezza
2. Integrità
3. Disponibilità



Principi fondamentali della protezione dei sistemi OT

1. Safety & Controllo
2. Disponibilità
3. Integrità
4. Riservatezza

Cybersecurity Risk Assessment According to ISA/IEC 62443-3-2



A Livello OT

Firewall Lv4 o LV7 IPS

VPN – Switch managed

Policy sulle Password di accesso

A livello PLC

Password, checksum, signature

Autorizzazione locale alla connessione in ingresso

Autorizzazione a muovere la macchina da locale

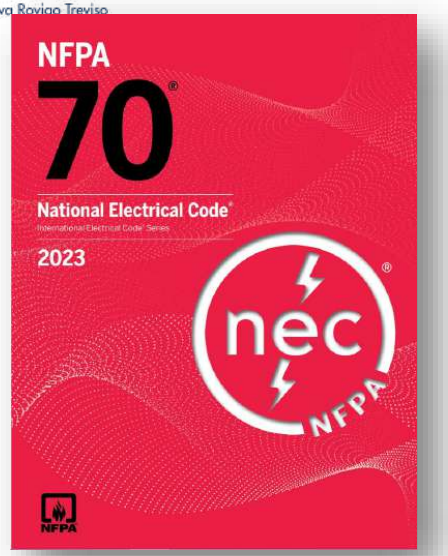
Cybersecurity = Collaborazione

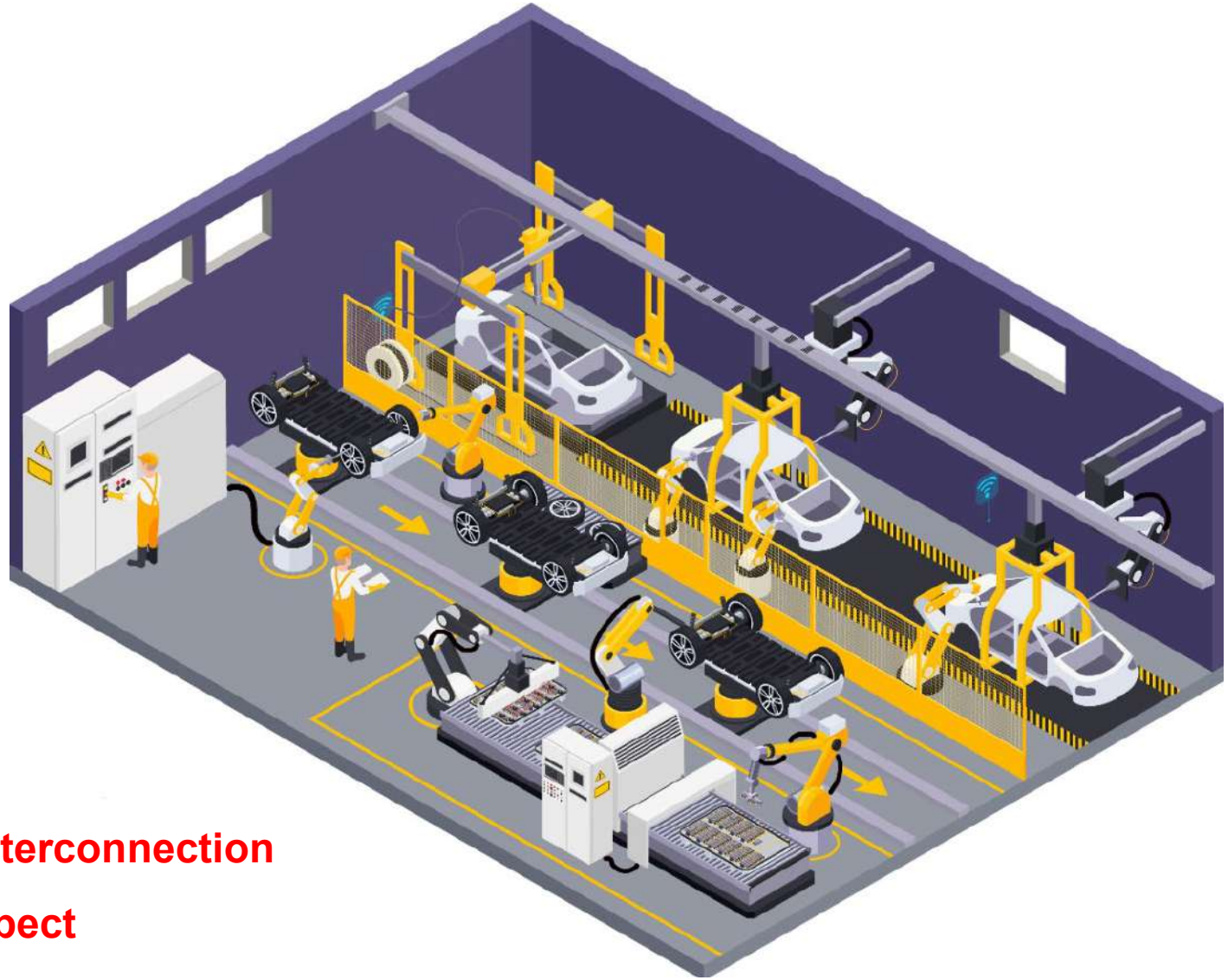
Advanced

CONFINDUSTRIA VENETO EST
Area Metropolitana
Venezia Padova Rovigo Treviso

NEC 2023

ac&e





UL 508A Industrial Control Panel

NFPA 79 Industrial Machinery

NEC 2023 for Installation and Interconnection

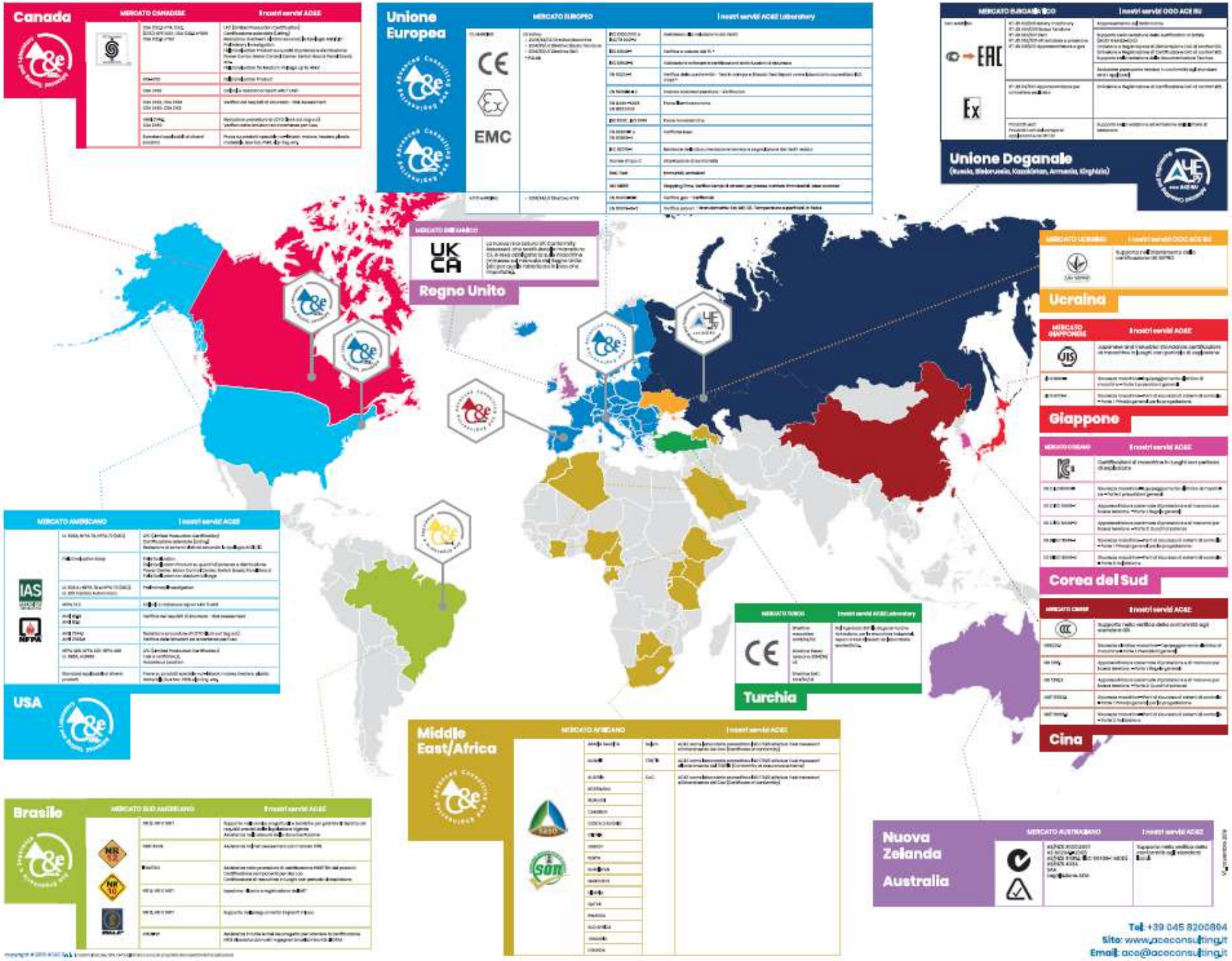
ISA 99 /IEC 62443 For Cyber Aspect


O
S
H
A
OCCUPATIONAL
SAFETY
HEALTH
ADMINISTRATION

Advanced

CONFINDUSTRIA VENETO EST
Area Metropolitana
Venezia Padova Rovigo Treviso

ac&e



Tel: +39 045 8200894
Sito: www.aceconsulting.it
Email: ace@aceconsulting.it

ac&e

Thank you!