Gestione della cybersecurity nella Operational Technology e impatto sulla safety

Bologna, 10/04/2026

ing. Andrea Ognibene - Business Development Manager AEP
cell. +39 340 3345349 | email: aognibene@phoenixcontact.com

PHOENIX CONTACT
INSPIRING INNOVATIONS

Andrea Ognibene – percorso professionale

- Mi occupo di salute e sicurezza nei luoghi di lavoro dal 2006.
- Nasco come figura tecnica (focus specifico sicurezza del macchinario ed ergonomia) per poi spostarmi verso l'area commerciale (focus specifico sicurezza del macchinario, direttive di prodotto quali ATEx, PED, ..., risk management).
- Da ottobre del 2019 sono in Phoenix Contact con l'obiettivo di sviluppare servizi in ambito «safety machinery».
- Da marzo 2025, sempre in Phoenix Contact, mi occupo anche di OT cybersecurity.

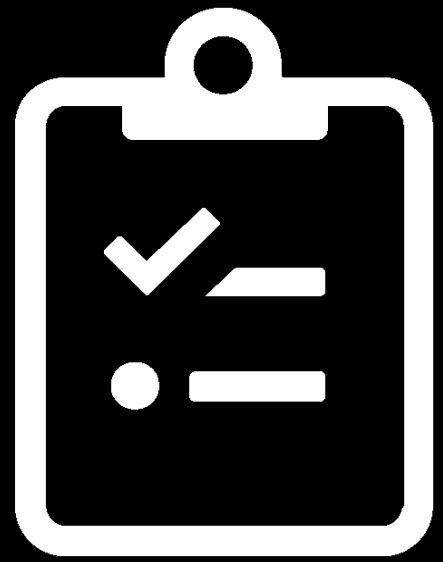
Dal 2014 al 2022 ho fatto parte della Commissione Sicurezza sul Lavoro dell'Ordine degli Ingegneri di Bologna e per qualche anno ho avuto il piacere di coordinarne un'area tematica.

PHOENIX CONTACT
INSPIRING INNOVATIONS

Gestione della cybersecurity nella Operational Technology e impatto sulla safety

Agenda

- Introduzione al gruppo Phoenix Contact con focus su expertise nel mondo OT Cybersecurity
- Perché si sente parlare cosi spesso di Cybersecurity nell'ultimo periodo?
- Lo scenario normativo sta mutando; punti di vista «orizzontali» e «verticali»
- Perché dobbiamo proteggerci?
- Come proteggere una rete OT? Safety meets Security



Phoenix Contact è una multinazionale privata fondata nel 1923 ad Essen in Germania.

Progettiamo componenti di automazione e tecnologie di rete eccellenti, li combiniamo per realizzare sistemi innovativi e orientati alle soluzioni e, in collaborazione con i nostri clienti, sviluppiamo soluzioni industriali su misura con la comprovata qualità Phoenix Contact.

PHOENIX CONTACT
INSPIRING INNOVATIONS

10

Production sites

Germany | China | Taiwan | India | Poland | Sweden | Switzerland | Turkey Greece | USA

100,000

Products

20,300

Employees worldwide

75%

Sales abroad

25%

Sales in Germany

10,200

Employees in Germany

1923 > **TODAY**

Founded in Germany

Present in more than 100 countries

Brands

pressmaster QUALITY TO HAND

perle Essential Network Connectivity

pulsotronic CUSTOMIZING FUTURE

EtherWAN

PROTIQ A Phoenix Contact Company

SKS SKS Kontakttechnik GmbH

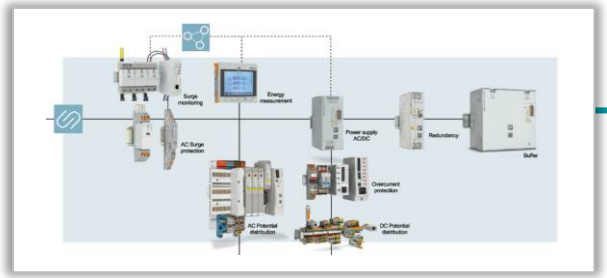
PHOENIX CONTACT INSPIRING INNOVATIONS

Di cosa ci occupiamo?

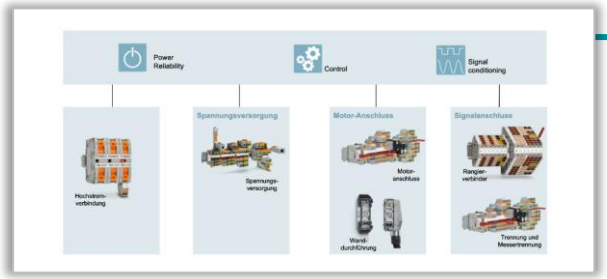
Portfolio completo per il quadro di controllo

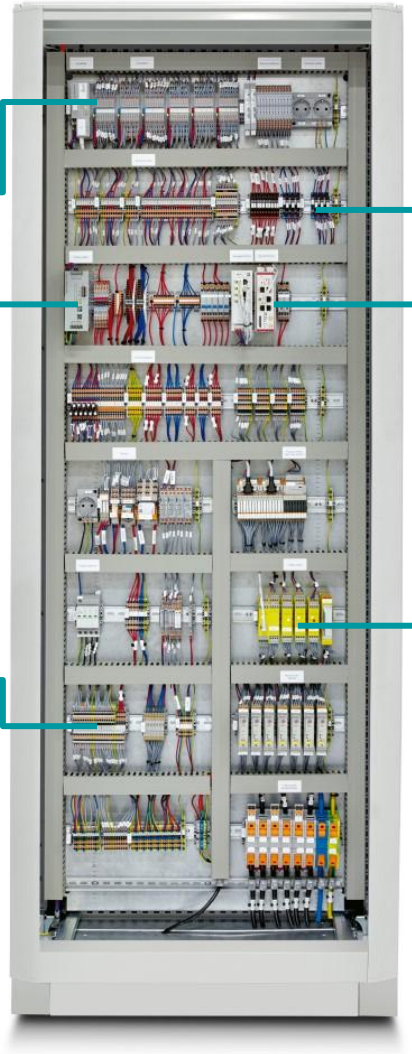
Control

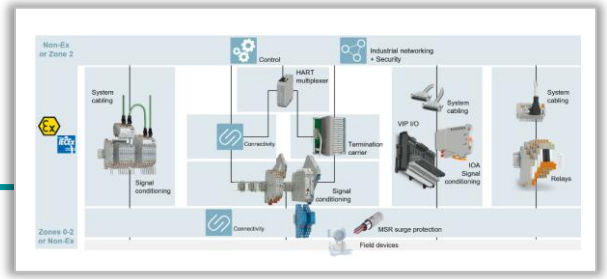
Power reliability



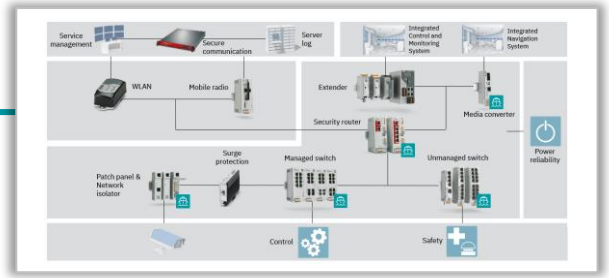
Connectivity



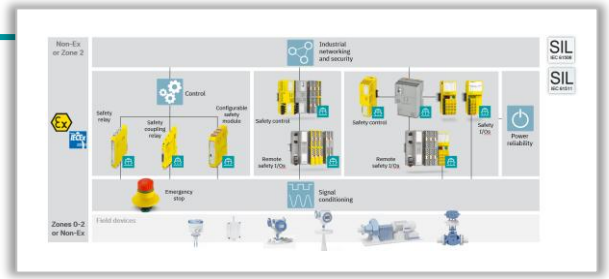




Signal conditioning



Industrial networking and security

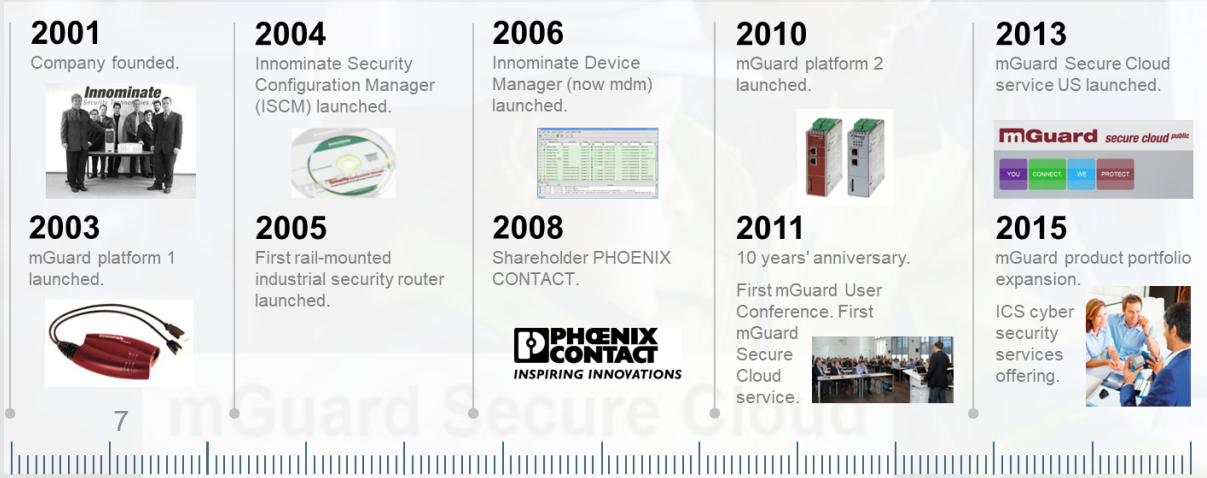


Functional safety

Industrial Cyber Security: la nostra esperienza

Produttori di security appliance e fornitori di servizi

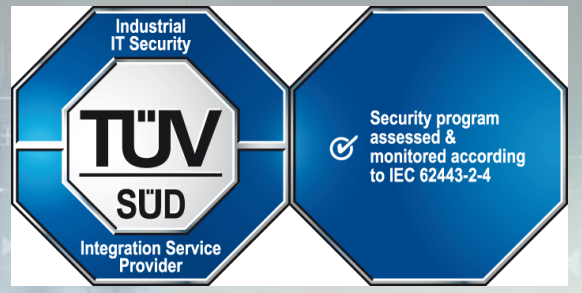
Attivi nella produzione di firewall industriali sin dal **2001**.



- ✓ Più di 3.000 clienti si affidano ai firewall mGuard per la protezione dei propri asset industriali
- ✓ Primo sistema di triangolazione Cloud attivo dal 2012 per la teleassistenza, completamente basato sulla tecnologia mGuard
- ✓ Fornitori di servizi di connettività e data transfer tra macchine e service engineers tramite VPNs (IPsec) per oltre 2.000 clienti worldwide
- ✓ Oltre 30.000 connessioni VPN gestite giornalmente
- ✓ Interfaccia Web di amministrazione e gestione con criptaggio-SSL, dotata di strong 2-factor authentication e brute-force protection
- ✓ Nessun salvataggio di dati sensibili dei clienti
- ✓ Sistema ridondante, con solid backup & recovery

Il gruppo solution sales di PxC: Safety meets Security

Partner certificati a 360°

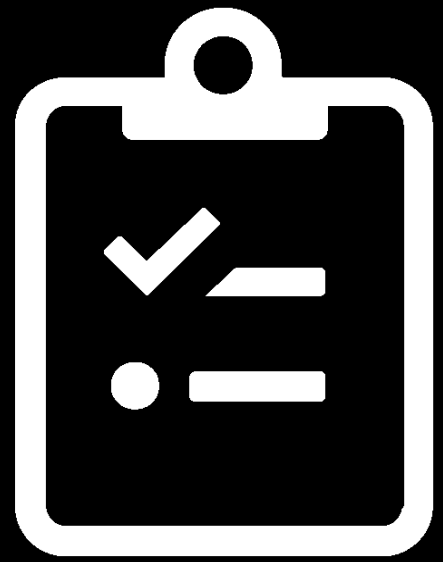


Certificati IEC 62443 per lo sviluppo di prodotti Security By Design già dal 2018, siamo certificati anche IEC 62443 come Security Provider e disponiamo di un gruppo trasversale a livello Italia in grado di erogare Servizi per la Safety e la CyberSecurity!

Gestione della cybersecurity nella Operational Technology e impatto sulla safety

Agenda

- Introduzione al gruppo Phoenix Contact con focus su expertise nel mondo OT Cybersecurity
- Perché si sente parlare cosi spesso di Cybersecurity nell'ultimo periodo?
- Lo scenario normativo sta mutando; punti di vista «orizzontali» e «verticali»
- Perché dobbiamo proteggerci?
- Come proteggere una rete OT? Safety meets Security



Il quinto dominio operativo

Cyberspazio

La tecnologia digitale ha una doppia natura

La tecnologia digitale stimola la crescita economica ma accentua rischi e minacce esistenti nel tessuto sociale.

Ciberspazio come quinto dominio

L'UE riconosce il cyberspazio come dominio operativo essenziale al pari di ***terra, mare, aria*** *e* ***spazio.***

Quadro di sicurezza europeo

Si delinea un quadro normative europeo che fornisce un approccio integrato finalizzato alla protezione, alla resilienza e alla cooperazione delle organizzazioni contro le minacce informatiche.
Prende forma il quadro strategico dell'Unione Europea in materia di difesa cibernetica: la cosiddetta cibersicurezza.

Un rischio tra i più temuti

Cyber Attacks

Al World Economic Forum 202x:

*«**Cyber Attacks** considerati uno dei **rischi più elevati** per l'economia in termini di IMPATTO e PROBABILITA'»*

COVID-19 was only one of many global hazards that threaten our existence.
Past warnings of a pandemic were often ignored, despite mounting evidence that countries needed to prepare for one.
Here is how **we must overhaul our risk reduction strategies to protect ourselves from other global disasters**.

PHOENIX CONTACT
INSPIRING INNOVATIONS

Questo riguarda anche il mondo industriale?

1980s

Bus di campo con protocolli proprietari

1990s

- Pc Standard con sistema operativo Windows entrano in impianto come HMI, sistemi SCADA ecc.

2000s

- Domanda crescente di connettività verso la rete di produzione

Today

- Le reti industriali sono sempre più basate su Ethernet (Profinet, Ethernet IP, Ethercat, PowerLink, etc.) , con un mezzo di comunicazione omogeneo dai MES fino alla rete di campo

PHOENIX CONTACT
INSPIRING INNOVATIONS

If it’s **software** is **hackable**

If it's **connected** it's **exposed**

Joshua Corman,

Director | Cyber Statecraft Initiative

@ Atlantic Council

Un po’ di storia: primo attacco alle infrastrutture critiche

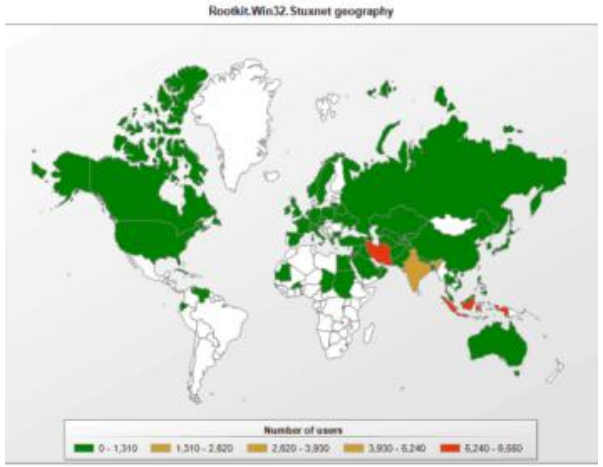
Stuxnet

- Prime infezioni a partire da Q1 2009
- Prime scoperte Q2 2010
- Infettati **100.000 impianti industriali** worldwide
- Usati ben 4 “0-day” exploits per Windows
- Diffusione attraverso service laptops, USB e rete
- Routine di attacco attivata solo su alcuni PLC setups
- Stuxnet attaccava i PLC direttamente modificandone

  delle variabili
- Cambiamenti invisibili agli operatori
  Danni causati: 2.5 – 10 milioni di dollari

Gli Hackers non hanno bisogno di grosse conoscenze su PLC o ICS per fermare il loro normale funzionamento

Fonte: http://www.langner.com/en/2011/07/21/a-time-bomb-with-fourteen-bytes/



% of PCs W32.Stuxnet Hits

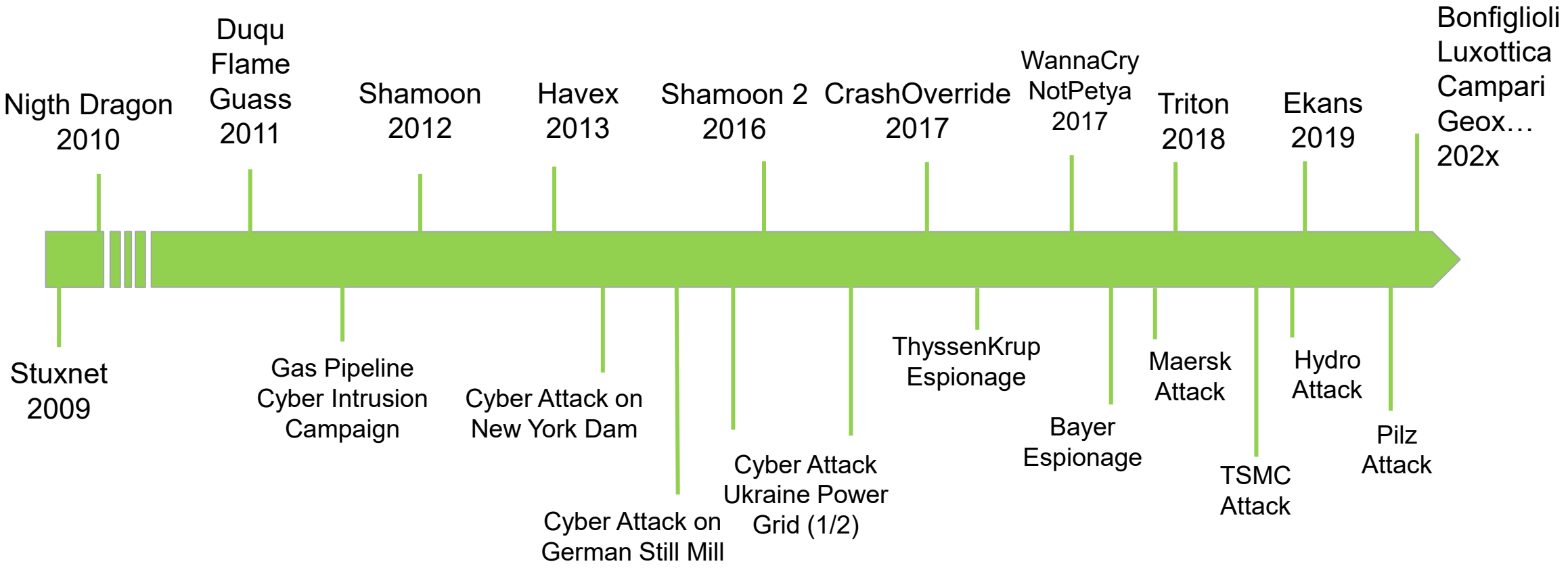
Country	Infected computers
Iran	58.85%
Indonesia	18.22%
India	8.31%
Azerbaijan	2.57%
United States	1.56%
Pakistan	1.28%
Others	9.2%

http://en.wikipedia.org/wiki/Stuxnet

PHOENIX CONTACT
INSPIRING INNOVATIONS

Un crescendo di problemi che verrà amplificato con l'arrivo delle AI…

Perché tornare a parlare di CyberSecurity adesso?



«**In passato c'erano le infrastrutture critiche. Oggi, invece, tutto è diventato critico**.
Non esiste più la 'periferia' della rete, il marginale e il secondario del sistema. È tutto centrale e primario, e ciò porta una nuova logica della vulnerabilità. Il punto fondamentale, su cui costruire sicurezza, è quindi l'intera architettura di sistema, e la visione olistica del tutto»
cit. Presidente ANIE Sicurezza

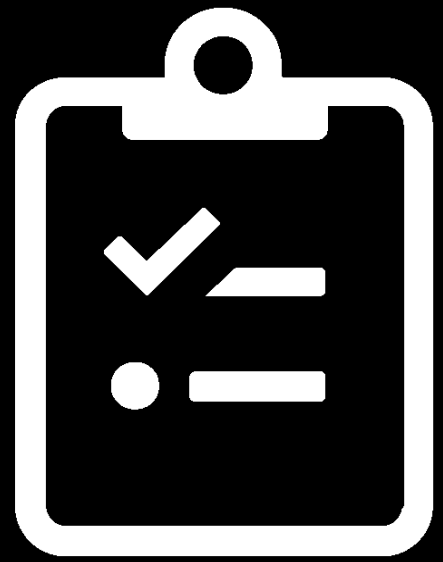
Non è questione di **se**,
Ma di **quando**

PHOENIX CONTACT
INSPIRING INNOVATIONS

Gestione della cybersecurity nella Operational Technology e impatto sulla safety

Agenda

- Introduzione al gruppo Phoenix Contact con focus su expertise nel mondo OT Cybersecurity
- Perché si sente parlare cosi spesso di Cybersecurity nell'ultimo periodo?
- Lo scenario normativo sta mutando; punti di vista «orizzontali» e «verticali»
- Perché dobbiamo proteggerci?
- Come proteggere una rete OT? Safety meets Security



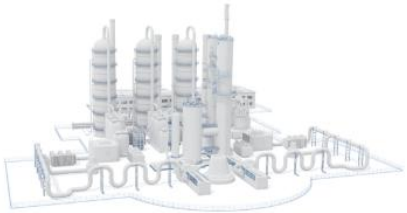
IEC 62443: lo standard di fatto

- Serie di standard internazionali che si occupano della Cybersecurity per l'Operational Technology in ambito di automazione e sistemi di controllo.
- Lo standard è diviso in diverse sezioni e descrive aspetti sia tecnici che di processo della Cybersecurity in automazione e sistemi di controllo.
- Nato 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.

PLCnext Technology
Designed by PHOENIX CONTACT

Distribuzione dei ruoli in una catena di valore secondo IEC 62443

Asset Owner



IEC 2700x ISMS

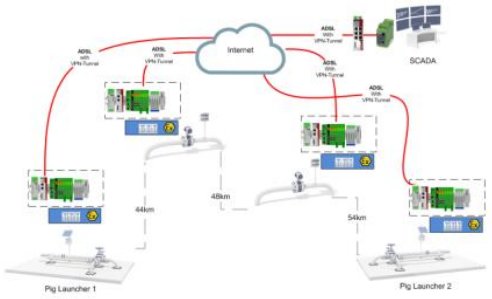
IEC 62443-2-1

IEC 62443-2-4

Protection requirements

Security Level

System Integrator



IEC 62443-3-3

Security Level

Security Level

IEC 62443-4-2

Functional requirements

Device Manufacturer

IEC 62443-4-1

Esempio: Programmazione & Implementazione di un nuovo impianto di produzione

PHOENIX CONTACT
INSPIRING INNOVATIONS

Nonostante lo standard IEC62443 esista da vent'anni la sua applicazione è sempre stata rimandata...Perché?

La Cybersecurity è da sempre percepita come un costo aggiuntivo non strettamente indispensabile al funzionamento (sicuro) delle macchine.

Cosa sta cambiando adesso?

L’Europa vuole affrontare il problema…secondo la IEC 62443 !!

L’Europa si sta muovendo con una serie di regolamentazioni e direttive con il fine di promanare fortemente una cultura a tutti i livelli sottoposti al rischio cyber sia dal punto di vista della formazione che dal punto di vista attuativo informatico IT/OT.

19.7.2016 EN Official Journal of the European Union L 194/1

I

NIS2

DIRECTIVES

DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 6 July 2016

concerning measures for a high common level of security of network and information systems across the Union

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Direttiva EU che mira a raggiungere un elevato livello comune di sicurezza informatica in tutta l'Unione europea, stabilendo i requisiti minimi di sicurezza informatica per i soggetti essenziali ed importanti

EUROPEAN COMMISSION

Brussels, 15.9.2022
COM(2022) 454 final

2022/0272 (COD)

Cyber Resilience Act

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020

Regolamento EU che mira a garantire che i prodotti con elementi digitali immessi sul mercato dell'UE presentino meno vulnerabilità possibili e che i produttori rimangano responsabili della sicurezza informatica per l'intero ciclo di vita dei loro prodotti

EUROPEAN COMMISSION

Brussels, 21.4.2021
SWD(2021) 83 final

Regolamento Macchine UE

COMMISSION STAFF WORKING DOCUMENT

EXECUTIVE SUMMARY OF THE IMPACT ASSESSMENT REPORT

Accompanying the

Proposal for a Regulation of the European Parliament and of the Council

on machinery products

{COM(2021) 202 final} - {SEC(2021) 165 final} - {SWD(2021) 82 final}

Regolamento EU che ha come obiettivo è quello di creare condizioni favorevoli per lo sviluppo di macchine sicure sotto i profili hardware e software dal momento della progettazione, dello sviluppo, fino all’immissione sul mercato e durante tutto il ciclo di vita delle medesime

Chi è interessato dalla NIS 2.0?

Essential Entities	Important Entities	Micro and Small Entities
Ex ante + ex post supervision	Ex post supervision	In generale escluse
Tutte le imprese **>250 dipendenti** nei settori di cui all'allegato I	Tutte le imprese **dipendenti >50 ma <250** nei settori di cui agli allegati I e II Tutte le imprese **dipendenti >250** nei settori di cui agli allegati II	Imprese con fatturato di <10 Mil € o <50 dipendenti **(Sono definite delle eccezioni)**

Annex I sectors

- Energy
- Transport
- Banking
- Financial Market Infrastructures
- Health
- Drinking Water
- Waste Water
- Digital Infrastructure
- ICT Service Management
- Public Administration
- Space
- \+ all critical entities under Directive (COM(2020) 829

Annex II sectors

- Postal and courier services
- Waste management
- Manufacture, production and distribution of chemicals
- Food production, processing and distribution
- Manufacturing
- Digital providers
- Research

NIS 2.0 – Che cosa bisogna fare?

Manufacturer's obligations:

1. **Policies:** Linee guida per i rischi e la sicurezza delle informazioni
2. **Incident management:** Prevenzione, rilevamento e gestione degli incidenti informatici
3. **Business Continuity:** BCM con gestione dei backup, DR, gestione delle crisi
4. **Supply Chain:** Sicurezza nella catena di approvvigionamento – fino alla richiesta di «secure developement» ai fornitori
5. **Acquisto:** Sicurezza nell'approvvigionamento di sistemi IT e di rete
6. **Efficacia:** Obiettivi per la misurazione delle misure informatiche e di rischio
7. **Training:** Igiene della sicurezza informatica
8. **Crittografia:** specifiche per la crittografia e, ove possibile, sua applicazione
9. **Personale:** Aumento Risorse umane per la Security
10. **Access Control**
11. **Asset Management**
12. **Authentication:** utilizzo dell'autenticazione a più fattori e SSO
13. **Comunicazioni:** Utilizzo di comunicazioni vocali, video e testuali sicure
14. **Comunicazioni di emergenza:** Utilizzo di sistemi di comunicazione di emergenza sicuri

Gli effetti della NIS2 cadranno a cascata dagli End User ai loro fornitori!

NIS 2.0 – Multe

Essential Entities

- almeno 10.000.000 € oppure
- almeno il 2 % del fatturato mondiale totale annuo

→ a seconda di quale sia il valore più alto

Important Entities

- almeno 7.000.000 € oppure
- almeno l'1,4 % del fatturato mondiale totale annuo

→ a seconda di quale sia il valore più alto

Gli organi di gestione dei soggetti essenziali e importanti vigilano sull'attuazione e possono essere ritenuti responsabili delle violazioni

Timeline NIS 2.0

A partire da 16 Gennaio 2023
Entrata in vigore a livello europeo

Fino a 18 Ottobre 2024
Recepimento nel diritto nazionale

Dicembre 2024- Marzo 2025
ACN – Agenzia Cybersicurezza Nazionale ITA
Chiede alle aziende di autoidentificarsi in base alla norma e auto-dichiararsi

Fino a 17 Aprile 2025
Presentazione delle aziende interessate da parte degli Stati membri dell'UE

Entro 31 Maggio 2025
ACN Chiede alle aziende di indicare domini, punto di contatto, etc

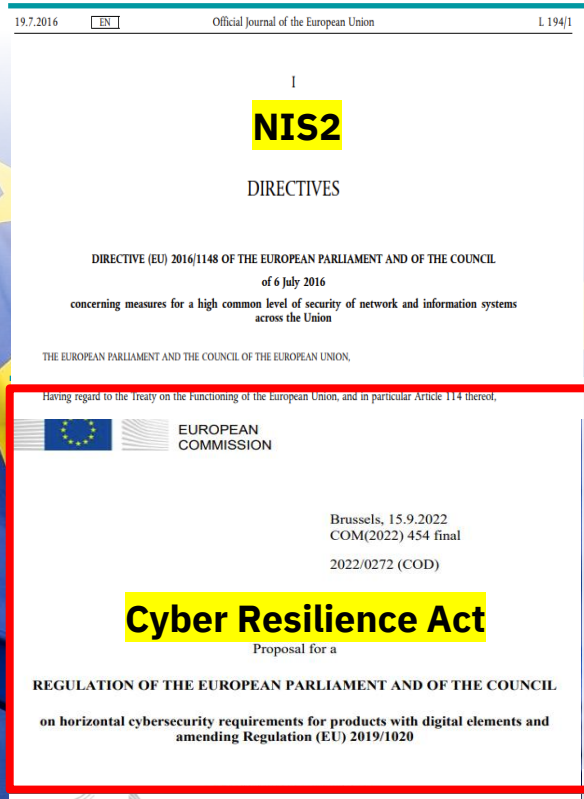
Gennaio 2026
Obbligo Notifica Incidenti

Inizio 2027
Entrata in vigore a livello nazionale

Un percorso in cui i clienti chiedono di essere aiutati!

L’Europa vuole affrontare il problema…secondo la IEC 62443 !!

L’Europa si sta muovendo con una serie di regolamentazioni e direttive con il fine di promanare fortemente una cultura a tutti i livelli sottoposti al rischio cyber sia dal punto di vista della formazione che dal punto di vista attuativo informatico IT/OT.



19.7.2016 EN Official Journal of the European Union L 194/1

I

NIS2

DIRECTIVES

DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 6 July 2016
concerning measures for a high common level of security of network and information systems across the Union

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Direttiva EU che mira a raggiungere un elevato livello comune di sicurezza informatica in tutta l'Unione europea, stabilendo i requisiti minimi di sicurezza informatica per i soggetti essenziali ed importanti

EUROPEAN COMMISSION

Brussels, 15.9.2022
COM(2022) 454 final

2022/0272 (COD)

Cyber Resilience Act

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020

Regolamento EU che mira a garantire che i prodotti con elementi digitali immessi sul mercato dell'UE presentino meno vulnerabilità possibili e che i produttori rimangano responsabili della sicurezza informatica per l'intero ciclo di vita dei loro prodotti

EUROPEAN COMMISSION

Brussels, 21.4.2021
SWD(2021) 83 final

Regolamento Macchine UE

COMMISSION STAFF WORKING DOCUMENT

EXECUTIVE SUMMARY OF THE IMPACT ASSESSMENT REPORT

Accompanying the

Proposal for a Regulation of the European Parliament and of the Council on machinery products

{COM(2021) 202 final} - {SEC(2021) 165 final} - {SWD(2021) 82 final}

Regolamento EU che ha come obiettivo è quello di creare condizioni favorevoli per lo sviluppo di macchine sicure sotto i profili hardware e software dal momento della progettazione, dello sviluppo, fino all’immissione sul mercato e durante tutto il ciclo di vita delle medesime

Cyber Resiliance Act

Prodotti con elementi digitali, per l'intero ciclo di vita

Obblighi del fabbricante, degli importatori e dei distributori:

La sicurezza informatica viene presa in considerazione nella fase di **pianificazione, progettazione, sviluppo, produzione**, **consegna** e **manutenzione**

Tutti i **rischi** per la sicurezza informatica sono **documentati**

I produttori dovranno **segnalare le vulnerabilità e gli incidenti** sfruttati attivamente

Per la durata prevista del prodotto o per un periodo di cinque anni (a seconda di quale sia il più breve), le vulnerabilità vengono gestite in modo efficace

Istruzioni chiare e comprensibili per l'uso dei prodotti con elementi digitali

Gli aggiornamenti di sicurezza devono essere resi disponibili per almeno cinque anni

CRA– Sanzioni

Non rispetto obblighi dei fabbricanti sui requisiti essenziali (AII, I)

- Fino a 15.000.000 € oppure
- Fino al 2,5 % del fatturato mondiale totale annuo

→ a seconda di quale sia il valore più alto

Cyber Resilience Act si applica integralmente dal 11 Dicembre 2027

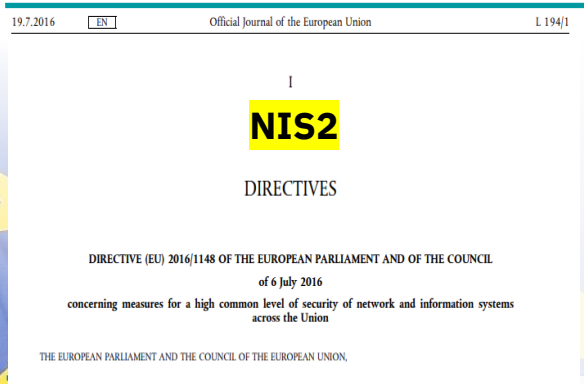
L'obbligo di comunicazione, da parte del fabbricante, delle vulnerabilità si applica da 11 Settembre 2026

Cyber Relisience Act: considerando 53

(53) I fabbricanti di prodotti che rientrano nell'ambito di applicazione del regolamento (UE) 2023/1230 del Parlamento europeo e del Consiglio ([24]) che sono anche prodotti con elementi digitali come definiti nel presente regolamento dovrebbero rispettare sia i requisiti essenziali di cui al presente regolamento sia i requisiti essenziali di cibersicurezza di cui al presente regolamento e di tutela della salute di cui al regolamento (UE) 2023/1230. I requisiti essenziali di cibersicurezza di cui al presente regolamento e alcuni requisiti essenziali stabiliti nel regolamento (UE) 2023/1230 potrebbero affrontare rischi di cibersicurezza simili. La conformità ai requisiti essenziali di cibersicurezza di cui al presente regolamento potrebbe pertanto facilitare la conformità ai requisiti essenziali che coprono anche determinati rischi di cibersicurezza di cui al regolamento (UE) 2023/1230, in particolare quelli riguardanti la protezione contro la corruzione e la sicurezza e l'affidabilità dei sistemi di controllo di cui all'allegato III, sezioni 1.1.9 e 1.2.1, di tale regolamento. Tali sinergie devono essere dimostrate dal fabbricante, ad esempio attraverso l'applicazione, se

L’Europa vuole affrontare il problema…secondo la IEC 62443 !!

L’Europa si sta muovendo con una serie di regolamentazioni e direttive con il fine di promanare fortemente una cultura a tutti i livelli sottoposti al rischio cyber sia dal punto di vista della formazione che dal punto di vista attuativo informatico IT/OT.



19.7.2016 EN Official Journal of the European Union L 194/1

I

NIS2

DIRECTIVES

DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 6 July 2016
concerning measures for a high common level of security of network and information systems across the Union

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Direttiva EU che mira a raggiungere un elevato livello comune di sicurezza informatica in tutta l'Unione europea, stabilendo i requisiti minimi di sicurezza informatica per i soggetti essenziali ed importanti

EUROPEAN COMMISSION

Brussels, 15.9.2022
COM(2022) 454 final

2022/0272 (COD)

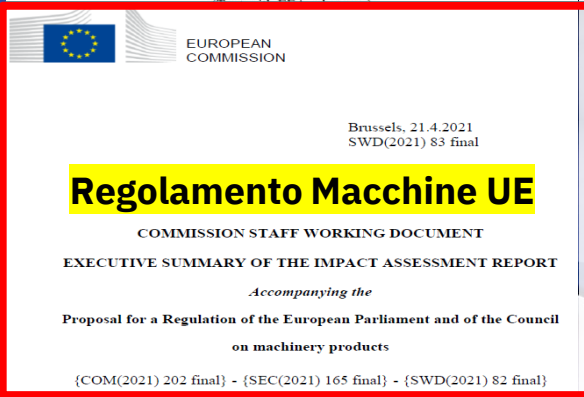
Cyber Resilience Act

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020

Regolamento EU che mira a garantire che i prodotti con elementi digitali immessi sul mercato dell'UE presentino meno vulnerabilità possibili e che i produttori rimangano responsabili della sicurezza informatica per l'intero ciclo di vita dei loro prodotti



EUROPEAN COMMISSION

Brussels, 21.4.2021
SWD(2021) 83 final

Regolamento Macchine UE

COMMISSION STAFF WORKING DOCUMENT

EXECUTIVE SUMMARY OF THE IMPACT ASSESSMENT REPORT

Accompanying the

Proposal for a Regulation of the European Parliament and of the Council on machinery products

{COM(2021) 202 final} - {SEC(2021) 165 final} - {SWD(2021) 82 final}

Regolamento EU che ha come obiettivo è quello di creare condizioni favorevoli per lo sviluppo di macchine sicure sotto i profili hardware e software dal momento della progettazione, dello sviluppo, fino all’immissione sul mercato e durante tutto il ciclo di vita delle medesime

Safety meets Security

Nuovo Regolamento Macchine UE 2023/1230

Sostituisce la Direttiva Macchine (dal 20 gennaio 2027), rappresenterà il punto di riferimento normativo in termini sicurezza macchine con lo scopo di garantire che le macchine immesse nel mercato europeo siano sicure.

Tra le novità introdotte ci sono requisiti in termini di cyber security al fine di garantire la sicurezza del macchinario anche se oggetto di manomissione o attacco informatico: Allegato III, Sezione 1.1.9

Non può esserci safety senza security!!

January 20, 2027

ACT NOW!

Regolamento Macchine – Alcune considerazioni

CONSIDERANDO

- → Direttiva Macchine: n.30
- → Regolamento Macchine: n.86

SOFTWARE

- → Direttiva Macchine: n.1 [p.to 1.2.1 Allegato I – «un'avaria nell'hardware o nel software del sistema di comando non crei situazioni pericolose»]
- → Regolamento Macchine: n.22 [5vv nei considerando – 17vv nel testo del regolamento, di cui 6vv nel p.to 1.1.9 Allegato III e 2vv nel p.to 1.2.1 Allegato III]

focus sull'importanza del SOFTWARE !!!

Regolamento Macchine – Alcune considerazioni

1.1.9. *Protezione dall'alterazione*

La macchina o il prodotto correlato devono essere progettati e costruiti in modo tale da fare sì che il collegamento ad essi di un altro dispositivo, tramite qualsiasi caratteristica del dispositivo connesso stesso o tramite qualsiasi dispositivo remoto che comunica con la macchina o il prodotto correlato, non determini una situazione pe

If it's software is hackable

If it's connected it's exposed

1.2.1. *Sicurezza ed affidab*

I sistemi di com l'insorgere di situazioni pericolose.

I sistemi di comando devono essere progettati e costruiti in modo tale che:

a) riescano a resistere, se del caso, a circostanze e rischi, a previste sollecitazioni di servizio e ad influssi esterni intenzionali o meno, compresi tentativi deliberati ragionevolmente prevedibili da parte di terzi che conducono a una situazione pericolosa;

focus sulla possibilità di comunicare con la macchina, NON sul collegamento a internet

Regolamento Macchine – Alcune considerazioni

Una classica domanda:

Se ho una macchina con la safety tutta elettromeccanica, senza possibilità di comunicazione in rete con PLC ed HMI il RESS 1.1.9 (e quindi 1.2.1 – ndr) è corretto considerare che non sarà applicabile?

NO!!! OVVIAMENTE NEL PROCESSO DI VALUTAZIONE DEL RISCHIO DI QUESTA MACCHINA SI DOVRA' TENERE CONTO SIA DI QUANTO RICHIESTO DAL RESS 1.1.9 CHE DI QUANTO RICHIESTO DAL RESS 1.2.1

MA COME ???

focus sulla possibilità di comunicare con la macchina, NON sul collegamento a internet

Safety meets Security – Alcune considerazioni

1. Esposizione al rischio di alterazione (evento involontario/attacco informatico) in base alla tipologia di connessione:
   - Nessuna connessione → livello di esposizione basso
   - Connessione esclusivamente alla rete aziendale → livello di esposizione medio
   - Connessione diretta o indiretta a internet → livello di esposizione alto

Già da questa prima e grossolana classificazione posso cominciare a stimare quanto la macchina sia esposta a possibili vettori di compromissione digitale, considerando sia la configurazione iniziale sia eventuali modifiche future (es. aggiunta di modem, gateway, assistenza remota, sensoristica IoT, aggiornamenti software, ecc.).

2. Livello di rischio della sicurezza funzionale (safety) come risultante dal risk assessment secondo le norme ISO 12100 e ISO 13849-1:
   - Definizione del Performance Level richiesto (PLr) → a, b, c, d, e

focus sulla possibilità di comunicare con la macchina, NON sul collegamento a internet

Safety meets Security – Potenziale norma armonizzata per i requisiti 1.1.9 ed 1.2.1

prEN 50742: Securing Machinery Against Corruption

Perché è importante?

La norma prEN 50742 fornisce un approccio strutturato alla progettazione, al funzionamento e alla documentazione di macchinari resistenti alle manomissioni e alle minacce informatiche, durante l'intero ciclo di vita.

Di cosa tratta?

- Definizione di un Safety Related Security Level per ogni funzione di sicurezza.
- Definizione delle contromisure minime necessarie per ogni SRLS riscontrato nell'analisi del rischio.
- Allineamento con IEC 62443-4-1 e -4-2 per la sicurezza tecnica e di processo di sviluppo mantenendo anche la strada aperta per un approccio più pratico.

Approach A
(Standalone approach)

- Risk assessment (EN ISO 12100:2010)
- Security context
- List of threats
- Impact on safety functions
- Countermeasures

Approach B
(IEC62443 approach)

- EN IEC 62443-4-1:2018
- EN IEC 62443-3-3:2019
- EN IEC 62443-4-2:2019

KNOW-HOW IN SAFETY
by GIT SICHERHEIT & PHOENIX CONTACT

Punti di vista normativi

Orizzontali o verticali?

NIS-2

- Pone sfide significative per gli ambienti **"brownfield»**
- Infrastrutture, sistemi IT/OT e impianti industriali preesistenti, spesso datati, che NON sono stati progettati con la sicurezza informatica nativa ("secure by design") e che devono ora essere adeguati.
- Per le aziende con ambienti brownfield, la compliance non passa necessariamente per la sostituzione totale degli impianti (costosa e poco pratica), ma per un approccio basato sulla gestione del rischio e sulla sicurezza stratificata: segmentazione, controlli compensativi, monitoraggio, training…
- Può essere considerata una norma **ORIZZONTALE**; non è verticale su un comparto ma impone requisiti su molteplici settori

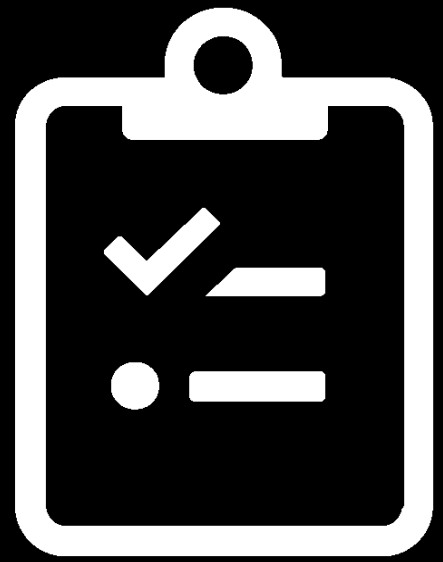
NUOVO REGOLAMENTO MACCHINE UE 2023/1230:

- Pone sfide significative per i costruttori ed il parco macchine **‘’greenfield’’**
- Mira a regolamentare l’uso delle moderne tecnologie introducendo requisiti necessari ad un adattamento all’era digitale (AI, Robotica avanzata, Cybersecurity..)
- Può essere considerata una norma **VERTICALE** poiché va ad impattare quasi unicamente il comparto degli OEM (e solo in caso di modifica sostanziale anche gli End User che agirebbero come OEM)

Gestione della cybersecurity nella Operational Technology e impatto sulla safety

Agenda

- Introduzione al gruppo Phoenix Contact con focus su expertise nel mondo OT Cybersecurity
- Perché si sente parlare cosi spesso di Cybersecurity nell'ultimo periodo?
- Lo scenario normativo sta mutando; punti di vista «orizzontali» e «verticali»
- Perché dobbiamo proteggerci?
- Come proteggere una rete OT? Safety meets Security



Le minacce di Cybersecurity sono in costante crescita e gli attacchi risultano più complessi e sofisticati

In passato le “infrastrutture” erano il punto “critico” su cui intervenire. Oggi, invece, le criticità risiedono in ogni area.

39 SECONDI
Tempo medio tra 2 Cyber Attack

4 milioni EURO
Costo medio di un Cyber Attack

~10.000 miliardi EURO
Danno mondiale annuale

10%
Budget medio per la Cybersecurity

1 EURO
Costo affitto tool su darkweb

Attacco informatico e Safety: malware TRITON/TRISIS

QUANDO E DOVE

→ 2017 | impianto petrolchimico in Arabia Saudita.

COSA

→ primo attacco informatico noto progettato per uccidere e creato per prendere il controllo dei controller di sicurezza (Safety Instrumented System) Triconex prodotti da Schneider Electric.

OBIETTIVO

→ permettere agli hacker di modificare la logica di sicurezza del sistema ESD (Emergency Shut Down), consentendo un attacco che potrebbe causare il malfunzionamento dell'impianto senza che i sistemi di allarme entrino in funzione, o forzandone un arresto non sicuro..

PHOENIX CONTACT
INSPIRING INNOVATIONS

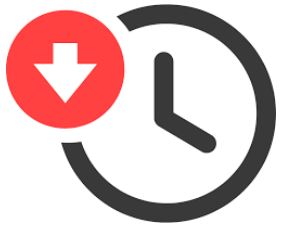
Possibili conseguenze di un attacco informatico

Perdita di dati

Safety

ransomware

Danni alla reputazione



Fermi produzione

Il valore dei rischi sulla vita umana non sono quantificabili...

Know How

ambientali

PHOENIX CONTACT
INSPIRING INNOVATIONS

Fermi impianto non previsti: I COSTI NASCOSTI DELLA NON SICUEZZA

Alla ricerca della resilienza ed antifragilità

IMPATTO SULLA DISPONIBILITÀ

Attacchi ransomware o malware possono bloccare asset critici (HMI, SCADA, PLC, ...) causando interruzioni produttive e perdita di efficienza.

EFFETTI SULLE PERFORMANCE

Traffico malevolo crea latenza e ritardi nella rete OT, riducendo la velocità e l'efficienza delle linee produttive.

COMPROMISSIONE DELLA QUALITÀ

Manipolazione dei setpoint e dati sensoriali alterati aumentano scarti e rilavorazioni, peggiorando la qualità produttiva.

323 ore

I grandi impianti perdono 323 ore di produzione in un anno.[1]

$532,000 ora

E' la media dei costi ora per fermi impianto non pianificato in grandi impianti manufatturieri industriali.[1]

OEE* = Disponibilità × Performance × Qualità

La cybersecurity è un fattore chiave per migliorare efficienza, resilienza e continuità produttiva.

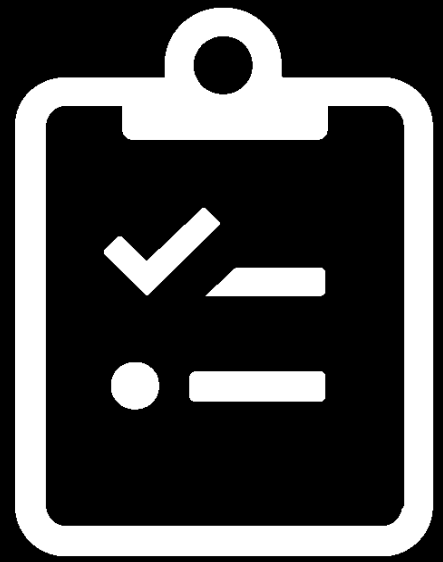
*Overall Equipment Effectivness

PHOENIX CONTACT

Gestione della cybersecurity nella Operational Technology e impatto sulla safety

Agenda

- Introduzione al gruppo Phoenix Contact con focus su expertise nel mondo OT Cybersecurity
- Perché si sente parlare cosi spesso di Cybersecurity nell'ultimo periodo?
- Lo scenario normativo sta mutando; punti di vista «orizzontali» e «verticali»
- Perché dobbiamo proteggerci?
- Come proteggere una rete OT? Safety meets Security



Differenze tra Information & Operation Technology

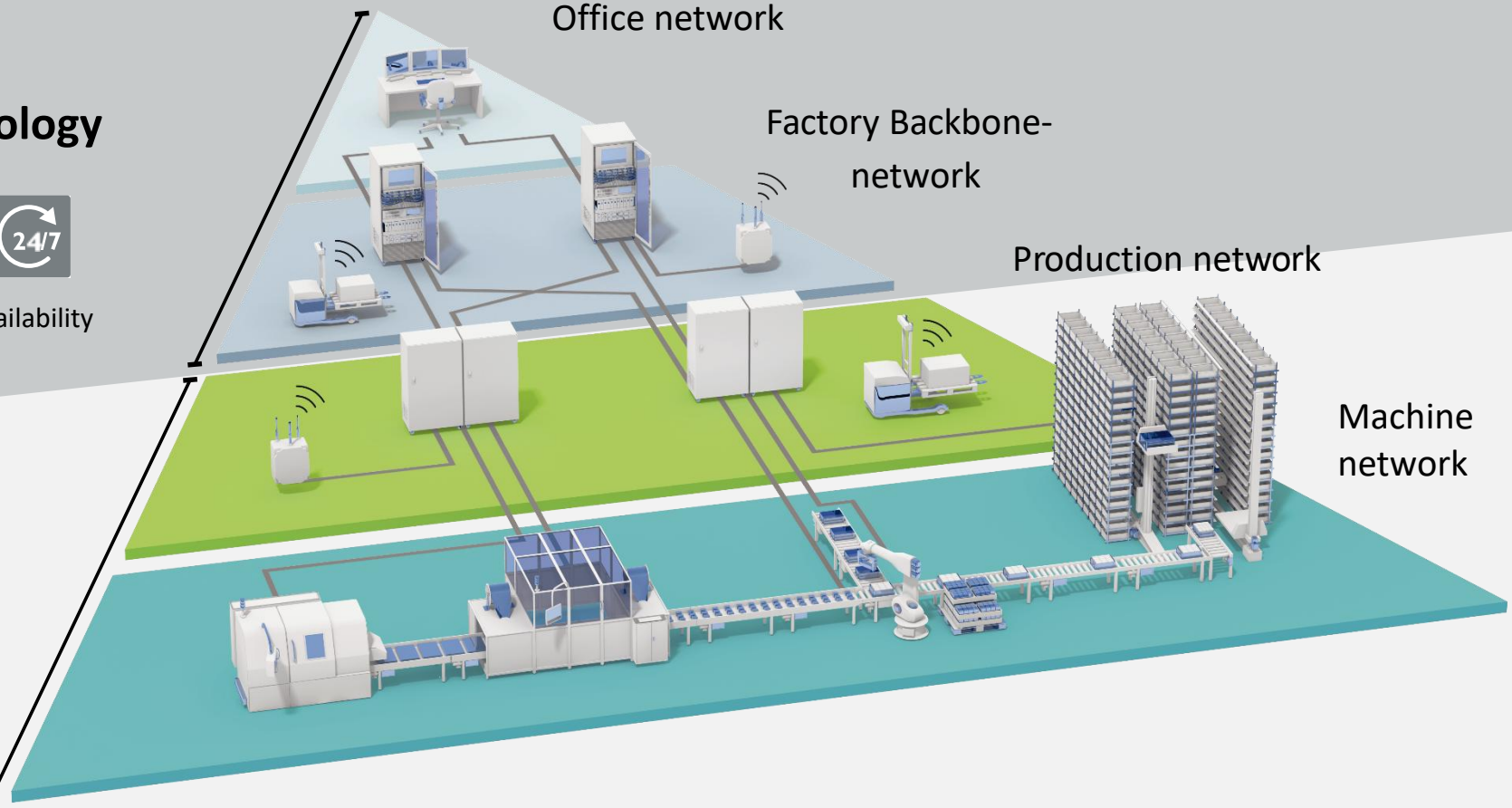
Information Technology

Confidentiality | Integrity | Availability

≠

Operation Technology

Availability | Integrity | Confidentiality



PHOENIX CONTACT
INSPIRING INNOVATIONS

Due approcci diversi che concorrono ad un’unica soluzione

Industrial Security vs. Office Security

Availability
Integrity
Confidentialy

ICS-Security

	Proprietà	
Fault non tollerabili	Availability	Brevi fault tollerabili
Difficili	Restart	Possibili
Grande Sfida	Patch Management	Automatizzati
7-20 anni	Lifetime HW	3-5 anni
Distribuito	Know How	Centralizzato

Confidentiality
Integrity
Availabitity

IT-Security

PHOENIX CONTACT
INSPIRING INNOVATIONS

Approccio Defense in Depth

I problemi peculiari del mondo OT

- ❑ PC in produzione con OS obsoleti
- ❑ PC in produzione senza Antivirus
- ❑ Credenziali di accesso deboli e mal salvate
- ❑ Accessi remoti non controllati alle macchine
- ❑ Porte USB non controllate
- ❑ Mancanze di aggiornamenti FW
- ❑ Reti piatte e non segregate

La classica soluzione IT di un firewall in testa alla rete non elimina i problemi; esistono molteplici punti di ingresso in grado di bypassarla.

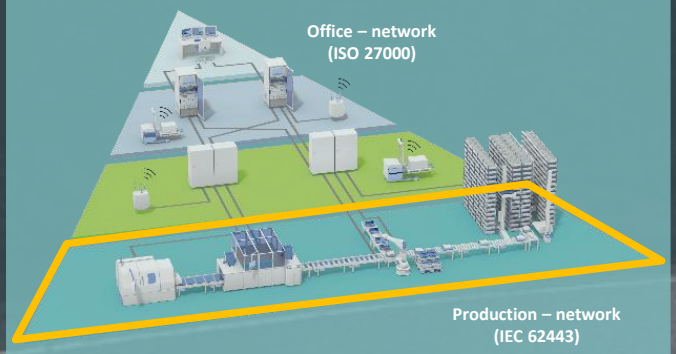
Esistono vulnerabilità note nel mondo OT che non possono essere fixate a meno di non fermare la produzione…serve un approccio diverso: la vulnerabilità va isolata e protetta con più «strati». Nasce il concetto di «Defense in Depth»

PHOENIX CONTACT
INSPIRING INNOVATIONS

Un percorso olistico: safety meets security

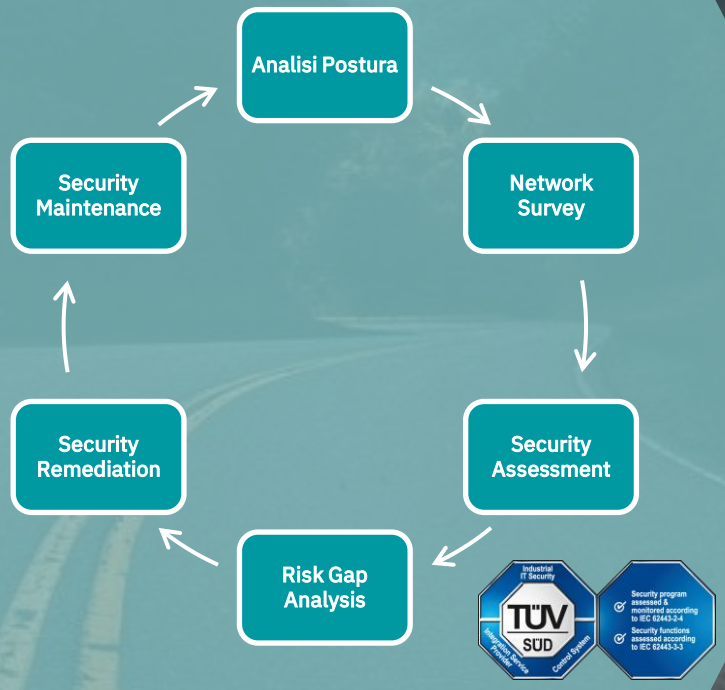
Progettazione di un concetto di “macchina sicura 5.0“ (safety meets security)

Punto di partenza:
Informazioni sullo stabilimento

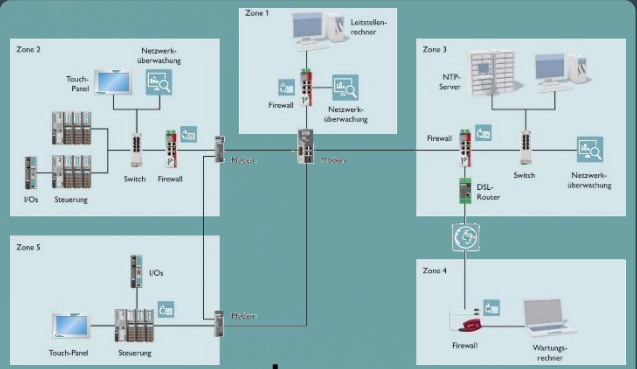


Concetto di sicurezza in ambito Operation Technology

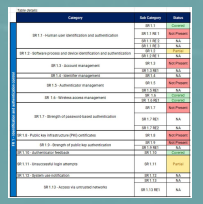
Percorso:
Progettazione di un concetto di sicurezza



Risultato:
Concetto di sicurezza olistico



+



Risultati Assessment + Documentazione Utile per accompagnamento macchina + Possibile Blueprint Soluzione + Training

Lo step fondamentale

Security Assesment

Il servizio di Security Assesment ha l'obiettivo di valutare la postura di sicurezza informatica dei sistemi OT esistenti (o in fase di introduzione) all'interno di un impianto, una cella o un'isola produttiva.

La valutazione può essere condotta in conformità allo standard IEC 62443-3-3, che consente di identificare le lacune (gap) rispetto ai requisiti tecnici richiesti per i vari Security Level (SL).

L'attività consente di:

- Mappare il livello di conformità ai requisiti di sicurezza definiti dallo standard;
- Evidenziare le aree critiche o non conformi;
- Fornire una base tecnica per la pianificazione di azioni correttive e l'elevazione del livello di protezione del sistema.

Table details:

	Category	Sub Category	Status
FR 1 - Identification and authentication control	SR 1.1 - Human user identification and authentication	SR 1.1	Covered
		SR 1.1 RE 1	Not Present
		SR 1.1 RE 2	NA
		SR 1.1 RE 3	NA
	SR 1.2 - Software process and device identification and authentication	SR 1.2	Partial
		SR 1.2 RE 1	NA
	SR 1.3 - Account management	SR 1.3	Not Present
		SR 1.3 RE1	NA
	SR 1.4 - Identifier management	SR 1.4	NA
	SR 1.5 - Authenticator management	SR 1.5	Not Present
		SR 1.5 RE1	NA
	SR 1.6 - Wireless access management	SR 1.6	Covered
		SR 1.6 RE1	Covered
	SR 1.7 - Strength of password-based authentication	SR 1.7	Not Present
		SR 1.7 RE1	NA
		SR 1.7 RE2	NA
	SR 1.8 - Public key infrastructure (PKI) certificates	SR 1.8	Not Present
	SR 1.9 - Strength of public key authentication	SR 1.9	Not Present
		SR 1.9 RE1	NA
	SR 1.10 - Authenticator feedback	SR 1.10	Covered
	SR 1.11 - Unsuccessful login attempts	SR 1.11	Partial
	SR 1.12 - System use notification	SR 1.12	NA
	SR 1.13 - Access via untrusted networks	SR 1.13	NA
		SR 1.13 RE1	NA

Uno step che non deve mai mancare

Security Trainings

Investire nella formazione Cybersecurity OT significa adottare un approccio proattivo alla sicurezza, aumentando la consapevolezza del personale e preparando l'organizzazione a fronteggiare minacce sempre più sofisticate.

Esistono formule di training personalizzate (in aula o attraverso tool informatici) in base ai ruoli e alle specifiche esigenze di ciascun gruppo.

Gli obiettivi dei corsi devono essere:

- Comprendere gli aspetti della cybersecurity specifici per le applicazioni OT;
- Individuare i potenziali rischi cyber di un impianto di automazione;
- Apprendere le tecniche per proteggere le reti OT;
- Comprendere le basi di networking e sicurezza IT in contesti OT.

Un percorso olistico: safety meets security

Una possible soluzione

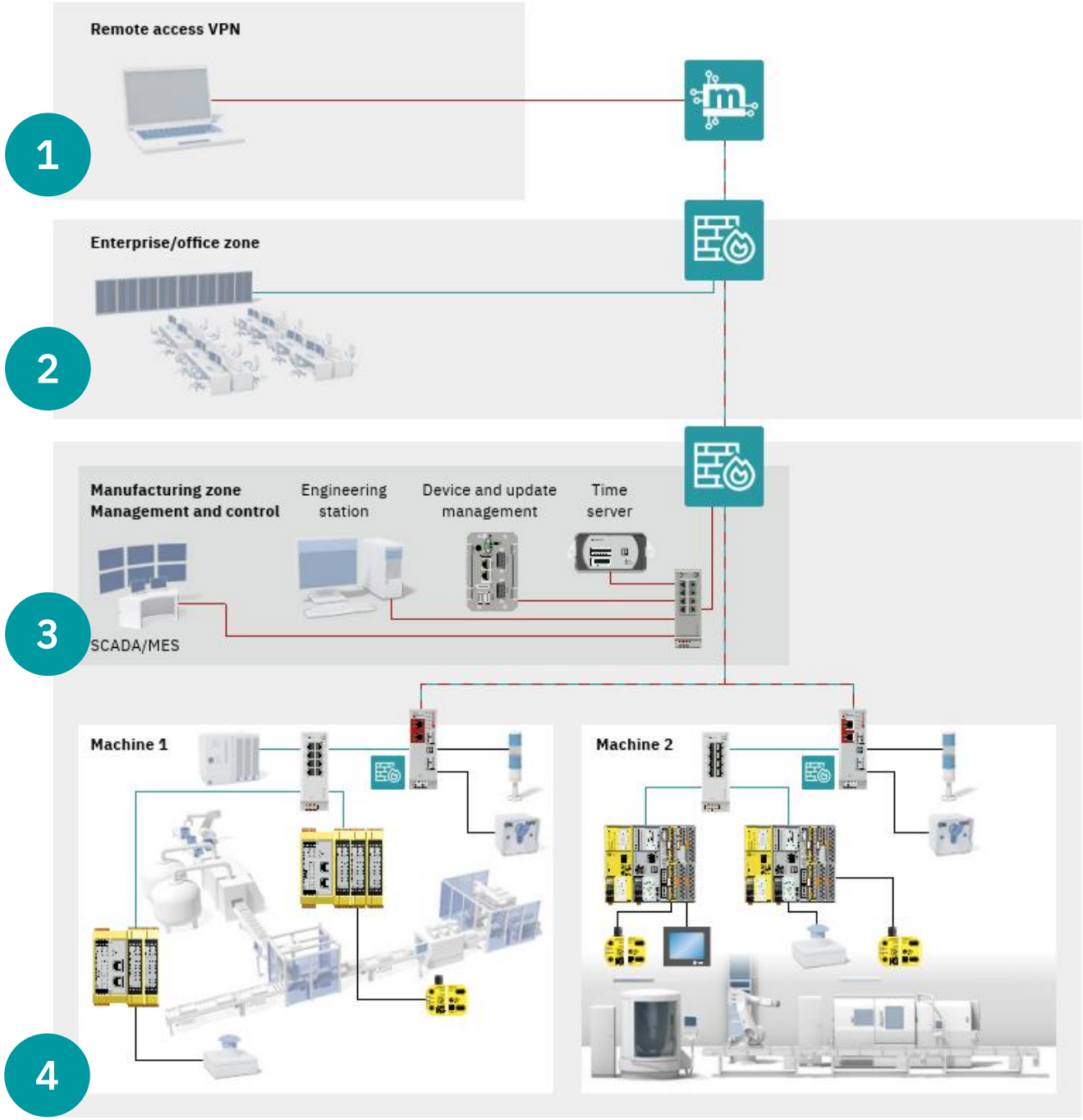
IT

1. REMOTE ACCESS VPN
2. ENTERPRISE/OFFICE ZONE

OT

3. MANUFACTURING ZONE
4. MACHINE ZONE

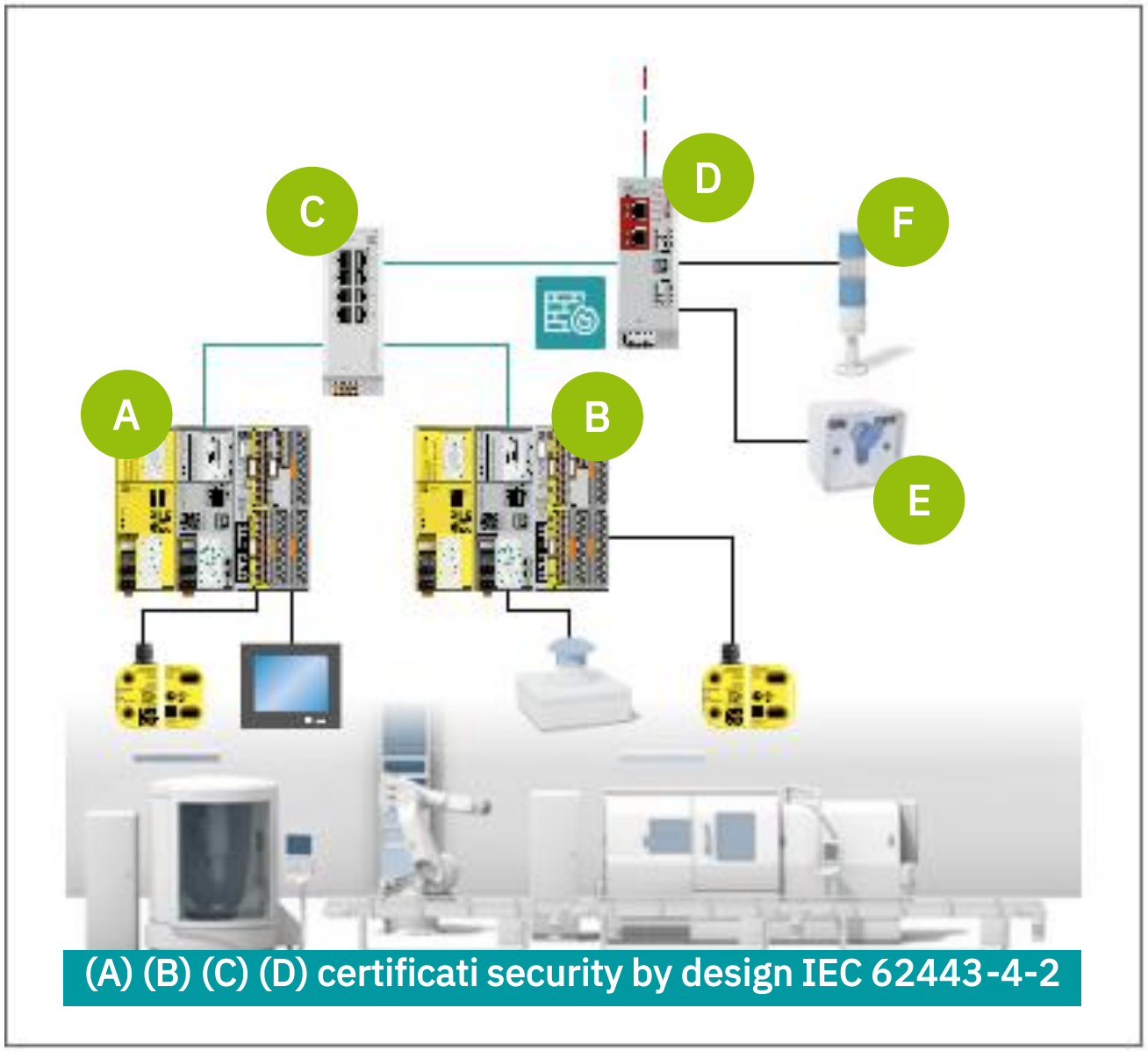
Defense in Depth – DMZ – Segmentazione OT



Un percorso olistico: safety meets security

MACHINE ZONE 2

- linea di produzione con Safety PLC (A) (B);
- comunicazione sicura dei controllori di sicurezza tramite switch managed (C);
- accesso «logico» sicuro alla linea di produzione grazie alla presenza del router industriale mGuard (D);
- interruttore a chiave (E) accessibile solo al personale autorizzato in loco per un controllo completo sulla creazione della connessione VPN. L'attivazione della connessione è reso visibile da specifica torretta di segnalazione (F).




PHOENIX CONTACT