
ANIE AUTOMAZIONE
ANIE FEDERAZIONE
CONFINDUSTRIA
Are You S(EC)URE ?
Massimiliano Spano
Rockwell Automation

La comunicazione efficace tra dispositivi aiuta le persone nel quotidiano, risparmiando energia e diminuendo i costi.

92% AZIENDE

# Parliamo di Italia

62% DANNI PER 80k€

«Ci sono due tipi di aziende: quelle che sono state hackerate e quelle che non sanno ancora di essere state attaccate»

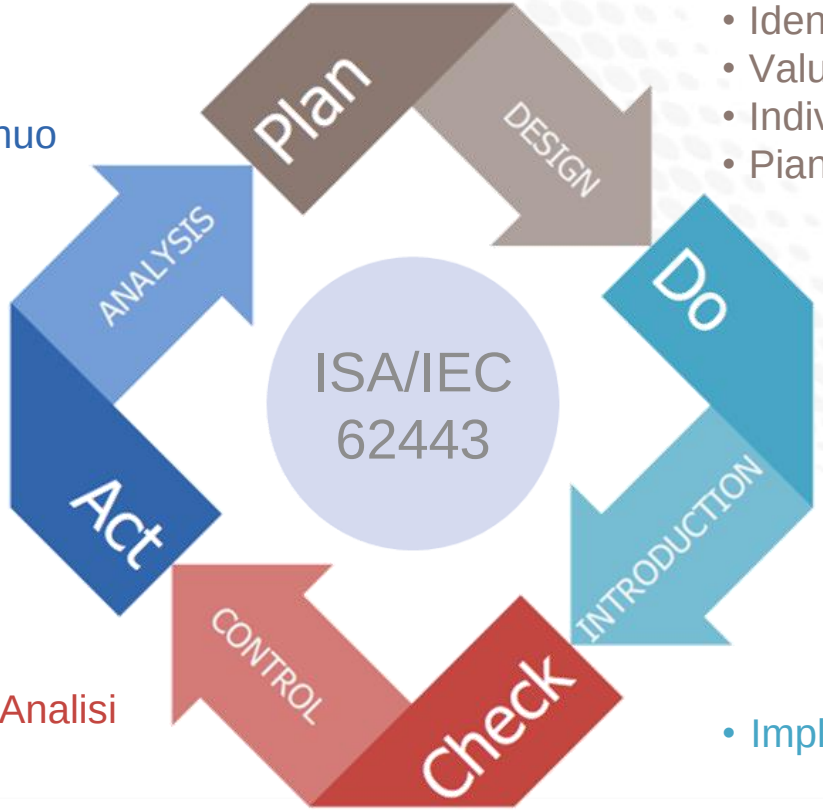
**John Chambers, ex CEO, Cisco**

# IACS Threat Vectors

# Metodo

Plan-Do-Check-Act (PDCA)

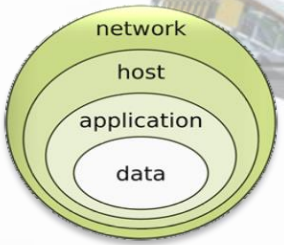
- Sviluppo continuo




- Identificazione del rischio
- Valutazione del rischio
- Individuare misure
- Pianificare il rilascio

- Implemetare le misure

- Monitoraggio&Analisi
- Revisione





**Security Assessment:** riconoscere le aree di rischio e le potenziali minacce

**Defense-in-depth security:** implementare un approccio di sicurezza a più livelli

**Trusted vendors:** prodotti progettati secondo i principi fondamentali di sicurezza

## La proposta delle aziende del settore Automazione Industriale

# DESIGN - IEC62443 3-3 Dove si trova oggi la tua azienda?

Cosa sono i “Target Security Level”?

Protect Against **Intentional Unauthorized Access Using Sophisticated Means with Extend Resources,** IACS specific Skills & High Motivation – **Nation-state**

Security Level 4

Protect Against Intentional Unauthorized Access Using **Sophisticated Skills** with Moderate Resources, IACS specific skills & Moderate Motivation – **Cyber Terrorism**

Security Level 3

Protect Against Intentional Unauthorized Access Using **Simple Means** with Low Resources, Generic Skills, & Low Motivation – **Cyber Crime, Hackers**

Security Level 2

Protect Against **Casual or Incidental** Unauthorized Access – **Employee Error**

Security Level 1

# Cybersecurity standards per IACS

Avere uno standard per la “Cybersecurity” ci permette di avere:

- **Linguaggio comune** e **terminologia** dedicata al settore industriale
- Una **metodologia standardizzata**
- Una linea guida per rispondere alle seguenti domande:
  - Qual’è il mio effettivo rischio **attuale**?
  - Quale potrebbe essere un livello di rischio **più accettabile** per la mia azienda
  - Come posso arrivare ad ottenere questo livello **più accettabile**?


The Cyber Security
THANK YOU
it affects all of US