L'ELIMINAZIONE DEI RISCHI DI CYBERSICUREZZA NELL'INDUSTRIA SOSTENIBILE 4.0

Seminario ASTRI

"Sustainability" 2022"

La problematica energetica

Roma, 24 Novembre 2022

Ing. Domenico Barone *– Consigliere ASTRI – Esperto Sicurezza degli impianti a rischio di incidente rilevante*

*Tecnologie Sicurezza Industriale S.r.l.***,** *via P. Lomazzo 51, 20154 Milano,* *do.barone.tsi@gmail.com*

Indice

1. Importanza della Cybersicurezza

- Negli ultimi 20 anni le grandi Società hanno iniziato ed elaborare fare report su tematiche e rischi ESG (Environment, Social, Governement)

- Nei Rapporti di Sostenibilità, la cybersicurezza ed ultimamente anche la cyberesilienza, sono state oggetto di reporting e di notizie sullo status

- I sempre maggiori investimenti in cybersicurezza sono basati su proiezioni di esperti che tengono conto delle minacce di cybersicurezza, le quali sono destinate ad evolvere in termini di numerosità e complessità

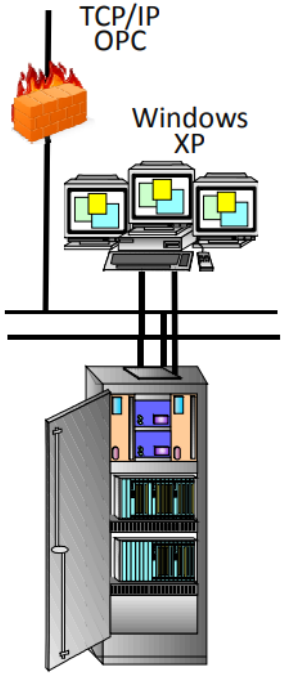
- La strategia di cybersicurezza è generalmente basata su standard ISO/IEC 27001 Information Security Management ed ISO 22301 Bussiness Continuity

2. Rischi di cybersicurezza

Nell'industria 4.0 ed in particolare nelle infrastrutture critiche è molto presente l'OT (Operational Technology) nei sistemi :

- SCADA per monitorare e controllare a distanza
- PLC Controllori logici programmabili
- DCS Sistemi di regolazione

Esempio di DCS

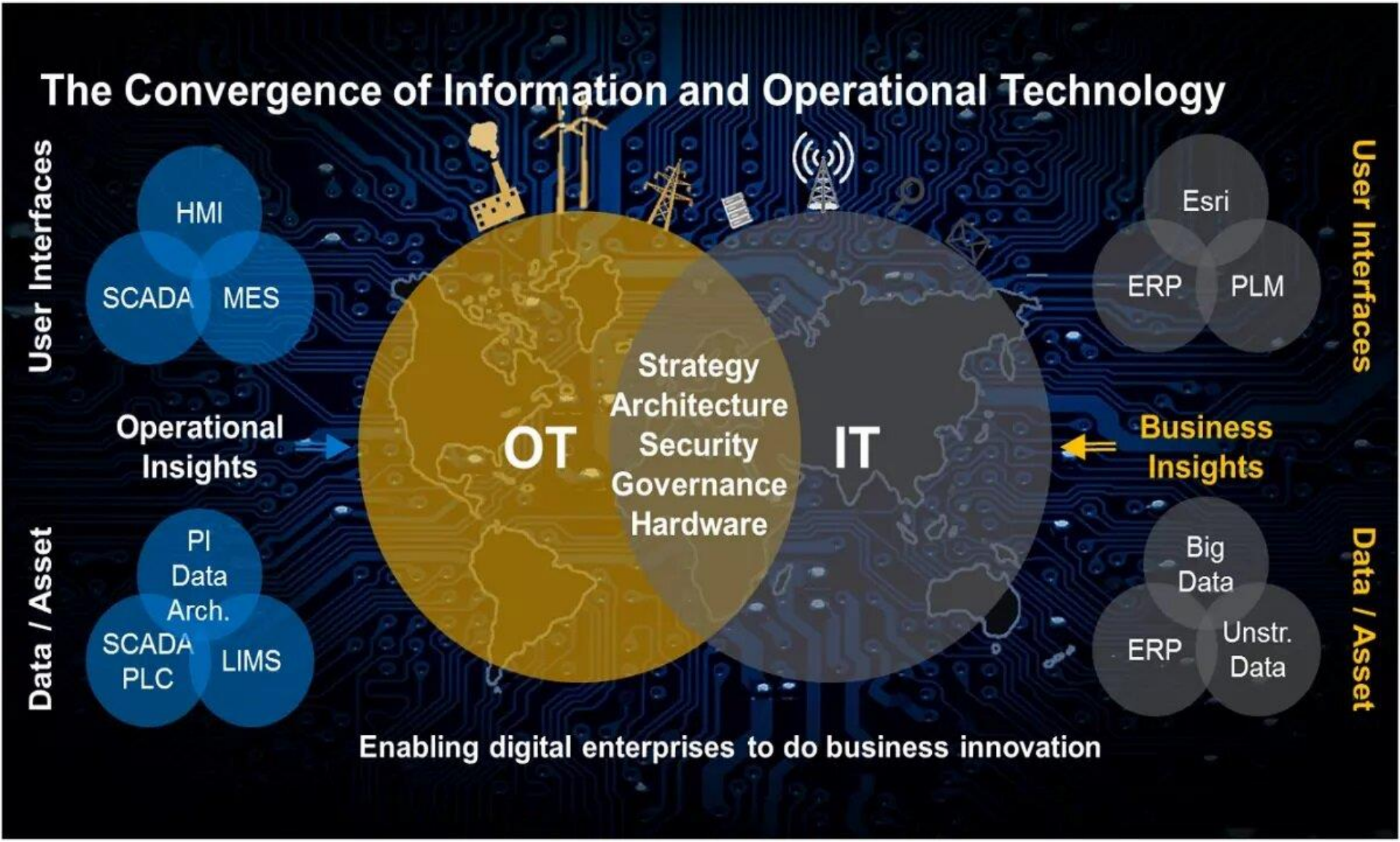


Device/Element: Distributed Control System (DCS) Interface: 100 Base FO, MS Windows, RTLinux, TCP/IP, OPC, IIS, MySQL			
Threats:	Consequences:	Attack Vector:	Countermeasures:
Physical damage to device	Process/unit trip	Physical access to device	Physical access controls
Modified regulatory control or safety logic	Create dangerous process conditions, possible injuries	Remote connectivity via Corporate WAN, via support access, via malware infection	Multi-layer DiD with strong boundary (DMZ) defenses, monitoring and full O&M controls
Op Console hijacking and manual override of controls	Explosive conditions, plant damage, death and injuries, threat to public health	Remote connectivity via Corporate WAN, via support access, via malware infection	Multi-layer DiD with strong boundary (DMZ) defenses, monitoring and full O&M controls
Disable communications (DOS attack)	Operators blind, process/unit trip, plant shutdown required	Remote connectivity via Corporate WAN, via support access, via malware infection	Multi-layer DiD with strong boundary (DMZ) defenses, monitoring and full O&M controls

- Tali sistemi OT sono generalmente costituiti da circuiti elettronici integrati, gestiti da un Sistema Operativo Windows ormai utilizzato in tutti i campi (aerospaziale, militare, industriale, medico…)

- I sistemi OT, inizialmente separati dal resto dei sistemi informatici IT (Information Technology), si sono progressivamente connessi a questi ultimi con possibilità di accesso dall'esterno tramite internet (vedi slide successiva)

Interconnessione tra OT ed IT



- Da recenti rapporti risulta che il sistema IT (Information Technology) è più soggetto ad attacchi rispetto al sistema OT (Operational Technology) che generalmente interessa l'industria 4.0

- Gli attacchi ai sistemi OT sono molto più limitati in quanto richiedono l'impiego di malware specializzati tipo Stuxnet, Triton, NotPetya, oltre che una esperienza specifica nel settore

- La notevole diffusione dei sistemi OT e dei relativi pericoli ha portato l'industria nucleare a modificare l'approccio alla problematica

3. I sistemi elettronici a matrici programmabili FPGA (Field Programmable Gate Array)

- L'esigenza di avere un sistema di controllo, allarme e blocco non hackerabile, ha portato ad abolire i sistemi operativi in alcuni settori critici quali aerospaziale, militare, nucleare

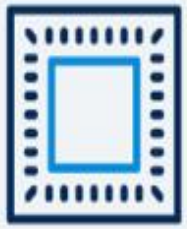
- L'assenza di un sistema operativo rende impossibile modifiche non autorizzate su sistemi già programmati

- L’impiego di circuiti elettronici a matrici programmabili FPGA non richiede alcun sistema operativo
- In molti casi non è necessario avere modifiche al sistema programmato inizialmente
- Il sistema programmato inizialmente FPGA non è modificabile e quindi non è necessario sistema operativo e relativa CPU
- Le principali differenze tra i sistemi con FPGA e quelli con CPU sono illustrate di seguito

FPGA

- Can only do what it is programmed to do – finite number of states
- Circuit can be extensively tested and validated
- FPGA configuration can only be updated through an independent data path
- Attacks often require physical access
- Difficult to find open source hacker tools because FPGA circuits are so customized

VS.



CPU

- Can be programmed to do anything – unlimited states
- Not practical to test every input/output combination
- Attack patterns are repeatable once successful
- Attacks can be done remotely
- Easy to find open source hacker tools with proven techniques – higher returns and quicker attack success

Circuiti a matrici FGPA

- Sono circuiti elettronici integrati programmabili in campo
- Possono eseguire solo ciò per cui sono stati programmati. Numero finito di stati
- I circuiti possono essere testati e validati estensivamente
- Le configurazioni dei circuiti possono essere aggiornate solo attraverso una apposita via dati

- Gli attacchi possono avvenire solo attraverso un accesso fisico al circuito
- Difficoltà a trovare strumenti di hackeraggio

Circuiti CPU

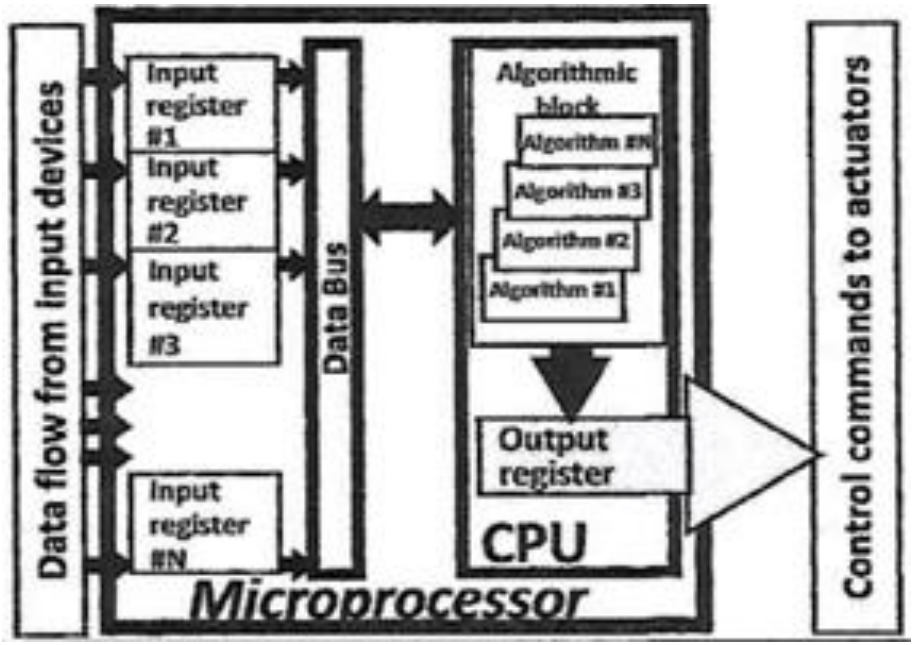
- Sono circuiti elettronici integrati con il sistema operativo
- Possono essere programmati per fare qualunque cosa. Numero illimitato di stati
- Non è praticamente possibile testare ogni combinazione input/output
- Le modalità di attacco sono ripetibili dopo un hackeraggio avvenuto con successo

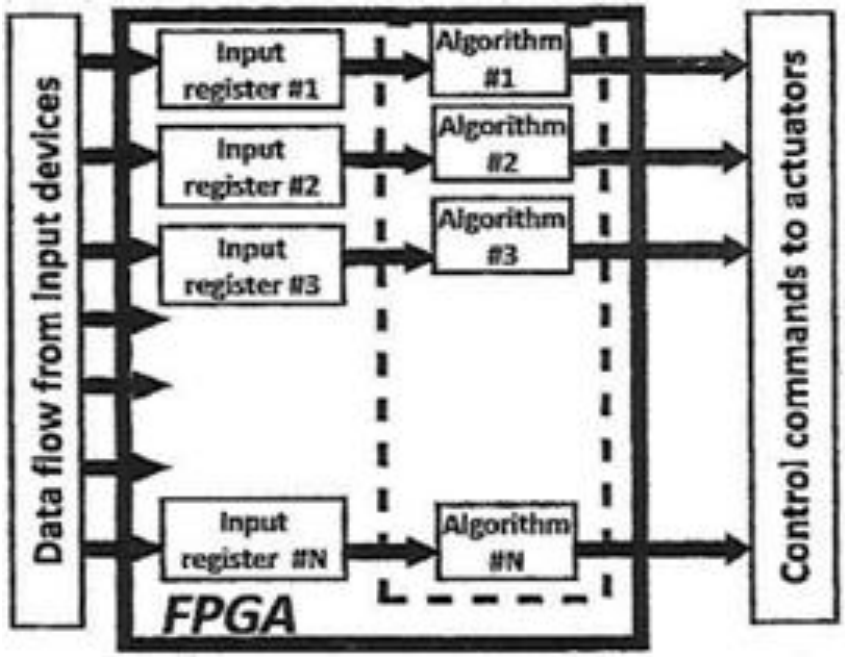
- Gli attacchi possono essere eseguiti da remoto
- Facilità a trovare strumenti di hackeraggio

Confronto CPU - FPGA

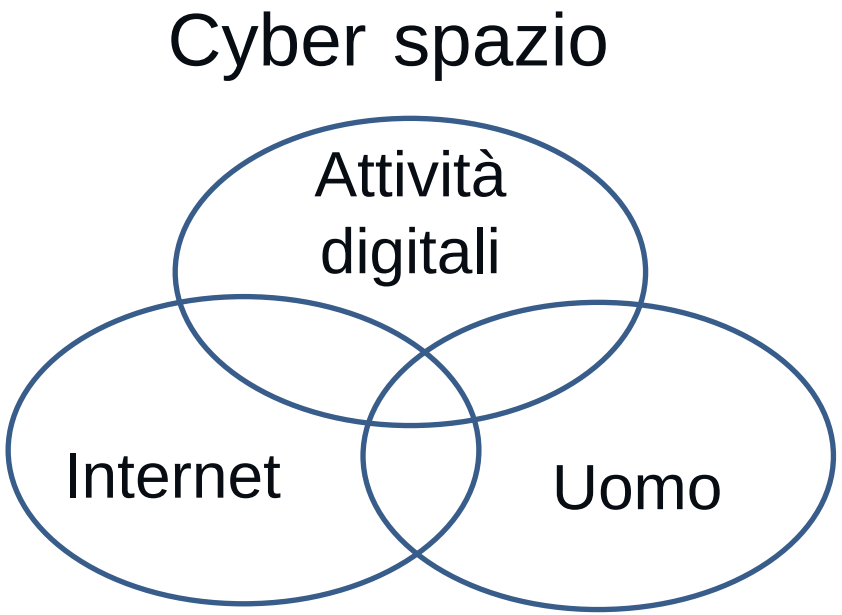
CPU, un microprocessore opera in modo seriale con sistema operativo

Un FPGA opera in parallelo ad alta velocità, senza software





4. Eliminazione del rischio cybersicurezza



- Attività digitali : SCADA, DCS, PLC , Telecom.
- Internet: provider, centro dati, rete telecom
- Uomo: operatori, persone

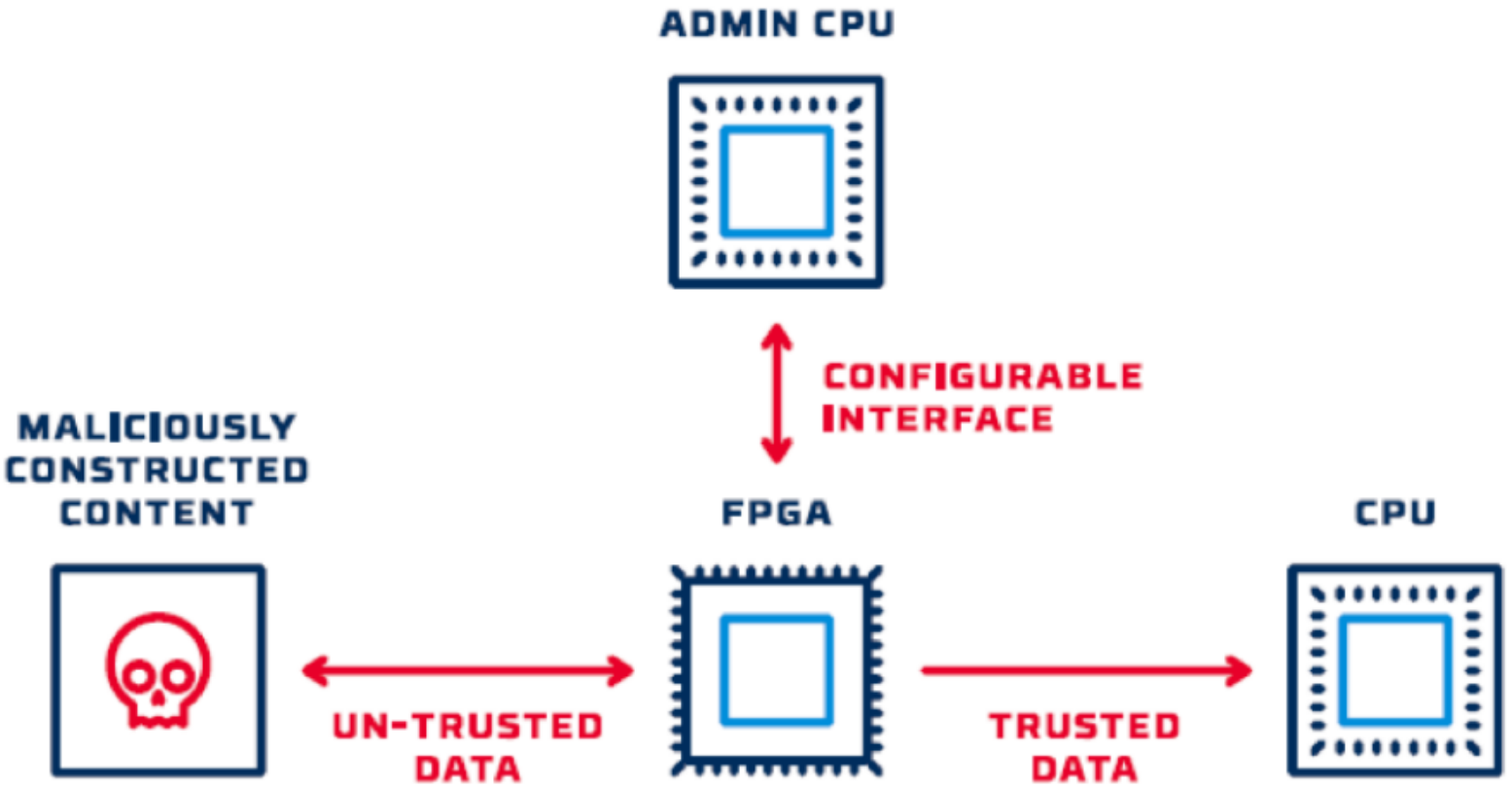
- Per eliminare il rischio cybersicurezza nelle attività digitali occorre che queste non abbiano un sistema operativo hackerabile, cioè CPU

- L’impiego di circuiti FPGA (senza CPU) nei sistemi SCADA, DCS, PLC, di installazioni critiche, rende questi ultimi non hackerabili

- Per quanto riguarda l'attuale situazione nel campo industriale 4.0, si prevede un impiego graduale dei circuiti FPGA per le nuove installazioni critiche, e nelle sostituzioni di quelle esistenti a fine del loro ciclo di vita

- I sistemi FPGA possono essere impiegati nei sistemi con CPU, per il controllo e la trasmissione dei dati protetti come indicato nella figura seguente

Impiego di sistemi FGPA nei CPU



- Una specifica applicazione, adeguatamente progettata, di filtro con FPGA, può assicurare che una vulnerabile CPU non riceva contenuti maliziosi

- Il livello di cybersicurezza con FPGA è largamente superiore a quello ottenibile con software based firewall

GRAZIE PER L'ATTENZIONE !