Un approccio totale per implementare la Cyber Security

Alessandro Bianco

ADVANTECH

Enabling an Intelligent Planet

Cosa si intende per Cyber Security?

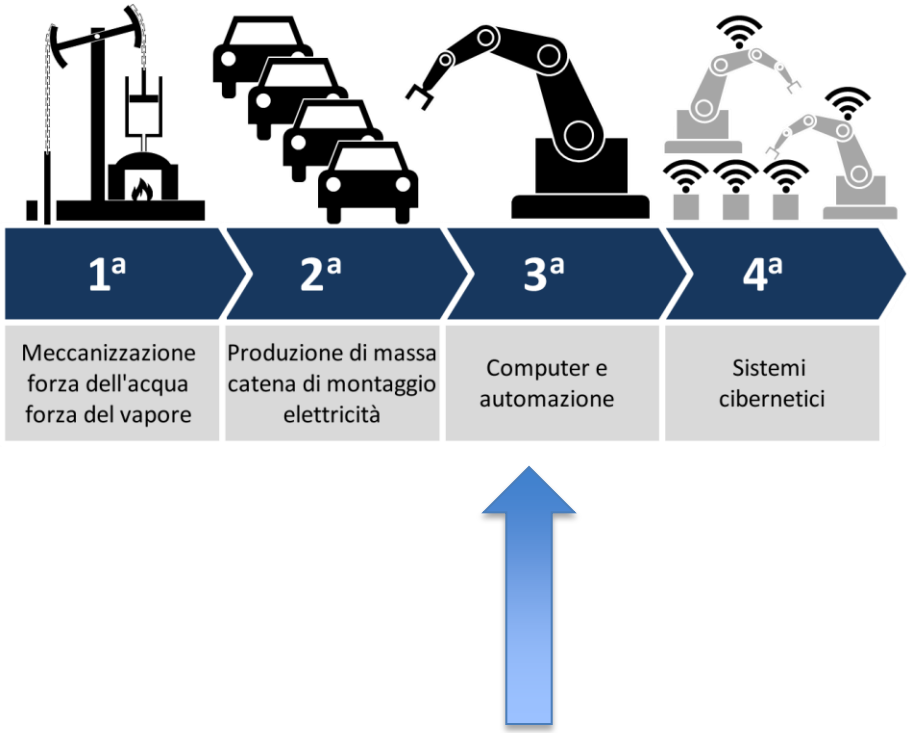
Per cybersecurity si intende quell'ambito dell'information security prettamente ed esclusivamente dipendente dalla tecnologia informatica. Nell'utilizzare il termine *cybersecurity* si vuole intendere, in particolare, un approccio mirato ad enfatizzare le *misure di prevenzione* e *misure di protezione*.

Furto delle informazioni

Alterazione dei processi produttivi

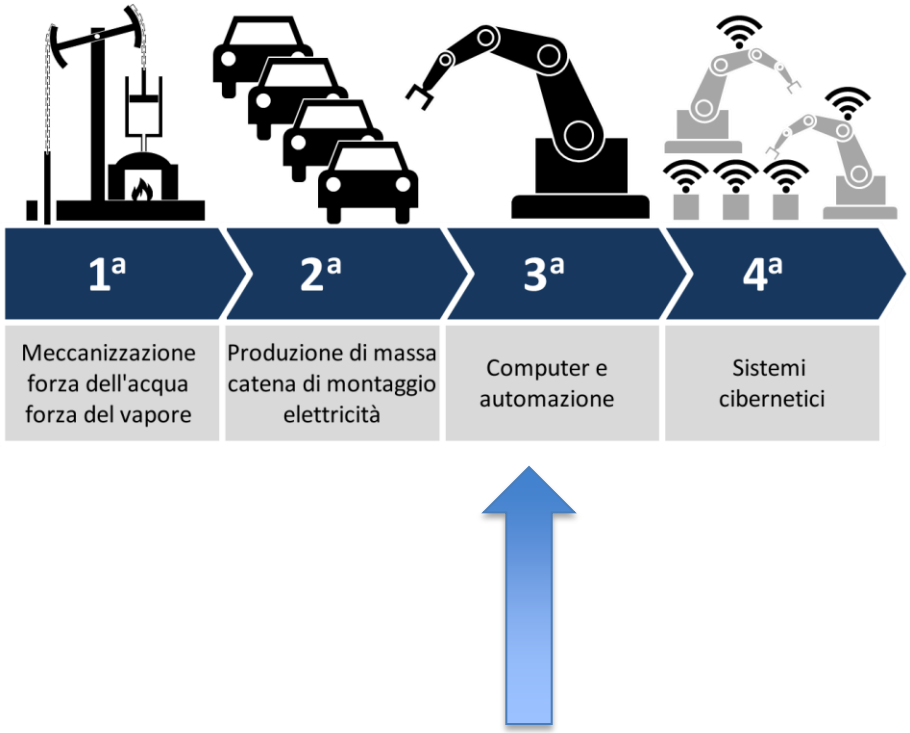
STOP dei processi produttivi

Cyber Security e Industry 4.0



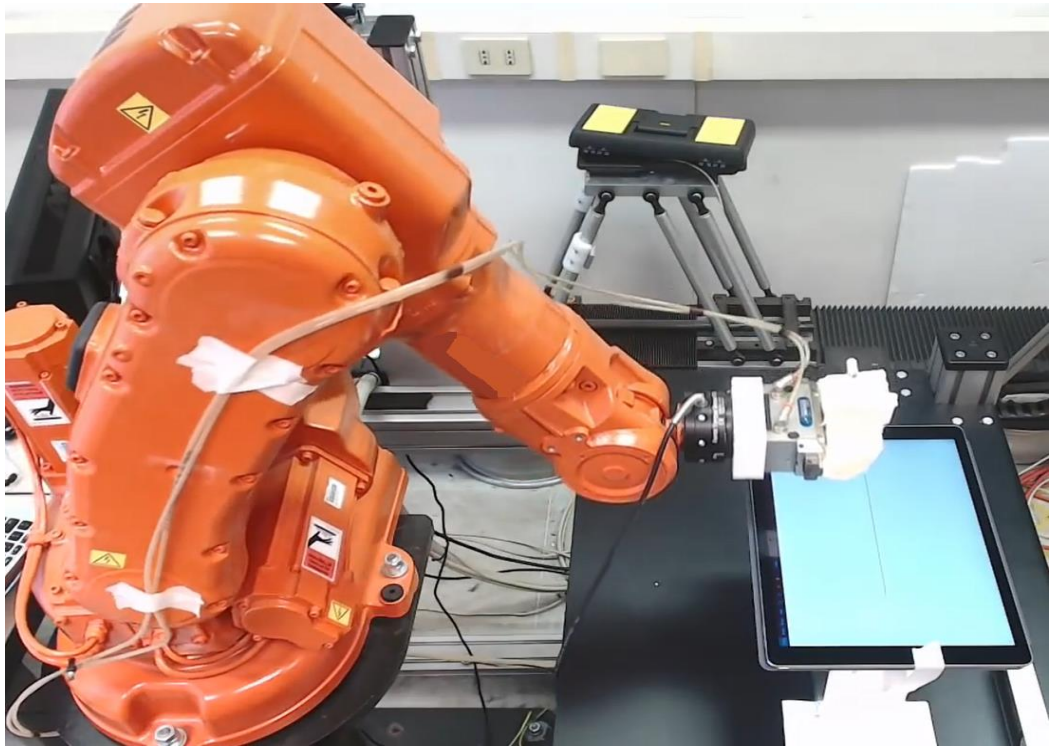
Già con la terza rivoluzione industriale, con l'introduzione di Computers ed Automazione, si fece sentire sempre di più l'esigenze di «Security» in quanto i dispositivi presenti in una fabbrica potevano essere attaccati con le stesse finalità mostrate prima

Cyber Security e Industry 4.0



L'interconnessione tra i sistemi fisici e quelli virtuali è alla basa della quarta rivoluzione industriale. Questa interconnessione e la convergenza tra OT e IT introducono un nuovo rischio: Cyber+Security. La natura interconnessa e la trasformazione digitale, elementi alla base del concetto di Industry 4.0, portano i cyberattacks ad avere effetti molto più estesi come mai prima. Aziende e loro fornitori potrebbero non essere preparate ai relativi rischi.

Cyber Security: quanto è importante?



Cyber Security: quanto è importante?

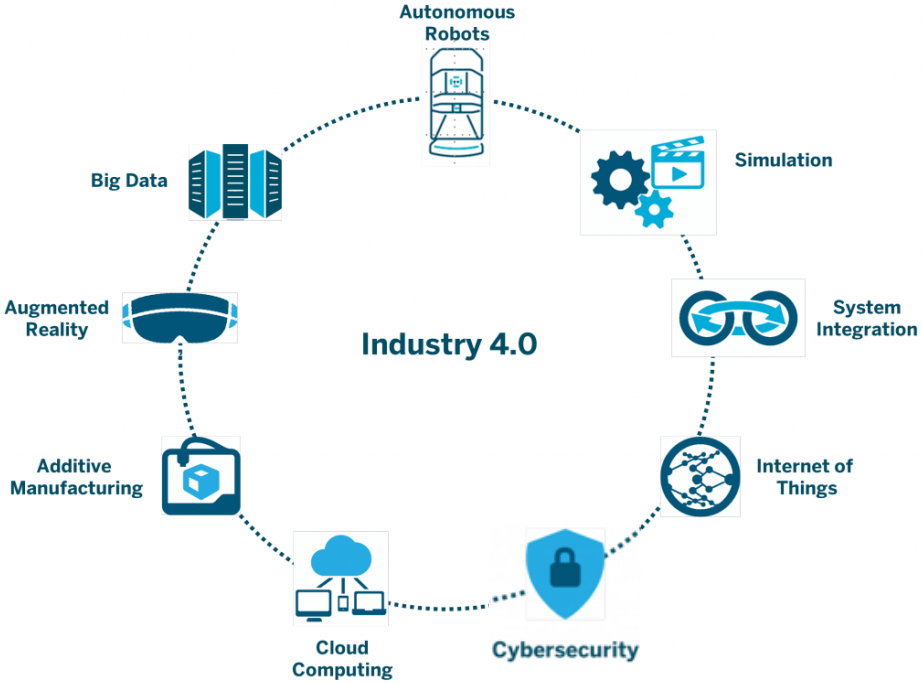
Cyber Security: quanto è importante?

Un minimo difetto (2mm) può comportare significative perdite economiche (e di immagine) per l'azienda produttrice per il richiamo dei droni «difettosi» e/o pagare per i danni causati.

Adesso immaginate cosa accadrebbe se i robot fossero in un contesto di produzione:

- Auto
- Aeroplani
- Cibo
- Medicine

Cyber Security e Industry 4.0

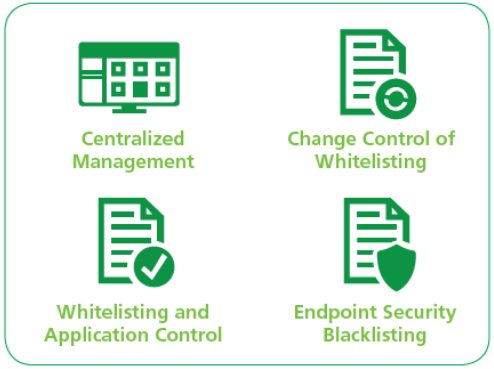


Uno dei 9 pilastri della quarta rivoluzione industriale è legato alla Cybersecurity.

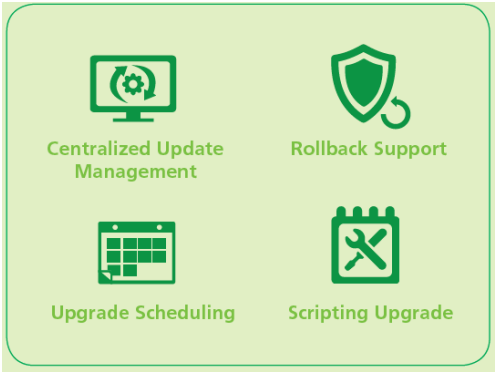
L'approccio alla Cybersecurity deve essere TOTALE:

Software + Hardware

Cyber Security: approccio software



McAfee



Over-the-Air Software Upgrade Management Services

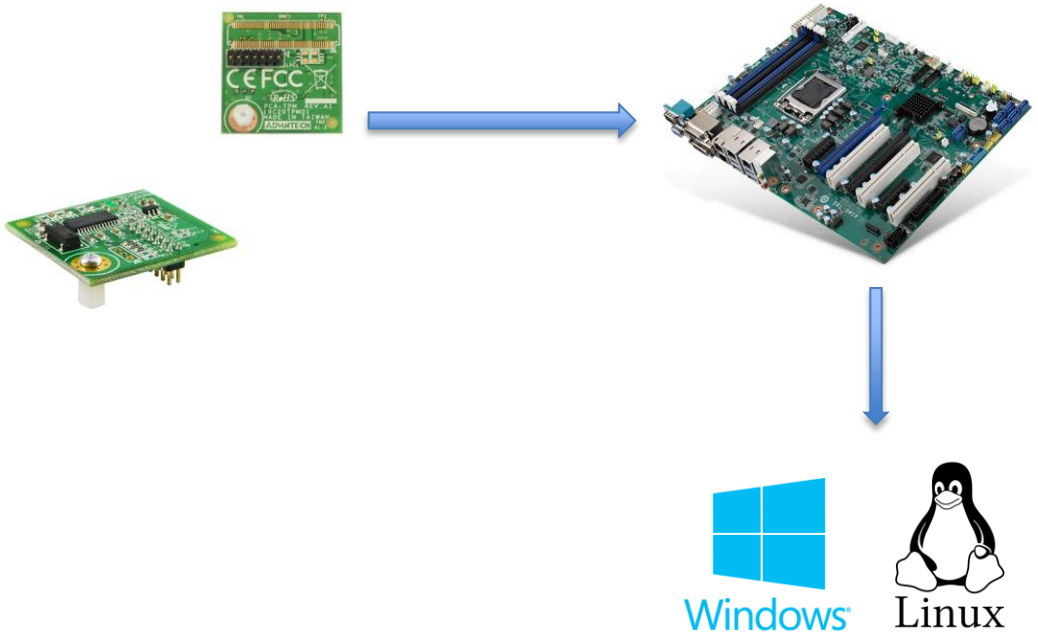
Le difese software contro i cyberattacks sono implementate attraverso l'utilizzo di specifici programmi che prevedono tra le varie funzioni:

- Centralized Management
- Whitelisting
- Blacklisting

Cyber Security: approccio software

Cyber Security: approccio hardware

La sicurezza a livello hardware viene affidata all'utilizzo di chipset TPM (*Trusted Platform Module*).



Cyber Security: approccio hardware

In che tipologia di hardware possiamo trovare la tecnologia TPM?

Fanless boxed PC

Rackmount IPC

HMI

Cyber Security: approccio hardware

Le specifiche pubblicate dal Trusted Computing Group definiscono quale dev'essere l'architettura del processore e quali funzionalità minime esso deve offrire.

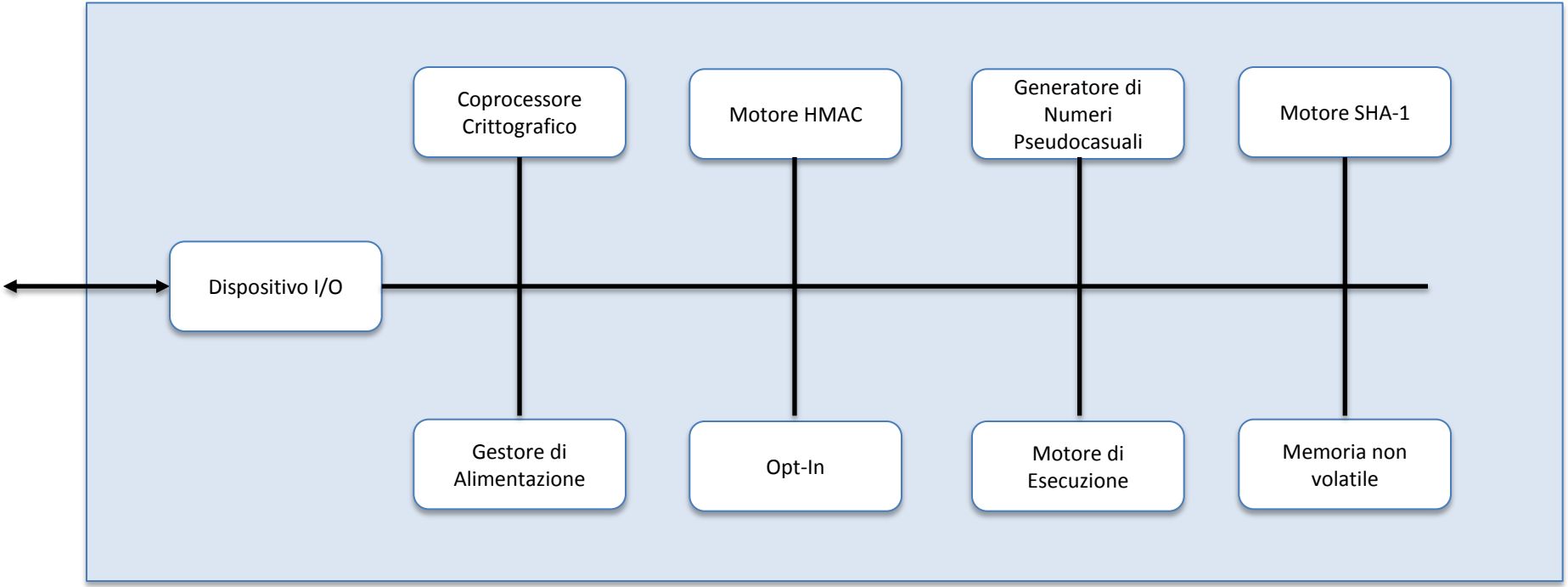
Ogni TPM deve offrire determinate minime funzioni, ovvero:

- generazione di numeri pseudo-casuali;
- generazione e memorizzazione di chiavi crittografiche (RSA);
- cifratura e decifratura di informazioni con RSA;
- generazione e verifica di hash SHA1.

A tale scopo, ogni TPM deve essere dotato di specifiche componenti, connesse tra loro attraverso un bus interno e capaci di interagire con il resto del calcolatore con un bus esterno. Tali componenti devono essere i seguenti:

Cyber Security: approccio hardware

Rappresentazione schematica di un TPM:



Cyber Security: approccio hardware

La sola tecnologia TPM è sufficiente a garantire un sistema protetto?

- Il BIOS lancia qualsiasi loader di S.O., compresi malware

- UEFI esegue, con l'apporto del TPM, esclusivamente loader di S.O. verificati (a partire da Win 8.1)
- NO Malware

Un approccio totale per implementare la Cyber Security

Fine

Grazie per l’attenzione

Alessandro Bianco