# Embedded World

n. 2 - aprile 2016

# La Sicurezza, forza propulsiva per le Fabbriche Intelligenti

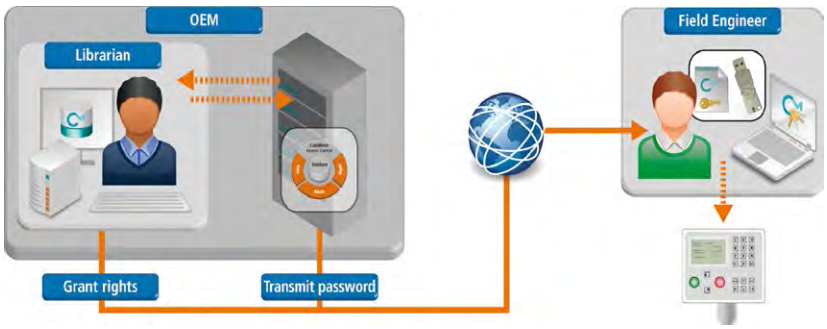
# Più sicurezza per le fabbriche intelligenti

**CodeMeter, una tecnologia di sicurezza sviluppata da Wibu-Systems, combina un potente motore crittografico per proteggere il codice del software, a una piattaforma di gestione licenze, a ulteriori meccanismi di sicurezza.**

Mentre negli Stati Uniti la Corte Federale ordina ad Apple di compromettere la sicurezza degli iPhone per avere accesso facilitato alle informazioni private degli utenti, nel mondo industriale la discussione prende la piega opposta e verte sul rafforzamento delle misure di sicurezza. Che l'Industrial Internet, le Fabbriche Intelligenti, i sistemi ciber-fisici costituiscano il fulcro su cui i governi scommettono per il rilancio dell'economia globale è un dato di fatto. Basti vedere il programma Horizon 2020, lanciato dalla Commissione Europea, che eroga 80 miliardi di euro per il finanziamento di progetti di ricerca e innovazione, atti a promuovere l'evoluzione del comparto industriale, delle comunicazioni, dell'informatica, della sicurezza, della scienza. In parallelo, i singoli Stati finanziano e sostengono le proprie imprese; è il caso, ad esempio, di IUNO, il progetto nazionale tedesco per la sicurezza nell'Industria 4.0, che riunisce 21 partner, tra comparto privato e accademico, accomunati da un unico scopo: individuare i rischi e le minacce cui le Fabbriche Intelligenti saranno oggetto in quattro aree applicative: la produzione personalizzata, il trattamento dei dati, l'assistenza remota e il monitoraggio dei processi. La promessa è dunque estremamente invitante: i sistemi di controllo che regolano l'erogazione energetica, i servizi sanitari, la produzione industriale, i trasporti e i servizi verranno portati in rete a formare grandi sistemi integrati, collegati con enti pubblici, privati e utenza. La mole impressionante di Big Data raccolti verrà analizzata in tempo reale e fornirà indicazioni preziose e istantanee per ottimizzare i processi decisionali e operativi. D'altro canto, ogni nuovo dispositivo che verrà aggiunto all'ecosistema IoT rappresenterà un veicolo di attacco, e ogni elemento umano rimosso costituirà un'opportunità per una violazione di sicurezza. Il rischio può essere ulteriormente esacerbato dall'insufficiente interoperabilità, portando nuovamente l'accento sul fattore sicurezza.


## Sicurezza per l'Industria 4.0

Per risultare efficaci, i sistemi dell'Internet Industriale delle Cose devono esprimere significativi incrementi nei livelli di prestazioni, scalabilità ed efficienza. Per una loro rapida e capillare distribuzione, gli IIoTS devono essere sostenuti da architetture comprensibili e facilmente applicabili, basate su standard aperti, orizzontali e interoperabili. L'architettura di riferimento per l'Internet Industriale, messa a punto dall'Industrial Internet Consortium, individua le seguenti aree su cui concentrarsi maggiormente:




CodeMeter protegge gli accessi fisici e logici dei manutentori

- la sicurezza fisica, espandendo i fondamenti contenuti nelle direttive Iso/Iec 61508;
- la sicurezza logica e la privacy;
- la resilienza, prendendo spunto da programmi militari;
- la capacità di integrazione e interoperabilità;
- la connettività di sensori, controllori, dispositive, macchine e sistemi;
- la gestione dei dati, in termini di archiviazione e scambio;
- l'esame analitico avanzato dei dati;
- il controllo intelligente e resiliente dei processi;
- il ricombinamento dinamico per un adattamento automatico del sistema.

Attualmente i sistemi di controllo industriale sono prevalentemente isolati e provengono da fornitori eterogenei, che utilizzano sistemi proprietari dotati di livelli variabili di sicurezza. In definitiva, un'infrastruttura vulnerabile, che non può garantire uno scudo a sabotaggi, manomissioni e attacchi informatici che si stanno intensificando ed evolvendo all'interno di un cyber-terrorismo professionale.

## Alleanze e paradigmi all'insegna della sicurezza

Una visione olistica porta, in prima battuta, a concentrarsi sulla sicurezza degli endpoint, delle comunicazioni tra di essi, dei meccanismi di gestione di endpoint e comunicazioni, dell'elaborazione e memorizzazione dei dati. Mentre il dibattito tra sicurezza "by design" e "by default" rimane acceso, prendono forma nuovi accordi tra gli specialisti It e le aziende più rappresentative dell'industria, che mirano a integrare gli elementi di sicurezza direttamente nelle piattaforme software e negli elementi hardware dell'IIoT. Di seguito alcuni esempi:

- **VxWorks** è facilmente definibile il sistema operativo real-time più utilizzato al mondo. A partire dalla versione 7, **Wind River** ha introdotto una serie di profili per incontrare le esigenze del mercato. Il Profilo di Sicurezza include funzioni native per la protezione del software, quali il caricamento sicuro della runtime, la sicurezza della rete, la gestione avanzata degli utenti, il boot sicuro e i contenitori dati crittografati.
- **Kontron**, pilastro dell'embedded computing technology, è appena scesa in campo per integrare un Asic di sicurezza su tutti i propri sistemi (schede, gateway e moduli) in modo da renderli pronti per l'Internet delle Cose.
- **Infineon** ha puntato sulla sicurezza sia nel campo dei Trusted Platform Module, sia dei microcontrollori. Nel primo caso, rilancia il ruolo dei TPM, in alternativa ai loro stessi chip smart card, come elemento hardware sicuro cui associare le chiavi crittografiche di licenza del software. Nel secondo caso, la vulnerabilità identificata si riferisce ai processi di aggiornamento del firmware dei microcontrollori; un diverso comportamento volutamente iniettato nel codice di un sistema di controllo è costoso, dannoso e potenzialmente letale.
- Nel mondo PLC, l'ambiente di sviluppo **Codesys** prevede la possibilità di salvare le licenze protette dell'applicativo, sviluppato in un contenitore hardware sicuro. Le licenze software rimangono così salvaguardate da pirateria e reverse engineering.
- **Rockwell Automation** ha posto l'accento su una ulteriore criticità: la componente umana, da individuarsi nella figura del manutentore. Una volta verificatene le credenziali, egli dovrà avere accesso esclusivamente alla manualistica e alle risorse specifiche per l'impianto per il quale è richiesto l'intervento, e per il solo tempo necessario a eseguire le operazioni di manutenzione.

## Una tecnologia di sicurezza

Il minimo comun denominatore di queste soluzioni è **CodeMeter**, una tecnologia di sicurezza sviluppata da **Wibu-Systems**, che combina un potente motore crittografico per proteggere il codice del software, a una piattaforma di gestione licenze che ne facilita la creazione, la distribuzione e il monitoraggio, a ulteriori meccanismi di sicurezza, quali il boot sicuro e il concatenamento di validità dei certificati digitali. Che il software venga sviluppato per computer tradizionale o industriale, dispositivo mobile, sistema embedded, PLC, microcontrollore o persino FPGA, CodeMeter ha una risposta adeguata ai requisiti tecnici del sistema, che non scende a compromessi con la sicurezza contro spionaggio industriale, manomissioni e cyber terrorismo. Inoltre, il licenziamento del software, offre nuove opportunità di ridisegnare i modelli di business anche in ambito industriale e offrire app store e concetti di post-vendita evoluti. L'Europa ha grandi ambizioni che gravitano intorno all'Industria 4.0: il mercato digitale unico, il pacchetto per l'unione energetica, l'economia circolare, l'unione dei mercati capitali, il fondo europeo per gli investimenti strategici e la strategia per un mercato interno potranno decollare e dare i loro frutti, nel momento in cui le innovazioni tecnologiche verranno favorite e adottate, nuove specializzazioni per la forza lavoro presente e futura verranno messe a punto e promosse, e la sicurezza digitale sarà pervasiva.

**Wibu-Systems**
www.wibu.com