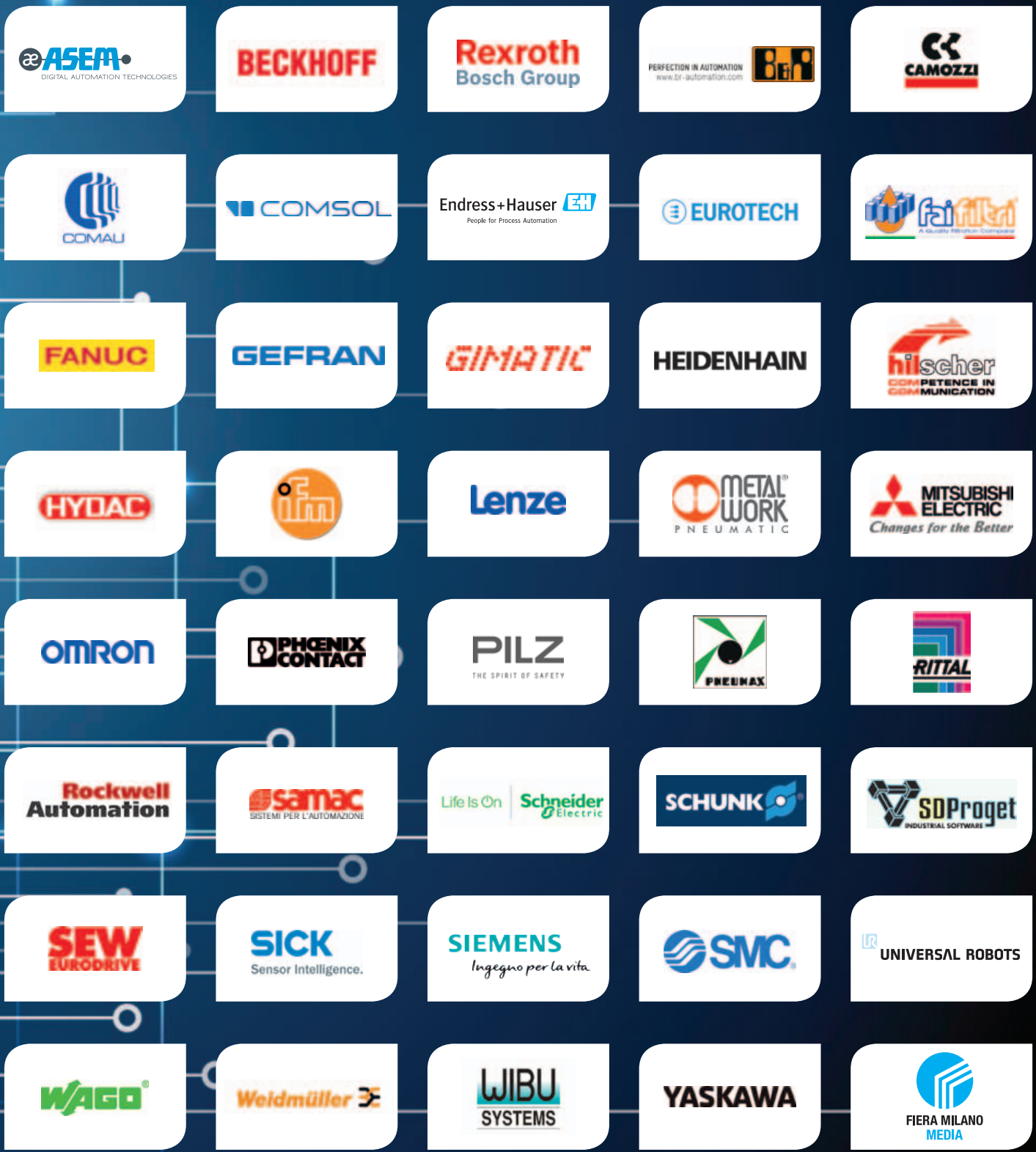
Dicembre 2016

ITALIA 4.0

TECNOLOGIE PER LO SMART MANUFACTURING



Supplemento a RPO 200 novembre/dicembre 2016

Wibu-Systems

Tra il 2004 e il 2014 i costi di produzione sono incrementati nella maggior parte dei primi 25 Paesi esportatori di tutto il mondo, ivi incluse Russia e Cina. Al contempo, l'aumento della potenza di calcolo, la pervasività della connettività, e tecniche avanzate di analisi dei dati hanno portato a una convergenza dell'OT (tecnologia operativa e di controllo) con l'IT (tecnologia informatica ed Internet). Questa integrazione può effettivamente rimettere in gioco fattori quali produttività, efficienza e prestazioni dei processi operativi esistenti.

Nonostante lo spiccato accento sugli aspetti tecnologici, le ragioni che hanno innescato la rivoluzione dell'industria 4.0 hanno carattere commerciale e sono dettate da scelte strategiche per il raggiungimento di una gestione intelligente della catena di approvvigionamento, una diminuzione del total cost of ownership, una riqualificazione del fattore umano, un'ottimizzazione della superficie produttiva, un minore impatto ambientale, e, in definitiva, un aumento dei profitti.

CodeMeter Embedded è ora integrato negli SDK per OPC UA di Unified Automation ed arricchisce le funzionalità native di sicurezza dello standard OPC UA.

Detlef Zuehlke, AD di SmartFactoryKL, e Oliver Winzenried, AD e fondatore di Wibu-Systems, all'inaugurazione del prototipo della linea di produzione creata in base ai principi dell'Industria 4.0.

Il fattore sicurezza

Per raggiungere questi obiettivi ambiziosi e agevolare la transizione da un modello che vedeva la collaborazione diretta tra produttore delle macchine e produttore delle merci, a uno in cui si inserisce tra i due un elemento critico ma controllato dall'esterno - la produzione as a service, l'intera struttura deve essere messa in discussione, e con essa i meccanismi di comunicazione, autenticazione e sicurezza.

Se da un lato sarebbe preferibile optare per standard aperti per consentire l'interoperabilità tra un più ampio spettro di macchine, dall'altro la loro sicurezza deve essere resa ancora più efficace. Questo è, ad esempio, il caso di OPC UA, uno standard multipiattaforma che sta trovando ampia diffusione nel mondo dell'automazione. La memorizzazione delle chiavi crittografiche e dei file di configurazione sensibili nel file system di OPC UA li espone al furto e alla manomissione. Gli SDK per OPC UA di Unified Automation, in cui è stata integrata la tecnologia di protezione CodeMeter Embedded di Wibu-Systems, salvaguardano le informazioni confidenziali in un elemento di sicurezza hardware, cruciale per un livello di protezione più elevato.

L'importanza di firmware e software

Un altro fattore di instabilità del sistema sono gli aggiornamenti di firmware e software. Un numero sempre maggiore di sistemi nei mercati professionale e consumer è gestito da microcontrollori, i quali fanno uso di algoritmi sofisticati e necessitano di aggiornamenti. I vendor si trovano dunque ad affrontare una doppia minaccia: la contraffazione del know-how di prodotto e un ambiente insicuro regolato dall'imprevedibilità dell'utente finale. Utilizzando microcontrollori con tecnologie di sicurezza integrate (come nel caso della famiglia XMC4500 di Infineon protetta da CodeMeter µEmbedded di Wibu-Systems), i produttori di dispositivi intelligenti proteggono la loro proprietà intellettuale, garantiscono la genuinità dell'aggiornamento agli utenti finali e possono ulteriormente implementare modelli di vendita delle licenze basati sulle funzionalità attivate dal cliente, esattamente come siamo abituati nel mondo delle app per i nostri smartphone.

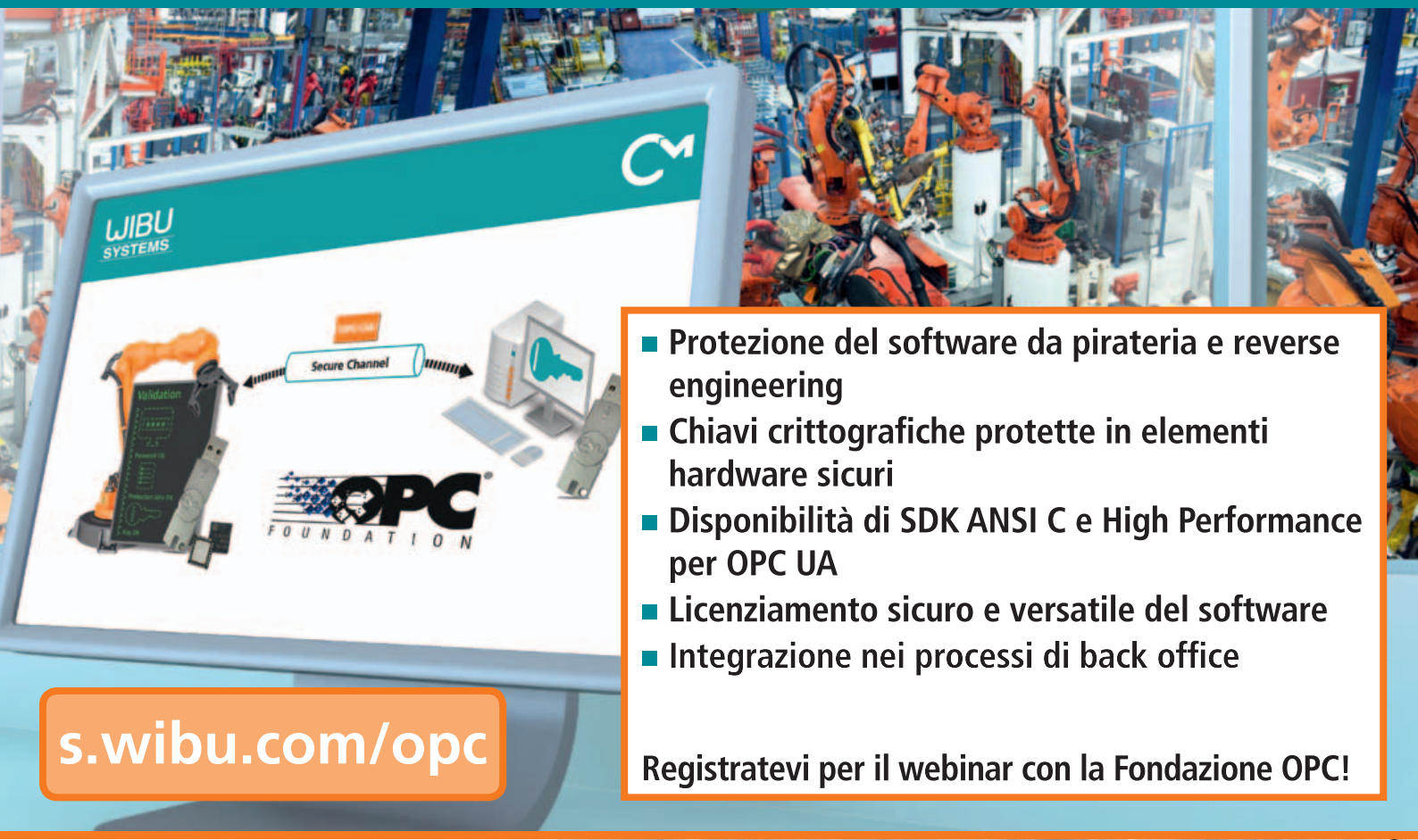
Nell'inversione di ruoli che l'Industria 4.0 promuove, l'utente finale diventa infatti il vero artefice dei propri prodotti. Anche da questo punto di vista, il rischio è abbastanza chiaro: la contraffazione-as-a-Service è la prossima frontiera dei crimini informatici. Un'implementazione della sicurezza by-design, come quella che ha adottato Kontron, dotando tutte le proprie schede di nuova generazione di CmASIC, un asic di sicurezza sviluppato da Wibu-Systems, mette al riparo la proprietà intellettuale di Kontron stessa e dei suoi clienti da attacchi informatici.

Wibu-Systems AG

Rueppurrer Strasse, 52-54 - 76137 Karlsruhe (Germania)
Tel. +39 035 0667070
team@wibu.com
www.wibu.com

CodeMeter®: Estensione di Sicurezza per lo Standard OPC UA

WIBU SYSTEMS



- Protezione del software da pirateria e reverse engineering
- Chiavi crittografiche protette in elementi hardware sicuri
- Disponibilità di SDK ANSI C e High Performance per OPC UA
- Licenziamento sicuro e versatile del software
- Integrazione nei processi di back office

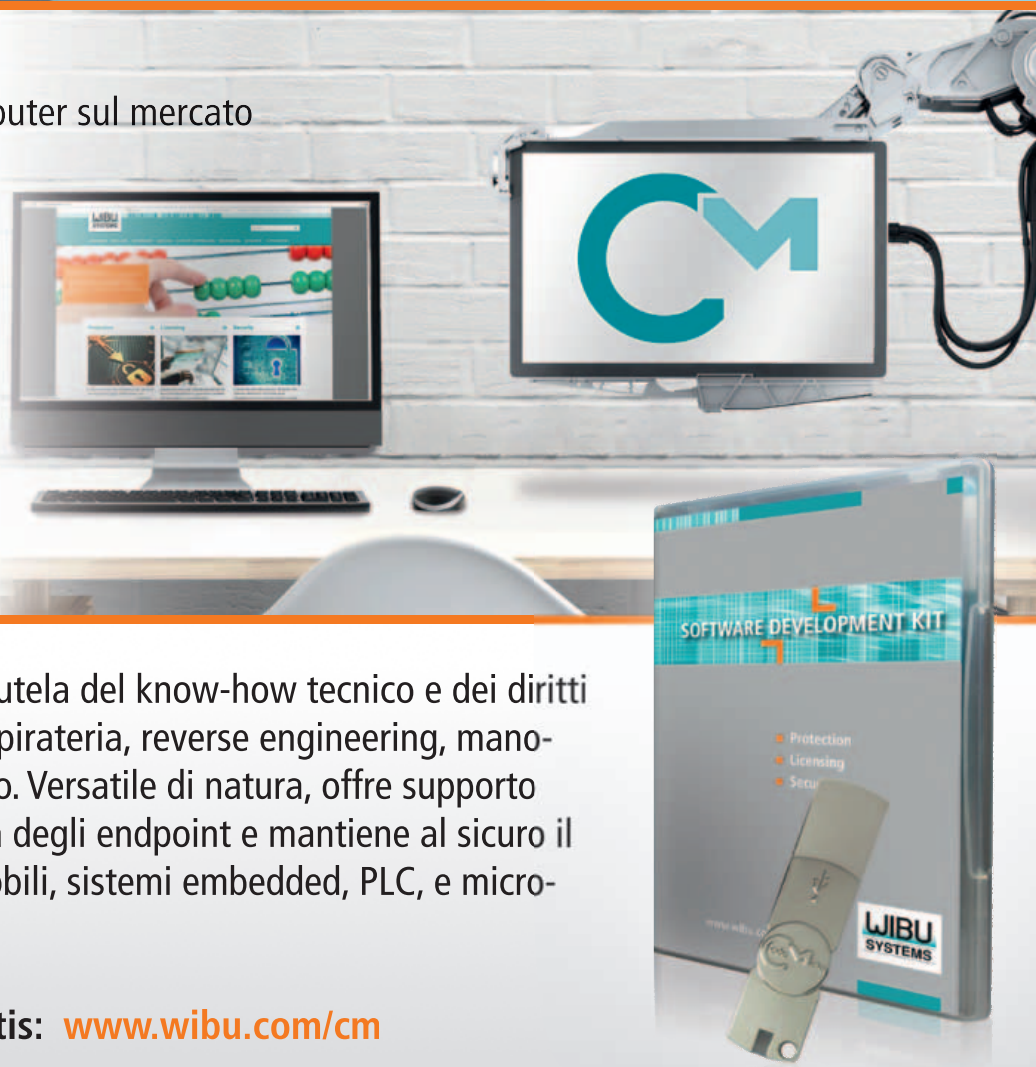
Registratevi per il webinar con la Fondazione OPC!

s.wibu.com/opc

40 anni fa apparvero i primi computer sul mercato
Oggigiorno, disponiamo di

- Molteplici piattaforme
- Dispositivi intelligenti
- Tecnologie mobile
- Internet delle Cose
- Industria 4.0

E siamo esponenzialmente esposti ad attacchi informatici.



CodeMeter è la soluzione per la tutela del know-how tecnico e dei diritti dei produttori di software contro pirateria, reverse engineering, manomissioni, sabotaggio, e spionaggio. Versatile di natura, offre supporto multi-piattaforma per la sicurezza degli endpoint e mantiene al sicuro il codice di computer, dispositivi mobili, sistemi embedded, PLC, e microcontrollori da atti predatori.

Richiedi adesso il tuo SDK gratis: www.wibu.com/cm