a cura di Ilaria De Poli @depoli_ilaria

RASSEGNA

Sicurezza hardware e software in fabbrica

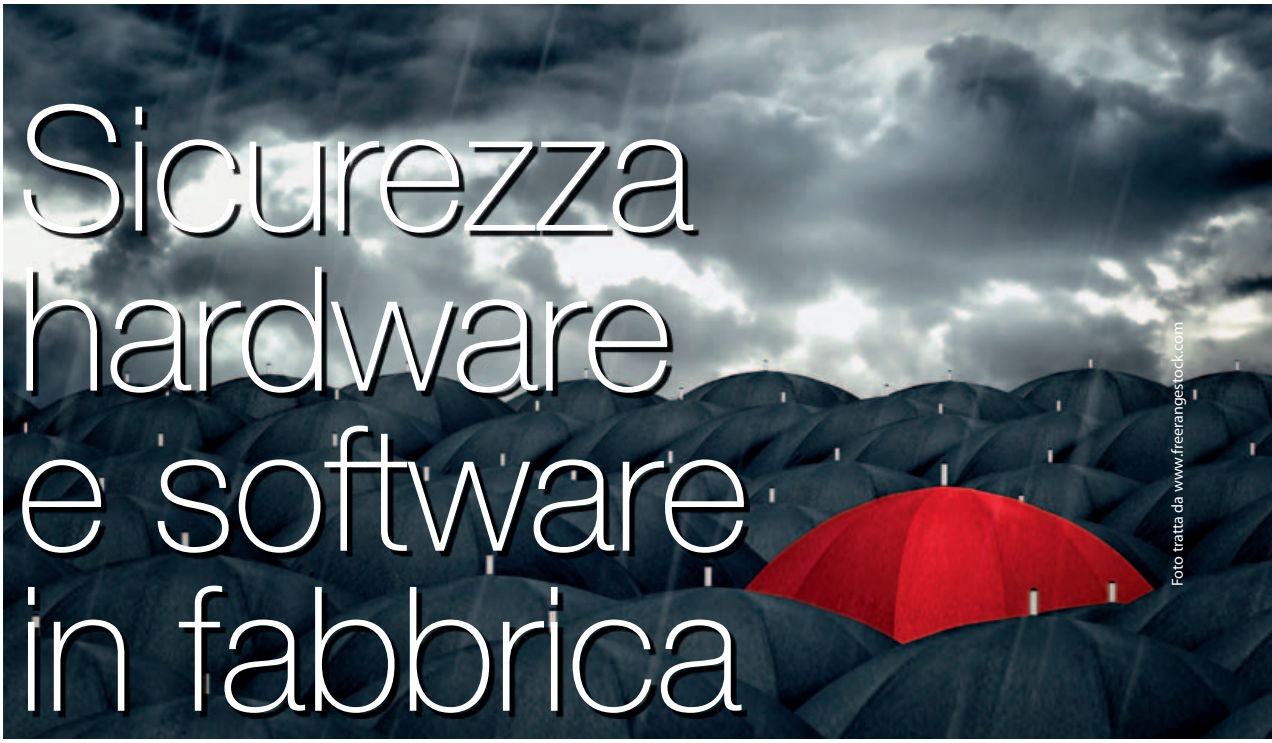


Foto tratta da www.freerangestock.com

Mercato, sistemi industriali e strategie di difesa: se da un lato l'ambito operativo aziendale diventa sempre più interconnesso e diffuso, dall'altro è d'obbligo implementare adeguate strategie di information security, nonché proteggere operatori e investimenti

Il mercato dell'information security in Italia è cresciuto dell'11% nel 2019 per il terzo anno consecutivo, raggiungendo un valore di 1,3 miliardi di euro secondo l'edizione 2019-2020 dell'Osservatorio Information Security & Privacy della School of Management del Politecnico di Milano. I risultati confermano che la disponibilità di tecnologie innovative come l'intelligenza artificiale, la spinta normativa e la crescita degli investimenti promuovono la domanda di competenze e la ricerca di nuovi profili dedicati alla sicurezza come security analyst, security architect e security engineer. La cybersecurity diventa quindi sempre più importante per l'affidabilità dei moderni processi industriali.

In ambito industriale, l'interconnessione di sistemi e la maggiore diffusione di dispositivi IoT stanno aumentando la vulnerabilità alle minacce informatiche degli ambienti OT (Operational Technology). I componenti dei tradizionali sistemi industriali di controllo (ICS), come sistemi di controllo di supervisione e acquisizione dati (Scada), sistemi di controllo distribuito (DCS) e controllori a logica programmabile (PLC), inizialmente isolati e basati su protocolli proprietari, con hardware e software dedicato e non connessi in rete, sono progressivamente sostituiti da dispositivi IP ad ampia diffusione e a basso costo, che aumentano la vulnerabilità. I moderni sistemi ICS si basano su soluzioni IT per la connettività ai sistemi aziendali e l'accesso remoto e sono progettati e implementati utilizzando PC, sistemi operativi e protocolli di rete standard. Questa integrazione aumenta le funzionalità IT ma riduce significativamente l'isolamento di questi sistemi dal mondo esterno, esponendoli a nuovi rischi. Richiede quindi misure di protezione dedicate. Un sistema industriale ha un impatto diretto sul mondo fisico e può mettere a serio rischio la salute e la sicurezza delle persone, causare gravi danni all'ambiente o determinare importanti conseguenze finanziarie in termini di perdita di produttività, impatto negativo sull'economia nazionale e compromettere informazioni proprietarie. Un programma di cybersecurity efficace deve gestire la sicurezza durante tutto il ciclo di vita del sistema, applicando strategie di difesa in grado di minimizzare l'impatto delle minacce informatiche.

Una strategia di difesa 'in profondità' deve prevedere tra i suoi obiettivi: lo sviluppo di politiche, procedure e formazione sulla sicurezza; l'implementazione di una topologia di rete a più livelli per proteggere le comunicazioni più critiche; una separazione logica tra le reti aziendali e di fabbrica con firewall e gateway; la limitazione dell'accesso fisico alle reti ICS e ai dispositivi; infine, il controllo degli accessi in base al ruolo funzionale. Deve prevedere inoltre la ridondanza dei componenti critici e la progettazione di sistemi in grado di rilevare e contenere gli incidenti, nonché soluzioni di ripristino. Importante è anche l'utilizzo di controlli di sicurezza come software di rilevamento delle intrusioni, antivirus e soluzioni di verifica dell'integrità dei file, e la gestione continua delle patch di sicurezza (fonte Nist-National institute of standards and technology). Un programma di sicurezza informatica industriale efficace deve infine essere affidato a un team interfunzionale per poter raggiungere gli obiettivi della strategia.

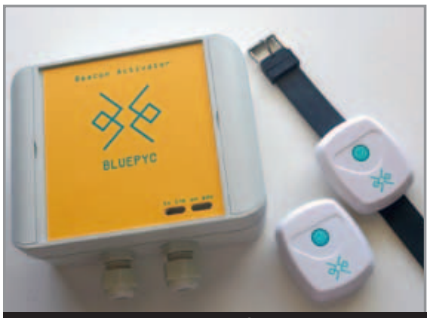
Cristina Paveri

un'intera applicazione di safety tra più dispositivi I/O intelligenti consente l'implementazione flessibile di architetture sempre più modulari, che possono essere adattate ai requisiti di sistema in maniera più efficace. La sinergica modularità del sistema TwinSafe semplifica l'implementazione di applicazioni di sicurezza anche molto complesse. La combinazione degli I/O e delle funzionalità di controllo TwinSafe in un singolo componente I/O semplifica la distribuzione dei compiti relativi alla safety tra le diverse parti della macchina, riducendo così i costi dell'hardware. In termini di engineering la funzione di customizzazione accelera il processo di sviluppo e lo rende più conveniente. Assicura inoltre un minimo sforzo in fase di validazione, che a sua volta riduce ulteriormente i costi di sviluppo.

www.beckhoff.it

BLUEPYC

Il sistema ibrido Beacon Wake-up & Activator, proposto da BluEpyc (Gruppo Softwork), mixa due tecnologie per perfezionare la capacità del protocollo BLE-Bluetooh Low Energy di rilevare in modo preciso la presenza di oggetti e persone in un'area indoor.



BLUEPYC

Il dispositivo Activator emette un apposito segnale radio, generando una bolla tridimensionale con un raggio settabile tra 0,6 m e 3,5 m; entrando in questo campo radio, lo speciale Beacon Wake-up (normalmente in deep-sleep, quindi con bassissimo consumo energetico della batteria) si risveglia e trasmette il segnale in BLE all'EchoBeacon o al Gateway in ascolto. Poiché il data-set di questo advertising contiene l'identificativo non solo del Beacon (chi sono?), ma anche dell'Activator che l'ha risvegliato (dove sono?), il risultato è un sistema per l'identificazione univoca, la tracciabilità automatica e la localizzazione precisa (presenza) di persone e/o oggetti, il tutto in modalità wireless (senza cablaggio) e su release 5.1 dello standard BLE. Altra nota distintiva del sistema è l'edge computing: spostando parte dell'intelligenza verso la periferia della rete, i Big Data sono filtrati ed elaborati in modo più efficiente e proattivo.

www.bluepyc.com

BOSCH REXROTH

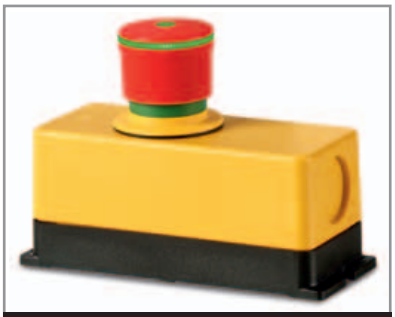
Potente, sicuro e affidabile, SafeLogic di Bosch Rexroth si programma liberamente ed è adatto a macchine e sistemi interconnessi. Si tratta di un PLC di sicurezza integrato e programmabile attraverso la piattaforma IndraWorks, per un numero esteso di periferiche di sicurezza. La soluzione estende dunque i controlli standard raggiungendo diversi livelli di sicurezza, conformi ai maggiori requisiti internazionali, quali Cat.4, PL e, SIL3, IEC62061 e ISO13849. Inoltre, SafeLogic è una scheda plug in facile da collegare ai controlli Rexroth per renderli sicuri. Tramite SafeLogic è possibile supportare una logica multi-master, per esempio CIP Safety on Sercos e Profisafe on Profinet. Infine, la soluzione si integra rapidamente con la piattaforma IndraDrive e SafeMotion.


BOSCH REXROTH

www.boschrexroth.it - expertise.bosch.it

EATON

La serie di pulsanti per arresto e interruzione di emergenza Small E-Stop di Eaton presenta una custodia flat in versione con sblocco 'a ruotare' o 'a tirare'; è disponibile anche in versione luminosa, con LED bicolore verde/rosso, e con due contatti che, a scelta, possono essere 2NC oppure 1NC+1NA. Progettati specificatamente per rispondere all'esigenza di progettisti e costruttori di macchine di risparmiare spazio, gli Small E-Stop si contraddistinguono per un ingombro inferiore del 30% rispetto ai pulsanti di emergenza standard. Nonostante le dimensioni ridotte, questi pulsanti di emergenza offrono gli stessi parametri di sicurezza di quelli standard e soddisfano pienamente i requisiti imposti dalle normative internazionali. Inoltre, i dispositivi offrono un grado di protezione IP66/67/69 e sono facili da installare e utilizzare in tutte le condizioni ambientali. Anche la custodia compatta, flat-enclosure, contribuisce alla riduzione degli ingombri e al miglioramento dell'aspetto estetico dell'equipaggiamento di macchina. Infine, gli Small E-Stop sono idonei al fissaggio sul profilato industriale in alluminio standard 40x40 mm.


EATON

www.eaton.it

ENDIAN

Si prevede che in un futuro prossimo le fabbriche intelligenti si trasformeranno in un articolato 'social network' in cui macchine, persone e risorse comunicheranno e interagiranno globalmente, connessi al resto del sistema logistico-produttivo e ai clienti tramite piattaforme cloud. I dati a disposizione saranno sfruttati per il miglioramento della capacità produttiva, l'efficienza e la sicurezza. Interconnessione sicura di utenti e macchinari, edge computing, containerizzazione dei servizi, monitoring e data analytics: tutto questo e molto altro è ciò di cui è capace la Secure Digital Platform di Endian, la soluzione completa e definitiva per l'IIoT e la smart

ENDIAN