INFORMATION SECURITY IN CAMPO

UNA TAVOLA ROTONDA ORGANIZZATA DA ROCKWELL AUTOMATION HA FATTO IL PUNTO SUL TEMA DELLA SICUREZZA DELLE RETI IN AMBITO MANUFACTURING: UN MONDO VARIEGATO DOVE LA SECURITY È DESTINATA AD ASSUMERE UN RUOLO IMPORTANTE

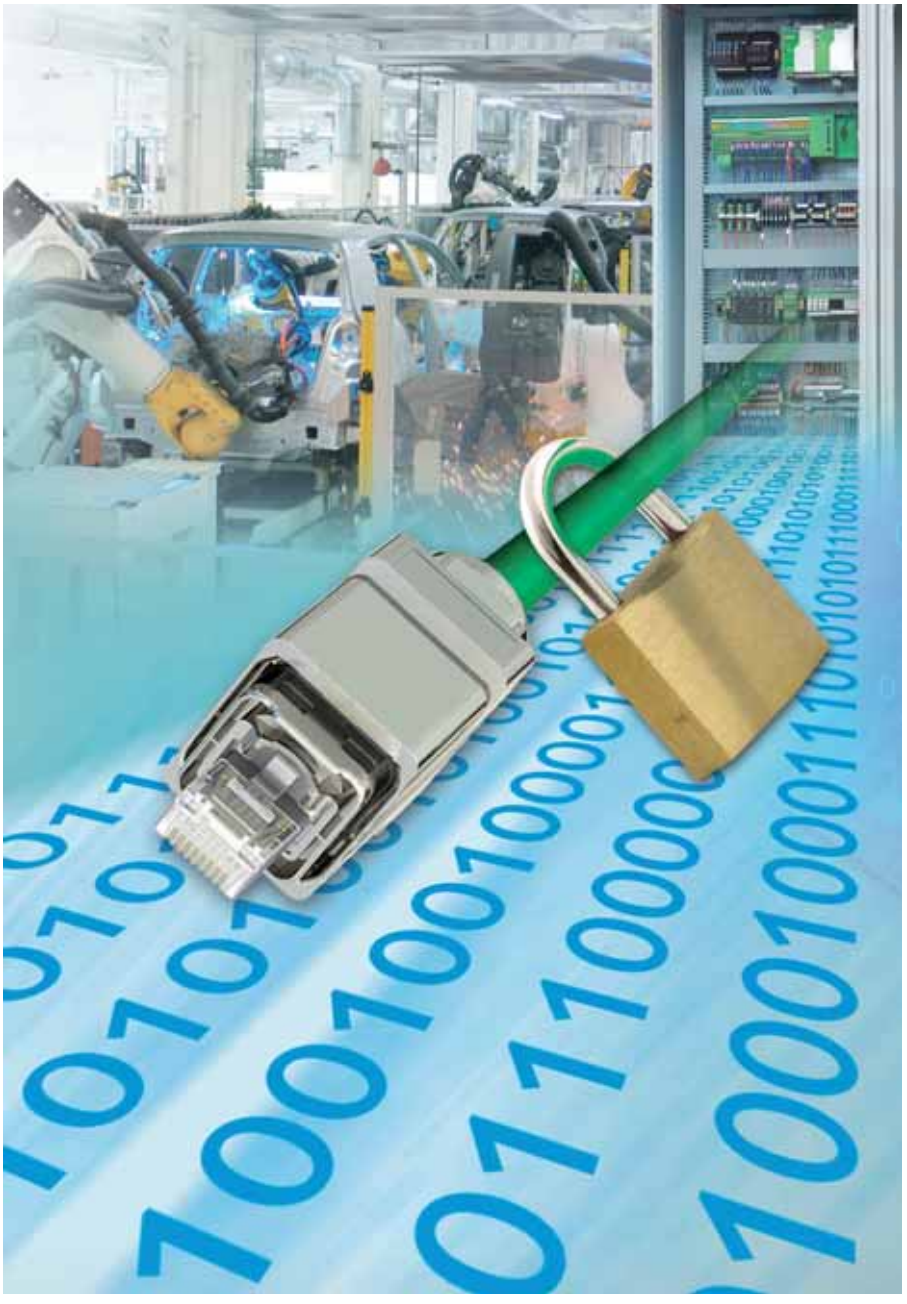
***di* Ilaria De Poli**

A lla fine di marzo si è tenuto a Milano l'evento 'Automation University', organizzato da Rockwell Automation al MIC - Milano Convention Centre, aggregando 600 fra tecnici, manager e partner in cerca di soluzioni di automazione, controllo e IT per il manufacturing in grado di aumentare la produttività e la sostenibilità degli impianti. Delle 100 sessioni di presentazione, dimostrazione e laboratorio, gli eventi e le tavole rotonde dedicate al management, che si sono susseguite nel corso della giornata, quelle legate alla sicurezza hanno forse riscosso il successo maggiore, confermando l'attesa del mercato per soluzioni che vadano in questo senso e la 'fame' di conoscenza del pubblico.

In particolare, il tema della sicurezza dei dati è stato affrontato, insieme ad altri, durante la tavola rotonda dedicata a "Risk assessment, tracciabilità e information security - le sfide nell'odierno scenario manifatturiero", moderata da Eugenio Alessandria di Ferrero e animata dagli interventi di Raffaele Di Lieto (Trelleborg), Alvise Biffi (Secure Network), Luca Durante (Cavanna), Luca Durante (CNR Torino), Claudio Ghidini (Sergraf) e Andrea Volpi (Università di Parma). "Se da un lato, è emersa una certa carenza culturale relativamente all'utilizzo di soluzioni di security in ambito manufacturing e di automazione, in quanto in passato non si è data importanza alla sicurezza informatica delle reti d'impianto, chiuse e separate dall'infrastruttura di rete aziendale, oggi si nota un interesse crescente per queste problematiche" riferisce Francesco Nanni di Rockwell Automation, presente durante il dibattito. "Del resto, questo atteggiamento è d'obbligo dato l'utilizzo sempre più spinto in ambito industriale delle reti a base Ethernet, collegabili a Internet per realizzare funzioni di manutenzione remota, telecontrollo e telegestione".

Un mondo variegato

I relatori hanno convenuto su questo punto: è ormai evidente che anche in ambito manifatturiero si sta andando sempre più verso l'adozione di un'unica rete integrata, aperta verso i sistemi esterni. "È anche vero, però, che a un hacker interessa di più 'impossessarsi' dei dati di un intero sistema di supervisione, che delle informazioni relative allo stato di un complesso sensore analogico, quindi è meno probabile che vada verso il campo" prosegue Nanni. Eppure anche il buon funzionamento di un sensore può essere critico per un'applicazione se non si adottano opportune strategie di ridondanza, segnalazione e diagno-



Fonte: www.pressebox.de

stica efficaci, tali da prevenire il sommarsi di più eventi sfavorevoli che possono avere impatti negativi sull'impianto, soprattutto quando si parla di siti produttivi 'sensibili' come centrali elettriche ecc. Si tratta qui non solo di proteggere i macchinari da eventuali malfunzionamenti che possano danneggiarli, o il personale dai rischi connessi a un guasto sulla macchina, bensì anche di assicurare un servizio pubblico efficiente, controllato e sempre disponibile, supervisionando sia la validità e congruità dei dati trasmessi, sia l'efficienza della rete che li trasmette. "Il concetto di Information Security comprende sia la protezione dei dati che transitano sulla rete, sia la sicurezza che non avvengano guasti sulla rete stessa, con conseguenti danni a infrastrutture che da essa dipendono" ha infatti ribadito Nanni. Inoltre, se in ambito IT, come primo aspetto da considerare viene la sicurezza, poi la connettività, infine la 'availability', intesa come garanzia della non interruzione dei servizi di rete; nel campo dell'automazione al primo posto va salvaguardata la 'availability', poi la connettività, infine la sicurezza dei dati. "In ambito produttivo non ci si può permettere un fermo della rete, che si tradurrebbe in perdite di produzione, oltre che in problemi di security/safety: si pensi a centrali elettriche, dighe, raffinerie ecc." spiega Nanni. "Nell'IT, invece, se si blocca la posta elettronica per 2 ore, non ci sono grossi problemi, ma è fondamentale garantire la sicurezza dei dati riservati".

Francesco Nanni, Solution Architect Motion Control di Rockwell Automation

Evoluzioni in atto

La sicurezza, intesa in tutte le sue accezioni, si ottiene pianificando accuratamente le architetture di rete, tenendo debitamente conto di tutti i potenziali punti deboli e realizzando un opportuno piano 'a monte' della soluzione. Occorre poi agire a livello culturale, per evitare comportamenti ingenui da parte degli operatori (un esempio su tutti: l'impiegato che lascia user name e password scritti su un post-it attaccato allo schermo del PC), oltre che per far comprendere a tutti come agire per non creare problemi sulla rete.

Esistono anche dei software in commercio per la validazione automatica della rete, attualmente non sono molto diffusi, anche per i costi elevati (decine di migliaia di euro). Le reti di automazione sono meno soggette a modifiche nel tempo, quindi si può ancora pensare di progettare e validare una rete manualmente, nodo per nodo. L'evoluzione però, anche in ambito industriale, rende sempre più complicato un approccio di questo tipo.

"Oggi i costi di una soluzione integrata di sicurezza sono ancora elevati e implicano un investimento sostanziale al quale non tutti gli utenti finali sono predisposti" conferma infine Nanni. "È certo però che si tratta di un'esigenza, quella della sicurezza, sempre più pregnante e che in futuro non potrà non giocare un ruolo di primo piano, come già oggi si intuisce. Proprio per offrire da subito delle soluzioni efficaci, Rockwell Automation ha deciso di affidarsi al know-how e alla competenza di propri partner, primo fra tutti Cisco, che già dispongono di prodotti e sistemi per assolvere ai compiti di sicurezza. Per questo la collaborazione fra le due realtà è stretta, anche nel campo della ricerca di tecnologie innovative".

Rockwell Automation