

Manutenzione da remoto e know-how per una produzione efficiente



Per le aziende manifatturiere che operano a livello internazionale, è fondamentale che l'accesso per la manutenzione da remoto di macchinari e impianti sia sicuro e controllato. Questo può essere ottenuto con l'implementazione di un'architettura di rete adattata alle esigenze OT e la suddivisione dell'infrastruttura in zone protette.

a cura del Gruppo Meccatronica di ANIE Automazione

Chi realizza macchine o impianti deve essere in grado di correggere eventuali malfunzionamenti in modo tempestivo, risolutivo e sicuro. Nel caso di macchine e impianti commercializzati a livello internazionale, tali azioni non sono garantite. Per una corretta gestione della produzione, è quindi essenziale poter accedere alle macchine a distanza ed effettuare i necessari interventi senza generare rischi e malware. In questo contesto, gli operatori devono considerare diversi criteri per proteggere in modo completo la propria rete aziendale e rendere sicuri gli accessi, evitando situazioni di pericolo con gravi conseguenze che impattano sull'intera catena di produzione.

L'analisi puntuale dei dati raccolti è di fondamentale importanza

La digitalizzazione offre in tal senso grandi opportunità. Grazie a un'analisi puntuale dei dati raccolti dalle macchine e impianti, è possibile gestire la produzione in modo più efficiente e sicuro, e intervenire in modo puntuale e specifico su eventuali anomalie. I fornitori di macchinari e di im-

TECHNOLOGY

Remote maintenance and know-how for **efficient production**

Secure and controlled access for remote maintenance of machinery and systems is essential for international manufacturing companies. This can be achieved by implementing a network architecture adapted to OT needs and the division of the infrastructure into protected zones.

Anyone who builds machines or systems has to be able to correct any malfunctions in a timely, decisive and safe manner. In the case of internationally marketed machines and systems, such actions are not guaranteed. For proper production management, it is therefore essential to be able to access machines remotely and carry out the necessary interventions without generating risks and malware. In this context, operators have to consider various criteria to fully protect their corporate network and secure access, avoiding dangerous situations with serious consequences that impact the entire production chain.

A punctual analysis of the data collected is of paramount importance

Digitalization offers great opportunities in this respect. Thanks to a punctual analysis of the data collected by

the machines and systems, it is possible to manage production more efficiently and safely, and to intervene promptly and specifically on any anomalies. Machinery and system suppliers are the first to know how to fully exploit this data, to manage it in the production process and to offer greater efficiency in production processes thanks to a global vision obtained from data digitalization.

The process of modernizing systems and machines is not so immediate. Objectives such as an increase in productivity, the implementation of new production processes or the automatic connection of production to a digital market require the integration of new machinery within the production process or even new products to be inserted into the network to modernize industrial communication. The increasing demand for detailed data to improve process optimization, energy





- La gestione degli accessi può essere effettuata centralmente tramite un sistema di gestione delle identità e degli accessi che garantisce che solo le persone autorizzate abbiano accesso ai dati critici.
- *Access management can be done centrally via an identity and access management system, which ensures that only authorized persons have access to critical data.*

pianti sono i primi a saper sfruttare appieno questi dati, a gestirli nel processo produttivo e ad offrire maggiore efficienza nei processi produttivi grazie ad una visione globale ottenuta dalla digitalizzazione dei dati.

Il percorso di ammodernamento degli impianti e delle macchine non è così immediato. Obiettivi come un aumento della produttività, l'implementazione di nuovi pro-

cessi di produzione o il collegamento automatico della produzione a un mercato digitale richiedono l'integrazione di macchinari nuovi all'interno del processo produttivo o addirittura nuovi prodotti da inserire nella rete per ammodernare la comunicazione industriale. L'aumento della richiesta di dati dettagliati per migliorare l'ottimizzazione dei processi, l'efficienza energetica e la disponibilità dei

efficiency and machinery availability is a significant challenge. In many countries, there is also a decrease in the qualified technical personnel available on the market. In this context, the know-how of machinery and system suppliers represents an excellent solution for managing upgrades with maximum security.

Implementing network architectures adapted to OT requirements

It is now customary to implement network architectures adapted to OT (Operational Technology) requirements. However, the use of different approaches by each machine and system manufacturer results in a variety of configurations and uncoordinated communication parameters and this creates complications for operators. This scenario makes it difficult to maintain control over such a sensitive and important business infrastructure. To face these challenges, it is becoming more and more strategic to hire specialized personnel in the field of information technology applied to production. The distinction between IT and OT stems from the different needs of business departments. While in

the IT sphere a brief communication breakdown may be tolerable, in manufacturing such an interruption may entail considerable costs. Furthermore, data transmission within production areas can affect the safety of machinery, which may no longer be guaranteed. Real-time communication is of great importance for the precise coordination of production processes, such as the timely stop of a trolley after the activation of a limit switch.

To face the challenges and enable effective and secure communication in global manufacturing, a network architecture adapted to OT needs can be adopted. This architecture consists of industrial network components, such as routers and switches, which can be monitored and controlled both locally at the corresponding factories and from the company headquarters. It is essential to protect the entire corporate IT infrastructure from the risks associated with global interconnection. An effective strategy to address these challenges is the segmentation of the infrastructure according to facilities and functions. For example, risk assessment, according to the IEC 62443 standard,

macchinari rappresentano una sfida significativa. In molti paesi, si osserva anche una diminuzione del personale tecnico qualificato disponibile sul mercato. In tale contesto, il know-how dei fornitori di macchinari ed impianti rappresenta un'ottima soluzione per gestire upgrade con la massima sicurezza.

Implementare un'architettura di rete adattata alle esigenze OT

È ormai consuetudine implementare architetture di rete adattate ai requisiti OT (*Operational Technology*). Tuttavia, l'utilizzo di diversi approcci da parte di ciascun costruttore di macchinari e impianti comporta una varietà di configurazioni e parametri di comunicazione non coordinati e questo crea complicazioni per gli operatori. Questo scenario rende difficile mantenere il controllo su un'infrastruttura aziendale così delicata e importante. Per affrontare tali sfide diventa sempre più strategico assumere personale specializzato nel campo dell'informatica applicata alla produzione.

La distinzione tra IT e OT deriva dalle diverse esigenze dei reparti aziendali. Mentre nella sfera dell'IT una breve interruzione della comunicazione può essere tollerabile, nella produzione tale interruzione può comportare costi considerevoli. Inoltre, la trasmissione dei dati all'interno delle aree di produzione può influire sulla sicurezza dei macchinari,



● Per affrontare le sfide e consentire una comunicazione efficace e sicura nella produzione globale, è possibile adottare un'architettura di rete adattata alle esigenze OT.

● *To face the challenges and enable effective and secure communication in global manufacturing, a network architecture adapted to OT needs can be adopted.*

che potrebbero non essere più garantiti. La comunicazione in tempo reale è di grande importanza per il coordinamento preciso dei processi di produzione, come l'arresto tempestivo di un carrello dopo l'attivazione di un fincorsa. Per affrontare le sfide e consentire una comunicazione efficace e sicura nella produzione globale, è possibile adot-

can guide the division of infrastructure into zones, taking into account information flows and specific risks. In addition to the division between IT and OT, it is possible to further divide the manufacturing infrastructure according to specific facilities and functions. This makes it possible to limit the spread of any accidents to individual zones. The rules configured in the routers ensure that the communication between the systems is selective, thus reducing the potential for attacks and interruptions. Each zone is protected by a VPN router, and security devices specially developed for industrial applications allow maintenance personnel to establish a communication channel with the machinery or system manufacturer, while ensuring protection against unauthorized access. A VPN tunnel is activated via a switch connected to the device, with an LED indicating the status of the connection to reduce the risk of unauthorized opening of the communication. To ensure stable data transmission, additional switches can be used to create redundant networks for machine access. The easy-to-use devices support special protocols and functions widely used in industrial environments such

as Profinet Class B and Ethernet/IP. Access management can be done centrally via an identity and access management system, which ensures that only authorized persons have access to critical data. Machinery and system suppliers can provide support for the implementation of such systems and offer advice on best practices to ensure the safety of the production infrastructure.

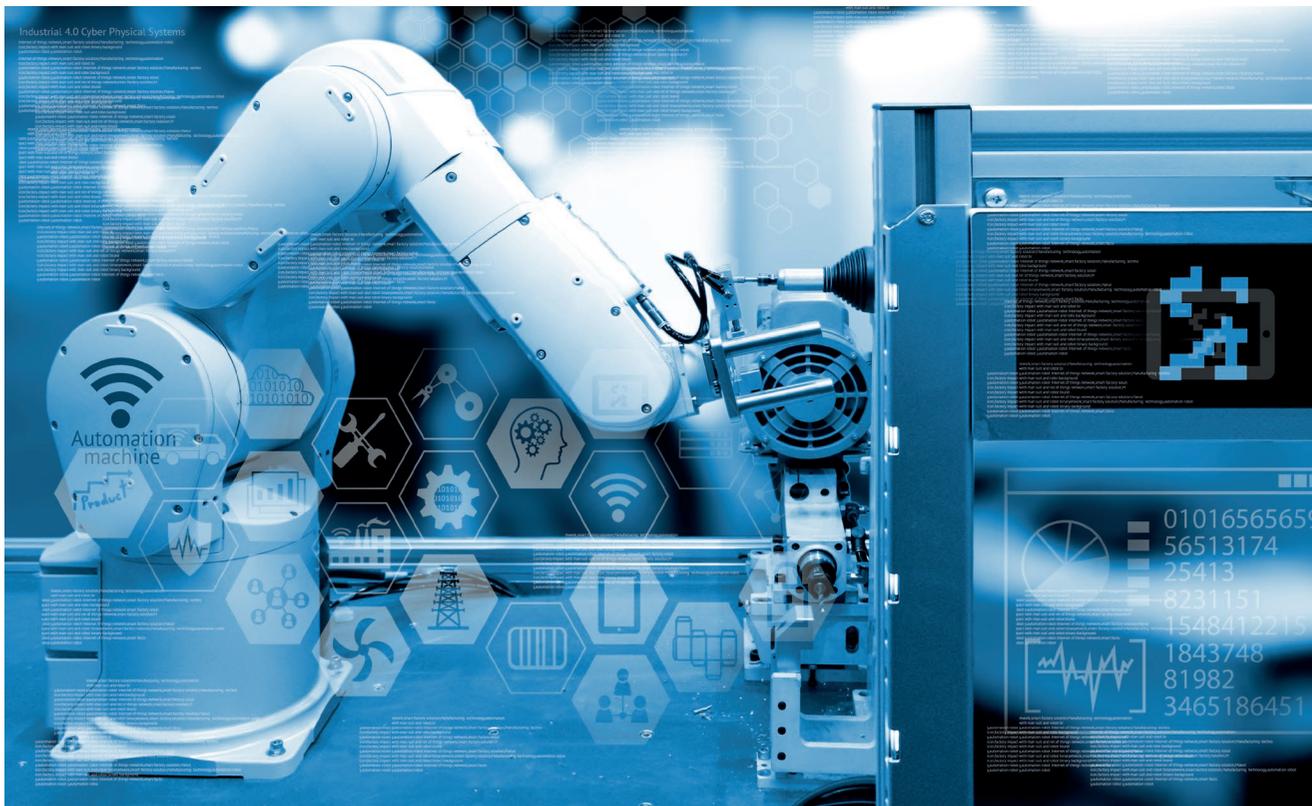
In conclusion...

Secure and controlled access for remote maintenance of machinery and systems is essential for international manufacturing companies.

The implementation of a network architecture adapted to OT needs and the division of the infrastructure into protected zones make it possible to guarantee effective and secure communication, minimizing the risks of unauthorized access and interruptions of production processes. Working with system and machinery suppliers to integrate their specialized knowledge into production processes can be a beneficial option to address the challenges of global manufacturing modernization. ●

● L'accesso sicuro e controllato per la manutenzione remota di macchinari e impianti è fondamentale per le aziende manifatturiere internazionali.

● *Secure and controlled access for remote maintenance of machinery and systems is essential for international manufacturing companies.*



tare un'architettura di rete adattata alle esigenze OT. Questa architettura è costituita da componenti di rete industriali, come router e switch, che possono essere monitorati e controllati sia localmente presso le fabbriche corrispondenti che dalla sede centrale dell'azienda.

È fondamentale proteggere l'intera infrastruttura IT aziendale dai rischi associati all'interconnessione globale.

Una strategia efficace per affrontare tali sfide è la segmentazione dell'infrastruttura in base agli impianti e alle funzioni. La valutazione dei rischi, secondo ad esempio la norma IEC 62443, può guidare la suddivisione dell'infrastruttura in zone, tenendo conto dei flussi di informazioni e dei rischi specifici. Oltre alla divisione tra IT e OT, è possibile ulteriormente suddividere l'infrastruttura di produzione in base agli impianti e alle funzioni specifiche. Questo permette di limitare la diffusione di eventuali incidenti alle singole zone. Le regole configurate nei router garantiscono che la comunicazione tra gli impianti sia selettiva, riducendo così il potenziale di attacchi e interruzioni. Ogni zona è protetta da un router VPN, e i dispositivi di sicurezza appositamente sviluppati per le applicazioni industriali consentono al personale di manutenzione di stabilire un canale di comunicazione con il produttore del macchinario o dell'impianto, garantendo al contempo la protezione dagli accessi non autorizzati. Un tunnel VPN viene attivato tramite uno switch collegato al dispositivo, con un LED che indica lo stato della connessione per ridurre il rischio di aperture

non autorizzate della comunicazione. Per garantire una trasmissione stabile dei dati, possono essere utilizzati switch aggiuntivi per creare reti ridondanti per l'accesso ai macchinari. I dispositivi di facile utilizzo supportano i protocolli e le funzioni speciali ampiamente utilizzati in ambienti industriali come Profinet Classe B ed Ethernet/IP.

La gestione degli accessi può essere effettuata centralmente tramite un sistema di gestione delle identità e degli accessi, che garantisce che solo le persone autorizzate abbiano accesso ai dati critici. I fornitori di macchinari ed impianti possono fornire supporto per l'implementazione di tali sistemi e offrire consulenza sulle migliori pratiche per garantire la sicurezza dell'infrastruttura di produzione.

In conclusione...

L'accesso sicuro e controllato per la manutenzione remota di macchinari e impianti è fondamentale per le aziende manifatturiere internazionali. L'implementazione di un'architettura di rete adattata alle esigenze OT e la suddivisione dell'infrastruttura in zone protette consentono di garantire una comunicazione efficace e sicura, minimizzando i rischi di accessi non autorizzati e interruzioni dei processi di produzione. Collaborare con i fornitori di macchinari ed impianti per integrare la loro conoscenza specializzata nei processi di produzione può essere un'opzione vantaggiosa per affrontare le sfide della modernizzazione della produzione globale. ●