La Cyber Security in applicazioni di automazione industriale

Oggi molti sistemi OT, progettati e implementati a suo tempo, non sono attrezzati per resistere agli attacchi informatici. Come possono essere resi più sicuri? Tra le diverse vie che possono essere seguite vi è lo standard IEC 62443, che può portare al miglioramento della sicurezza, alla conformità normativa, all'aumento della produttività e delle opportunità di business oltre alla maggiore trasparenza per i clienti finali del mondo industriale. Vediamo come.

a cura del Gruppo Meccatronica di ANIE Automazione

L'incremento degli attacchi informatici contro i processi industriali genera sempre maggiore preoccupazione per le aziende, di qualsiasi settore. Interruzioni nei processi industriali possono causare perdite economiche significative, interrompendo la produzione e danneggiando la reputazione dei clienti finali.
Secondo l'ultimo rapporto Clusit, il numero di attacchi informatici nel settore manifatturiero è cresciuto del 34% rispetto all'anno precedente, con un aumento del 53% degli attacchi gravi dal 2018.
Questi numeri dimostrano che la minaccia degli attacchi informatici continua a crescere, nonostante le misure di sicurezza adottate dalle aziende.
Ci sono aziende che si sono organizzate e hanno investito in misure di sicurezza, ma ci sono ancora molte realtà che non riescono a integrare efficacemente queste misure per mancanza di risorse o di organizzazione interna.
Oggi le reti industriali hanno diversi problemi di sicurezza informatica. Molti sistemi OT sono stati progettati e implementati molto tempo fa e non sono stati concepiti per

Technology

Cyber Security in industrial automation applications

Today, many OT systems, designed and implemented long ago, are not equipped to resist cyber attacks. How can they be made more secure? Among the many paths that can be followed is the IEC 62443 standard, which can lead to improved security, regulatory compliance, increased productivity, increased business opportunities and greater transparency. Let's see how.

The increase in cyber attacks against industrial processes is generating growing concern for companies, in any industry. Disruptions in industrial processes can cause significant economic losses, interrupting production and damaging the reputation of end customers.
According to the latest Clusit report, the number of cyber attacks in the manufacturing sector grew by 34% compared to the previous year, with a 53% increase in serious attacks since 2018. These numbers show that the threat of cyber attacks continues to grow, despite the security measures taken by companies.
There are companies that have organized themselves and invested in security measures, but there are still many realities that fail to effectively integrate these measures for lack of resources or internal organization.
Today industrial networks have several IT security problems. Many OT systems were designed and implemented a long time ago and were not designed to withstand modern cyber attacks. These systems are often obsolete and unsupported, which means they are no longer update with the latest security patches.
If we take a closer look at the corporate network, we realize that there are many weaknesses and we often have to deal with a completely flat OT network. Then there are serious issues such as, for example, non-separate IT and OT networks, use of unmanaged switches within the productive islands, unsafe remote access, uncontrolled and unprotected Ethernet

● Secondo l'ultimo rapporto Clusit, il numero di attacchi informatici proprio nel settore manifatturiero è cresciuto del 34% rispetto all'anno precedente.

● *According to the latest Clusit report, the number of cyber attacks in the manufacturing sector grew by 34% compared to the previous year.*

resistere agli attacchi informatici moderni. Questi sistemi sono spesso obsoleti e non supportati, il che significa che non sono più aggiornati con le patch di sicurezza più recenti.
Se guardiamo più attentamente la rete aziendale ci accorgiamo che ci sono moltissimi punti deboli e spesso e volentieri abbiamo a che fare con una rete OT completamente *flat*. Ci sono poi problematiche serie come, per esempio, reti IT e OT non separate, utilizzo di switch non gestiti all'interno delle isole produttive, accessi da remoto non sicuri, punti di accesso alla rete ethernet non controllate e non protette fisicamente.
Un altro tema è la formazione del personale interno che è uno dei primi passi da fare per aumentare la sicurezza dei processi industriali. La politica "zero trust" che, per garantire la sicurezza, punta sul concetto di non fare affidamento su nulla all'interno di una rete, richiede la verifica e l'autenticazione di ogni richiesta di accesso alla rete. Essa può essere una soluzione efficace per proteggere la rete da minacce interne ed esterne.

Come si possono rendere più sicuri i sistemi OT?

Lo standard IEC 62443, che si sposa perfettamente con la politica "zero trust" in ambito OT, può portare al miglioramento della sicurezza dei sistemi OT, alla conformità normativa, all'aumento della produttività, all'aumento delle opportunità di business e alla maggiore trasparenza per i clienti finali del mondo industriale.
Quando verrà rilasciato il nuovo regolamento europeo (ex Direttiva Macchine), le aziende dovranno condurre un'analisi approfondita dei rischi dei propri sistemi OT per identificare le minacce alla sicurezza e le vulnerabilità che potrebbero compromettere la sicurezza dei sistemi.
È richiesto un design sicuro dei sistemi OT che include diverse misure per proteggere l'intero sistema. La prima cosa da fare è gestire le password di ogni singolo dispositivo, magari chiudendo gli armadi a chiave e le porte di accesso ethernet. Se, ad esempio, si possiede uno switch gestito, si possono bloccare le porte non utilizzate. Successivamente, si possono dividere tutte le zone in isole e tra una zona e l'altra è possibile utilizzare un router firewall idoneo per effettuare la segmentazione di rete. In questo modo, se una zona viene compromessa, il virus avrà maggiori difficoltà a propagarsi nelle altre aree aziendali.

Anche la certificazione IEC 62443 può contribuire alla sicurezza

Nella valutazione dei sistemi da adottare per proteggere le macchine, si può arrivare persino all'implementazione di PLC certificati IEC 62443. Inoltre, si possono utilizzare sistemi di monitoraggio del traffico (*Intrusion Detection System*) e dei protocolli di automazione che circolano tra i sistemi. Si possono creare delle VPN e aprire i canali della teleassistenza solo quando necessario, dei sistemi di autenticazione crittografati e, ancora meglio, prevedere un SIEM per analizzare tutti i log popolati dai dispositivi di automazione.

network access points. Another theme is the training of internal staff which is one of the first steps to be taken to increase the safety of industrial processes. The "zero trust" policy, which focuses on the concept of not relying on anything within a network to ensure security, requires verification and authentication of each request for network access. It can be an effective solution to protect the network from internal and external threats.

How can OT systems become more secure?

The IEC 62443 standard, which fits perfectly with the "zero trust" policy in the OT field, can lead to an improvement in the safety of OT systems, regulatory compliance, increased productivity, increasing business opportunities and greater transparency for end customers in the industrial world.
When the new European regulation (former machine directive) is released, companies will need to conduct an in-depth risk analysis of their OT systems to identify security threats and vulnerabilities that could compromise system security.
It requires a secure design of OT systems that includes several measures to protect the entire system. The first thing to do is to manage the passwords of each individual device, perhaps by locking cabinets and Ethernet access ports. For example, if you have a managed switch, you can lock unused ports. Next, you can divide all zones into islands and between zones you can use a firewall router suitable for network segmentation. In this way, if an area is compromised, the virus will have more difficulty spreading to other business areas.

The IEC 62443 certification can also contribute to security

In evaluating the systems to be adopted to protect

● Nella valutazione dei sistemi da adottare per proteggere le macchine, si può arrivare persino all'implementazione di PLC certificati IEC 62443.

● *In evaluating the systems to be adopted to protect the machines, it is even possible to implement IEC 62443 certified PLCs.*

Le aziende dovrebbero adottare un approccio proattivo alla gestione delle vulnerabilità, con patch regolari, aggiornamenti software e procedure di gestione delle vulnerabilità per ridurre il rischio di attacco. È altrettanto importante formare e sensibilizzare il personale sui processi di sicurezza, i rischi informatici, le buone pratiche di sicurezza.
IEC 62443 prevede una serie di livelli di sicurezza, ognuno dei quali definisce un insieme di controlli di sicurezza da implementare per raggiungere quel livello. Questi livelli sono applicabili sia ai sistemi di controllo industriale che alle reti IT.
Il primo livello è il "Security Level 0", che si applica a sistemi che non richiedono particolari misure di sicurezza. Al contrario, il "Security Level 4" è il livello più alto e prevede controlli di sicurezza rigorosi per proteggere i sistemi di controllo industriale critici.
L'implementazione degli standard IEC 62443 richiede un approccio olistico alla sicurezza, che coinvolge l'intero ciclo di vita del sistema, dalla progettazione alla manutenzione.
In conclusione, l'implementazione dello standard IEC 62443 richiede un impegno da parte delle aziende, ma i benefici che ne derivano in termini di sicurezza, conformità normativa, produttività e trasparenza sono notevoli. In un'epoca in cui gli attacchi informatici contro i processi industriali sono sempre più frequenti, adottare misure di sicurezza efficaci diventa un'esigenza prioritaria per proteggere la produzione e garantire la continuità del business. ●

the machines, it is even possible to implement IEC 62443 certified PLCs.
In addition, traffic monitoring systems (Intrusion Detection System) and automation protocols circulating between systems can be used.
You can set up VPNs and open up remote assistance channels only when needed, encrypted authentication systems and, if you want to do things right, set up a SIEM to analyze all the logs populated by automation devices.
Companies should take a proactive approach to vulnerability management, with regular patches, software updates and vulnerability management procedures to reduce the risk of attack. It is equally important to train and raise awareness of security processes, IT risks and good security practices.
IEC 62443 provides a number of security levels, each of which defines a set of security controls to be implemented to reach that level.
These levels are applicable to both industrial control systems and IT networks.
The first level is "Security Level 0", which applies to systems that do not require special security measures. In contrast, "Security Level 4" is the highest level and provides strict security controls to protect critical industrial control systems.
The implementation of IEC 62443 requires a holistic approach to safety, involving the entire system lifecycle from design to maintenance.
In conclusion, the implementation of IEC 62443 requires a commitment from companies, but the resulting benefits in terms of security, regulatory compliance, productivity and transparency are remarkable.
At a time when cyber attacks against industrial processes are increasingly frequent, taking effective security measures becomes a priority to protect production and ensure business continuity. ●