Memoria per Telecontrollo 2015

Autore della memoria
Raffaele Esposito
Product Manager Safety, I/O & Networking
Phoenix Contact Spa

Titolo della memoria
La Cyber Security quale elemento strategico dell'approccio Industry 4.0

Abstract (in italiano)
La sfida costituita dalle necessità di flessibilità ed efficienza produttiva è affrontata dal mondo dell'industria con un ricorso sempre più massiccio e consapevole alle tecnologie digitali in senso lato.
La costante evoluzione di tali tecnologie consente di immaginare e sperimentare sempre nuovi scenari innovativi per i processi di progettazione e produzione industriale, con un'influenza che lascia ormai pochi dubbi sul fatto che queste tecnologie stanno, di fatto, avviando una vera e propria nuova Rivoluzione Industriale.
Si tratterebbe della quarta (dopo quelle caratterizzate dall'uso a fini produttivi del vapore, dell'elettricità e dell'energia nucleare), da qui il termine ''Industry 4.0'' utilizzato per la prima volta a livello ministeriale tedesco.
Come per ogni evento ''rivoluzionario'' che si rispetti, Industry 4.0 si propone di modificare radicalmente approcci, strumenti e modalità operative del mondo industriale basandosi sui cosiddetti ''sistemi virtuali-reali'' (Cyber Physical Systems in inglese), vale a dire sistemi ad alta complessità costituiti da componentistica intelligente basata su varie tecnologie quali ad esempio quella meccanica, l'elettronica, l'informatica e che, in genere, sono posti tra loro in comunicazione attraverso una rete, spesso costituita da Internet.
In queste nuove realtà industriali, sinteticamente ed eccellentemente identificate con la definizione "smart factory", i vantaggi tecnologici introdotti potrebbero essere del tutto annullati da una politica non efficace di protezione da accessi non autorizzati all'infrastruttura di rete.
Facilmente intuibili ma ancora colpevolmente sottovalutate sono infatti le conseguenze di una possibile perdita di dati aziendali legate a un accesso fraudolento (on site o da remoto) a un'infrastruttura di rete aziendale.

La perdita di semplici dati di produzione o di tipo statistico potrebbe essere visto come privo di conseguenze particolari per la solidità di un'azienda ma diverso è lo scenario se si cala anche questo possibile evento nella giusta prospettiva: si pensi solo al costo in termini di ore lavorative di specifiche risorse aziendali o alla necessità produttiva di impianto necessarie per ricostruire i dati persi.

La perdita di dati sensibili può invece avere conseguenze letali per una qualsiasi azienda se si pensa alla perdita di know-how, aspetto più o meno quantificabile in termini monetari a seconda dei casi, o, soprattutto, alle possibili conseguenze di un danneggiamento irreversibile della reputazione aziendale sul mercato.

Anche il semplice accesso fraudolento all'infrastruttura di rete aziendale, pur senza la capacità di accesso alle aree della stessa ove sono contenuti i dati aziendali sensibili, può risultare estremamente dannoso anche per altri aspetti quali il possibile sabotaggio degli impianti produttivi, la modifica delle caratteristiche di sicurezza degli stessi o il cosiddetto "Hijacking" (uso di un computer di cui si è preso il controllo in modo fraudolento per spiare o attaccare una terza parte).

Conseguenze economiche e/o legali che possono, nei casi più estremi, compromettere il possibile proseguimento dell'attività aziendale stessa.

Nel corso dell'intervento la Cyber Security verrà declinata mediante l'illustrazione di tecniche di protezione utili a impedire accessi fraudolenti a infrastrutture di rete più o meno complesse e che possono essere, in maniera più o meno agevole, calate anche nella realtà industriale.

Questa sintetica panoramica di possibili misure di protezione toccherà quegli ambiti applicativi ove possa risultare necessario una protezione da accessi locali (on site) piuttosto che applicazioni che prevedono un accesso sicuro da remoto per operazioni di telecontrollo o teleassistenza.

In quest'ultimo caso si porrà in particolare l'attenzione su soluzioni verticalmente dedicate alle applicazioni di tipo industriale capaci di coesistere con infrastrutture aziendali di tipo IT anche molto complesse e capaci di essere implementate da tecnici esperti in automazione aziendale e poco avvezzi a soluzioni tipiche dell'area IT.

Abstract (in inglese)

In the new industrial realities that operate following the so called "Industry 4.0" approach, the also called "Smart Factories", the technical advantages introduced form the new digital technologies could be completely frustrated from a not sufficient protection against not authorized accesses to the Ethernet network.

Easily foreseeable but still underestimated are the consequences of a company data loss due to a fraudulent access (on site or from remote) to an industrial network.

The loss of "simple" production or statistic data could be seen as lacking in particular consequences for the stability of an industrial company but this scenario becomes a little different if

we consider also the costs needed in term of working or production hours for the rebuilding of the lost data (when possible!).

The loss of substantial data can on the contrary introduce lethal consequences for any industrial company.

Let's consider the potential know-how loss, aspect that with difficulties can in advance be economical quantified, or, especially, let's think about potential lethal consequences of an irreversible damage to the company reputation on the market.

The simple fraudulent access to the network, also in case of limitation of this access to the network part(s) where the substantial data are not available, can in any case result extremely dangerous for additional aspects like for example potential sabotage of the production facilities, modification of the safety level of these facilities or the so called "Hijacking" (use of a computer kept fraudulently under control for spying or attacking a third part company).

The economic and/or legal consequences of such an erroneously underestimated access could, in extreme cases, even compromise the continuity of the company activity.

During the presentation the description of the Cyber Security aspects will be limited to the illustration of some protection techniques useful to avoid fraudulent access to industrial network, independently from their complexity.

This concise potential protective measures survey will include both applications where a local or a from remote access can be necessary, like for example applications for remote control and/or remote assistance.

In this last case, a particular focus will be reserved to those vertical solutions for industrial applications able to coexist with also complex IT company infrastructures and able to be used and installed from typical industrial automation technicians, not expert for IT solutions.