La cibersicurezza nella manutenzione dell'industria di processo 4.0

La nuova digitalizzazione comporta rischi addizionali ed emergenti. Perché è importante tutelarsi con misure riguardanti l'hardware ed il software

Domenico Barone
Esperto in sicurezza industriale, Tecnologie Sicurezza Industriale Srl

Con la sempre più diffusa digitalizzazione delle industrie di processo in accordo al paradigma dell'Industry 4.0 e, in particolare, con l'interconnessione ad Internet e l'utilizzo di dispositivi mobili digitali (PC, chiavette USB, laptop, ecc.), sia per il controllo operativo sia per le attività di manutenzione locale e/o a distanza, gli impianti diventano vulnerabili ad eventuali attacchi informatici esterni e/o interni, intenzionali oppure casuali. E' quindi di assoluta importanza la Cibersicurezza (Cyber security), vale a dire la protezione della confidenzialità, integrità e disponibilità del cyberspazio, che è l'ambiente complesso derivante dalle interazioni di persone, software e servizi internet mediante dispositivi tecnologici e reti connesse ad esso (Norma ISO /IEC 27032:2012 Information Technology-Security techniques-Guidelines for cybersecurity). Le reti informatiche aziendali IT (*Information Technology*), relative al trattamento dei dati aziendali per il personale, gli acquisti, le vendite, l'amministrazione, ecc., e le reti OT (*Operational Technology*), relative al controllo di processo ed alla manutenzione eseguito tramite DCS, PLC, SCADA, SIS, HMI, ecc., sono sempre più interconnesse tra di loro. In questo ambito, si ritiene spesso che la funzione aziendale che si interessa dei sistemi informatici IT controlli adeguatamente anche la rete OT mediante "fire walls" multipli e/o sistemi di rilevazione intrusioni che non sono spesso sufficienti, essendo anch'essi vulnerabili.

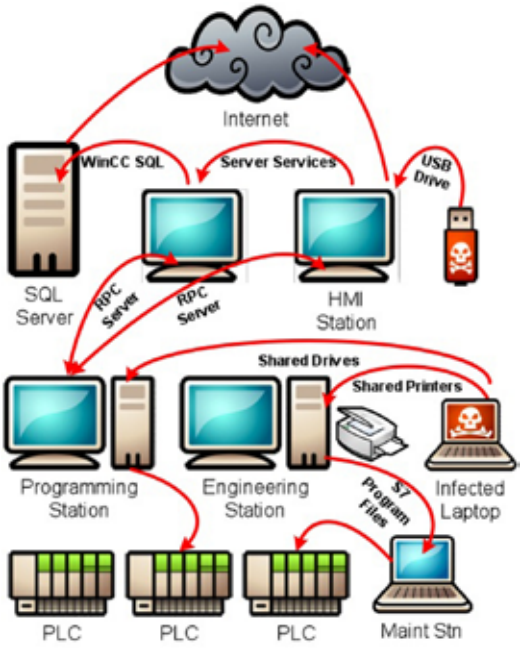
Reti IT/OT e vulnerabilità

La tipologia di manutenzione negli impianti di processo è generalmente reattiva (su guasto), preventiva (a scadenza), secondo condizione (in base allo stato del componente) e predittiva (con monitoraggio continuo). Per l'esecuzione di ciascuna tipologia sono necessari sistemi digitali sia per la parte IT che la parte OT. Per la parte IT, i sistemi servono a gestire dati macchine ed apparecchiature, dati interventi/scadenze/risultati, permessi di lavoro. Per la OT parliamo di sistemi di monitoraggio e controllo macchine (ICS), sistemi allarmi e blocchi automatici (SIS), sistemi di sicurezza (rilevatori gas, incendio, impianti antincendio).
I sistemi digitali facenti parte dell'OT hanno avuto negli ultimi tempi un incremento delle interconnessioni con intranet ed internet a causa di:

- *aggiornamento dei sistemi operativi (es. Windows);*
- *aggiornamento apparecchiature/strumentazione del tipo "smart";*
- *centralizzazione monitoraggi;*
- *modifiche apparecchiature elettroniche.*

Ma con la connessione aumenta la vulnerabilità. Negli anni passati sono avvenuti incidenti connessi alle attività di manutenzione e controllo in sistemi digitali, quali ad esempio:

- inserimento nei sistemi di controllo di centrifughe in Iran (2010) per l'arricchimento di uranio del virus Stuxnet tramite chiavetta USB durante una procedura di manutenzione ordinaria; tale virus ha causato la distruzione e messa fuori servizio di molte centrifughe a causa dell'alta velocità imposta al sistema di controllo digitale, senza alcuna segnalazione agli operatori ai quadri di controllo;



- rottura di oleodotto BTC con incendio ed esplosione in Turchia (2008) a causa di una sovrappressione intenzionale dovuta ad un attacco hacker al sistema di controllo con soppressione degli allarmi, manipolazione dei set di processo ed assenza di segnalazione agli operatori;
- incidente nella raffineria BP di Texas city (2005) con 15 morti e circa 170 feriti; a seguito di anomalia di processo non correttamente gestite dai sistemi ICS e SIS; durante l'avviamento di un impianto di isomerizzazione, dopo una manutenzione generale dello stesso, ci fu il rilascio di idrocarburi liquidi dallo scarico di emergenza dello stesso; la nube di vapori sviluppatisi fu innescata da un veicolo di servizio presso una baracca mobile del personale di manutenzione ubicata vicino all'impianto; tale incidente non fu intenzionale ma è stato utilizzato come studio di riferimento da molti esperti di cibersicurezza come esempio di conseguenze di un attacco informatico.

Il numero di incidenti connessi alla cibersicurezza negli impianti di processo e nelle infrastrutture critiche continua ad aumentare, rendendo necessaria l'adozione di misure di sicurezza per ridurre i rischi informatici.

Alcune misure adottabili per la cibersicurezza

Le misure di cibersicurezza adottabili, ove possibile, nei sistemi digitali utilizzati nelle industrie di processo per la manutenzione ed il controllo sono generalmente:

- *isolamento da internet (protezione fisica);*
- *procedure di security digitale (fattore umano);*
- *barriere di isolamento (firewall);*
- *controllo chiavette USB (protezione fisica);*
- *test di penetrazione (software, hardware).*

I sistemi di controllo di processo (ICS) e di allarme e blocco automatico (SIS) possono essere verificati valutando il Security Level (SL) in accordo alla IEC 62443-3. Questi SL, a differenza dei SIL (*Safety Integraty Level*) che secondo IEC 61511 sono valutati in probabilità, sono definiti da vettori di 7 Requisiti Funzionali (FR) con valori da 1 a 4 che riguardano i seguenti punti fondamentali della cibersicurezza:

- *controllo autenticazione ed identificazione;*
- *controllo utilizzo;*
- *integrità sistema;*
- *confidenzialità dati;*
- *limitazione flusso dati;*
- *risposta all'emergenza;*
- *disponibilità risorse.*

La verifica dello stato di cibersicurezza della OT di una industria di processo con pericolo di incidenti rilevanti quali esplosioni, incendi, rilasci tossici per l'uomo e per l'ambiente (soggetta alla legge Seveso - Dlgs 105/2015) può essere effettuata con check lists basate sui pericoli/attacchi rilevati recentemente ai sistemi di controllo industriali (CS) negli USA. Qui è in vigore da alcuni anni (2013) un ordine esecutivo presidenziale relativo alla cibersicurezza che rende obbligatorio alle imprese la denuncia di ogni attacco informatico subito alla autorità. A breve ciò avverrà anche in Europa. Essi sono stati in ordine di priorità crescente:

- *ingegneria sociale e truffa online (phishing);*
- *infiltrazione codici maligni (malware) attraverso mezzi /hardware esterni;*
- *infiltrazione codici maligni (malware) attraverso internet ed intranet;*
- *intrusioni attraverso accesso remoto;*
- *errore umano e sabotaggio;*
- *malfunzionamenti tecnici ed eventi di forza maggiore;*
- *compromissione dei componenti extranet e cloud;*
- *attacchi per negazione del servizio (DoS);*
- *compromissione di smart phone nei luoghi di produzione.*

Conclusioni

Le conseguenze di eventuali attacchi informatici esterni e/o interni ai sistemi IT o OT di una industria sono diverse. Nel caso dei sistemi IT si ha generalmente il blocco dei sistemi raccolta e gestione dati, la cui mancanza temporanea non provoca generalmente problematiche di sicurezza alle persone e/o agli impianti produttivi.

Nel caso dei sistemi OT degli impianti di processo (Seveso) e/o delle pipelines, oltre alla possibilità di blocco della produzione, si possono avere problematiche connesse al mancato o improprio funzionamento dei sistemi automatici di sicurezza con possibili rilasci delle sostanze pericolose presenti, con formazione di nubi tossiche e/o infiammabili, incendi, esplosioni e contaminazioni di acque e/o suolo. I nuovi rischi addizionali ed emergenti dovuti al fenomeno della digitalizzazione 4.0 devono essere adeguatamente gestiti con misure di cibersicurezza riguardanti sia l'hardware ed il software sia le procedure connesse.Tali misure dovrebbero far parte del risk management aziendale data l'importanza delle conseguenze di eventuali attacchi.