LA CYBERSICUREZZA NELL'INDUSTRIA 4.0 SOSTENIBILE

Ing. Domenico Barone, Tecnologie Sicurezza Industriale S.r.l.,
Via P. Lomazzo 51, 20154 Milano, do.barone.tsi@gmail.com

Seminario AEIT: La Sostenibilità – Roma 1 marzo 2018

SOMMARIO

La cybersicurezza dell'industria 4.0 sostenibile riguarda generalmente i sistemi digitali di controllo e blocco automatico che hanno un ruolo importante nella sicurezza attiva, soprattutto negli impianti di processo (Seveso), per evitare esplosioni, incendi, rilasci tossici, inquinamento e le loro conseguenze sul piano ambientale, economico e sociale.

I nuovi rischi informatici addizionali ed emergenti devono essere adeguatamente gestiti con misure di cybersicurezza riguardanti sia l'hardware ed il software sia le procedure di security, ovvero l'impiego di tecnologie analogiche, alternative a quelle digitali, per i settori critici dell'industria. Tali misure dovrebbero far parte del risk management aziendale, data l'importanza di eventuali attacchi sull'ambiente, sull'economia e sulle società.

L'INDUSTRIA 4.0 SOSTENIBILE

L'industria 4.0 è considerata la quarta rivoluzione industriale dopo quelle precedenti caratterizzate come di seguito:

1.0 Impiego di energia meccanica con l'utilizzo dell'acqua e del vapore (fine 1700-inizio 1800)
2.0 Impiego di energia elettrica (fine 1800)
3.0 Impiego di automazione con sistemi elettronici ed informatici (metà 1900)
4.0 Impiego di sistemi cyberfisici intelligenti ed interconnessi (inizio 2000).

L'industria 4.0 comporta la trasformazione dei settori industriali attraverso l'integrazione dei sistemi di automazione in quelli di Information Technology (IT) con l'impiego delle seguenti principali tecnologie:

- Robot collaboratori interconnessi e rapidamente programmabili
- Stampanti 3D connesse a software di sviluppo
- Realtà aumentata a supporto dei processi produttivi
- Simulazione tra macchine interconnesse
- Internet industriale con comunicazioni tra processi produttivi e prodotti
- Gestione di elevate quantità di dati su sistemi aperti (Cloud)
- Analisi dati per ottimizzazione prodotti e processi.

I principali elementi di sostenibilità nell'industria 4.0 automatizzata ed interconnessa sono quelli come di seguito descritto:

- *piano sociale*: evoluzione del mondo del lavoro con nuove professionalità, modalità di produzione, di utilizzo prodotti e servizi
- *piano economico*: maggiore produttività e qualità, minori costi
- *piano ambientale* : ottimizzazione dei processi produttivi con minore impiego di risorse naturali e di energia, di minor produzione di rifiuti e di emissioni in aria, acqua, suolo.

CYBERSICUREZZA E SISTEMI DI GESTIONE

Secondo la norma ISO/IEC 27032:2012 (Information Technology – Security Techniques for Security) il cyberspazio è l'ambiente complesso derivante dalla interazione di persone, software e servizi internet mediante dispositivi tecnologici e reti connesse ad esso.
La cybersicurezza (o sicurezza informatica) riguarda la protezione della confidenzialità, integrità e disponibilità del cyberspazio.

Elementi fondamentali di un sistema di gestione della cybersicurezza sono la politica e la tecnologia.

La politica richiede un rigoroso inventario di tutti gli assets informatici dell'organizzazione, la considerazione dei principali elementi chiavi (quali informazioni proprietarie, antivirus, passwords, gestione incidenti, back up e recupero) e la gestione dei rischi.

La tecnologia per far fronte ad accessi non autorizzati, alla perdita di dati, ad attacchi tipo negazione del servizio (DoS) consiste essenzialmente nella difesa del perimetro, nel back up e recupero, nella criptatura e nella firma digitale.

La difesa del perimetro contro accessi non autorizzati alle risorse informatiche è generalmente effettuata con barriere (firewall), con sistemi di rilevazione intrusione e con Reti Virtuali Private (VPN).

RETI INFORMATICHE AZIENDALI (IT/OT) E SISTEMI DI CONTROLLO AUTOMATICO INDUSTRIALE (IACS)

Le reti informatiche aziendali IT relative al trattamento dei dati aziendali per il personale, gli acquisti, le vendite, l'amministrazione contabile sono state per lungo tempo completamente isolate sia dal mondo esterno sia dagli altri sistemi elettronici, generalmente analogici relativi alla produzione: tali sistemi si sono successivamente digitalizzati con l'adozione di sistemi a controllo distribuito (DCS) per le regolazioni, di logiche programmabili (PLC) per i sistemi di blocco automatico (SIS), di sistemi di controllo e supervisione telecomandati (SCADA), di stazioni di lavoro (Work Station HMI), con tastiere di comando e schermi di controllo. I suddetti sistemi costituiscono la rete di OT (Operational Technology).

L’avvento di internet quale strumento di interconnessione per ricevere/inviare dati ed informazioni digitali ha inizialmente coinvolto solo la IT e successivamente la OT a causa dell’aggiornamento necessario dei sistemi operativi (es. Windows), delle apparecchiature/strumentazioni del tipo smart e della centralizzazione dei monitoraggi.
Nel caso di attacco informatico al sistema IT si ha generalmente il blocco ai sistemi di gestione e raccolta dati la cui mancanza temporanea non provoca generalmente problematiche di sicurezza alle persone e/o agli impianti produttivi.

Esempi di sistemi IACS per un piccolo stabilimento industriale e per uno di grande estensione sono riportati nelle figure 1 e 2. In tali figure sono riportate: la rete IT (Corporate Network), il sistema IACS che fa parte della Basic Process Control System (BPCS) zona, il sistema di blocco automatico (SIS), la zona di isolamento DMZ (Demilitarized Zone).

Fig. 1

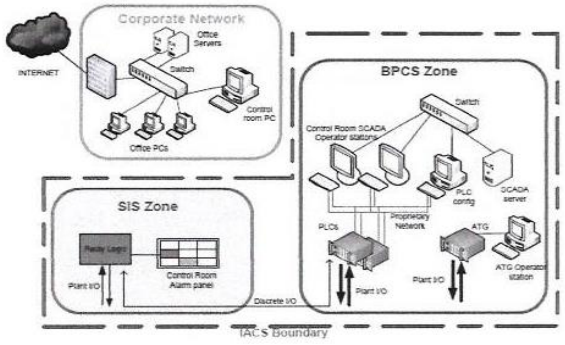
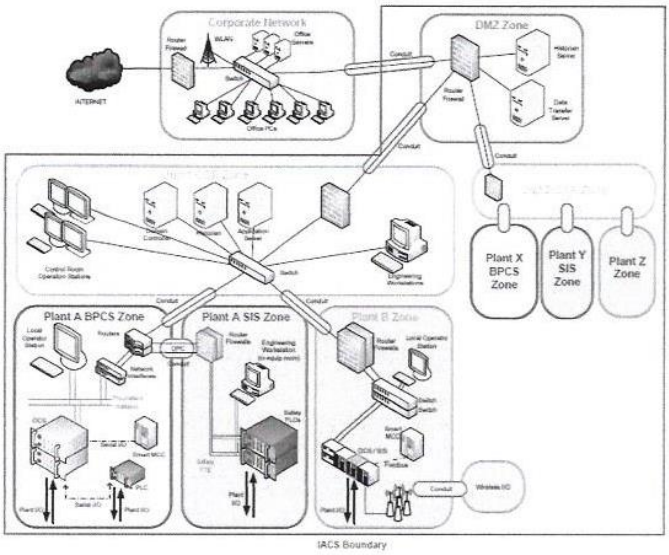


Fig. 2



I sistemi di controllo IACS presenti nell’industria 4.0 sono quasi tutti completamente digitalizzati ed essendo connessi ad internet/intranet, possono essere oggetto di attacchi informatici dall’esterno e dall’interno, intenzionali o casuali che possono bloccare o compromettere la loro funzionalità e la sicurezza degli impianti. Tali sistemi provvedono infatti al controllo della

produzione ed hanno un ruolo importante nella sicurezza attiva degli impianti di processo tipo Seveso per evitare esplosioni, incendi e rilasci tossici nell'ambiente (aria, acqua, suolo).

I sistemi di controllo elettronici analogici e/o di blocco automatico di tipo elettromeccanico a relè sono invece completamente isolati dal mondo esterno (internet o chiavetta USB) e non sono attaccabili. Tali sistemi analogici, peraltro ancora esistenti in molti impianti nucleari ed alcune industrie, sono oggetto di rivalutazione e di modernizzazione per alcune installazioni critiche industriali.

INCIDENTI AVVENUTI PER ATTACCHI INFORMATICI A SISTEMI IACS

Negli anni passati sono avvenuti numerosi incidenti nei sistemi IACS dell'industria (raffinerie, petrolchimici, pipeline, utilities). Nel seguito si riportano alcuni di quelli che hanno avuto un maggior impatto.

- IRAN (2010) L'inserimento, nei sistemi digitali di controllo, di centrifughe per l'arricchimento di uranio del virus Stuxnet, tramite chiavetta USB, durante una procedura di manutenzione ordinaria ha causato la distruzione e la messa fuori servizio di molte centrifughe. Ciò è stato causato dall'alta velocità imposta al sistema di controllo, senza alcuna segnalazione agli operatori sul quadro di controllo.
- TURCHIA (2008) Rottura dell'oleodotto BTC con incendio ed esplosione a causa di una sovrappressione intenzionale dovuta ad attacco hacker al sistema di controllo con soppressione degli allarmi, manipolazione dei set di processo ed assenza di segnalazione agli operatori (vedi fig. 3).

Fig. 3 – BTC 2008

- ARABIA SAUDITA (2017) Inserimento nel sistema di blocco automatico (SIS) del virus Triton con successivo blocco generale dell'impianto con rischi per la sicurezza dello stesso.

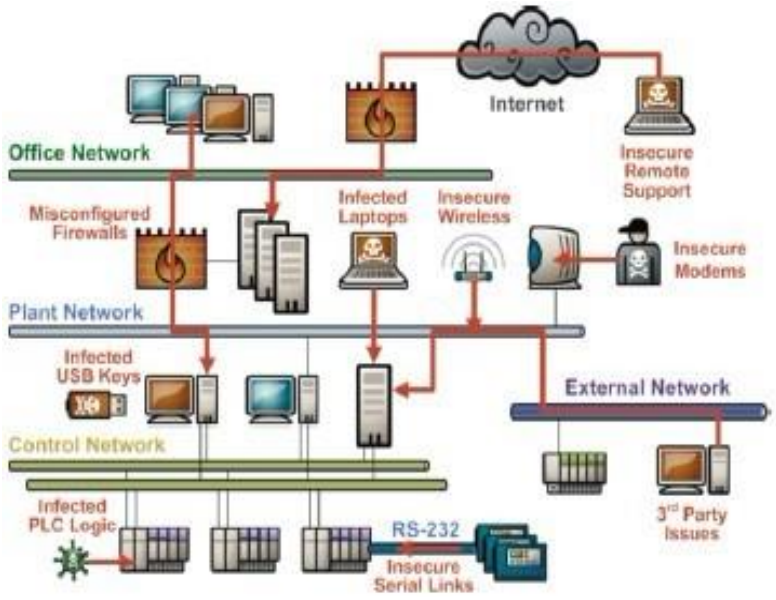
Un altro incidente avvenuto nel 2005 a Texas City (USA) connesso al malfunzionamento del sistema IACS di un impianto di raffineria è stato considerato da molti esperti di cybersicurezza come esempio delle possibili conseguenze di un attacco informatico.
L'incidente è avvenuto nella raffineria BP di Texas City a seguito di anomalie di processo (controllo livelli) non correttamente gestite dai sistemi di regolazione, allarme e blocco automatico.
Durante l'avviamento di un impianto di isomerizzazione benzine, dopo una manutenzione generale dello stesso, ci fu il rilascio incontrollato di idrocarburi liquidi da uno scarico di emergenza. La nube di vapori infiammabili fu innescata da un veicolo di servizio presso una baracca mobile utilizzata dal personale di manutenzione ubicata vicino all'impianto. L'esplosione ed il successivo incendio provocò 15 morti, 170 feriti e notevoli danni materiali (vedi fig. 4).

Fig. 4 - Texas City 2005y

MISURE DI PREVENZIONE, PROTEZIONE E MITIGAZIONE PER LA CYBERSICUREZZA

Le possibili vie di attacchi informatici ad una rete industriale 4.0 costituite da internet, chiavetta USB, modem, firewall, sono rappresentate nella figura 5.

Fig. 5 – possibili vie di attacchi informatici ad una rete industriale 4.0



Le possibili misure di prevenzione, protezione e mitigazione per la cybersicurezza adottabili nei sistemi digitali IACS nell'industria di processo sono le seguenti:

- Isolamento da internet (protezione fisica)
- Barriere di isolamento (firewall)
- Controllo porte per chiavette USB
- Controllo accessi a locali contenenti apparecchiature OT
- Procedure di security informatica (fattore umano, ingegneria sociale)
- Gestione password
- Utilizzo firma digitale
- Utilizzo antivirus
- Utilizzo crittografia
- Controllo intrusioni
- Test di penetrazione (software, hardware)
- Sistemi di backup e recupero per desktop, file server
- Gestione degli incidenti (emergenze).

VERIFICHE E CONTROLLI DI CYBERSICUREZZA DEI SISTEMI IACS

I sistemi IACS di controllo, allarme e blocco automatico possono essere verificati valutando il livello di sicurezza SL (Security Level) in accordo alla norma IEC 62443-3-3 (Industrial Communication Networks – Network and System Security–Part 3-3: System Security Requirements and Security Levels).

I valori di sicurezza SL previsti crescenti variano da 1 a 4 e vengono attribuiti dopo una valutazione dei seguenti punti fondamentali della cybersicurezza:

- Controllo identificazione ed antintrusione
- Controllo utilizzo
- Integrità sistema
- Confidenzialità dati
- Limitazione flussi dati
- Risposte all'emergenza
- Disponibilità risorse.

Per gli impianti di processo (Seveso) con pericolo di incidente rilevante l'autorità di controllo inglese (HSE) ha emesso nel 2017 una linea guida relativa alla cybersicurezza dei sistemi IACS già rappresentati nelle figure 1 e 2.

Tale linea guida richiede che il responsabile di un impianto Seveso gestisca il sistema IACS in modo da ridurre al minimo i rischi di cybersicurezza connessi tramite:

- L'identificazione dei pericoli di cybersicurezza
- La definizione dello IACS di impianti
- L'effettuazione di una valutazione dei rischi
- La definizione ed attuazione di contromisure
- L'attuazione ed il mantenimento delle misure di sicurezza (security)
- L'effettuazione di audit, monitoraggio e revisione del sistema di cybersicurezza.

E' quindi richiesto un approccio sistematico per valutare e gradualmente migliorare la cybersicurezza dei sistemi IACS di stabilimento.

CONCLUSIONE

I nuovi rischi addizionali ed emergenti dovuti alla crescente digitalizzazione ed interconnessione dell'industria 4.0 devono essere adeguatamente gestiti con misure di cybersicurezza riguardanti sia l'hardware ed il software sia le procedure di security connesse, ovvero con l'impiego di tecnologie analogiche alternative a quelle digitali per i settori critici dell'industria.
Tali misure dovrebbero far parte del risk management aziendale data l'importanza delle conseguenze di eventuali attacchi (quali esplosioni, incendi, rilasci tossici, inquinamenti) sul piano ambientale, economico e sociale.

BIBLIOGRAFIA

- ISO/IEC 27032 : 2012 Information technology – Security techniques for security- Guidelines for cybersecurity
- HSE 2017 Cybersecurity for industrial automation and control system (IACS)
- RISI 2015 Repository of industrial security incidents
- IEC 62443-3-3 :2013 Industrial communication networks – Network and system security – Part 3-3: System security requirements and security level
- API 2014 State of operational technology – Cybersecurity in the oil and natural gas industry
- DHS 2011 Common cybersecurity vulnerabilities in industrial control systems
- SANS 2017 Securing industrial control systems
- MIT/IPRI 2017 Toward more secure networks for critical sectors