ENERGIA e DINTORNI
IL CTI INFORMA
Rivista del Comitato Termotecnico Italiano – Energia e Ambiente
MAGGIO 2019
News e attualità

Attività a rischio di incidente rilevante

La cyber resilienza dei sistemi di controllo ICS (DCS, SCADA) e di blocco automatico ESD (PLC)

Premessa

La quasi completa digitalizzazione della strumentazione di controllo ICS (DCS, SCADA) e dei sistemi di blocco automatico ESD (PLC) presenti negli impianti petrolchimici, della raffinazione e di altre attività a rischio di incidente rilevante ha reso tali attività, tramite la interconnessione ad internet e ad altri dispositivi mobili (USB,laptop...), vulnerabili ad attacchi informatici esterni/interni, intenzionali/casuali.

Tali attacchi possono portare alla disattivazione generale dei sistemi di controllo e blocco automatico e/o alla manipolazione nascosta degli stessi allo scopo di causare incidenti con comandi a distanza.

Esiste una consistente bibliografia e banche dati di tali attacchi a partire dal malware in Windows (Esplosione oleodotto turco BTC Baku 2008) al virus Stuxnet (Distruzione centrifughe arricchimento uranio Iran 2010) al virus Black Energy (Blocco reti elettriche Ucraina 2016) al virus Triton (Disattivazione sistemi di blocco automatico impianti petroliferi Arabia Saudita 2017).

L'esistenza di diverse linee guida, standard, norme di cybersicurezza di carattere generale/specifico non ha migliorato la situazione.

Modalità degli attacchi cyber e conseguenze

Le modalità di iniezione dei software maligni (malware,virus) nei sistemi sono stati generalmente sia l'utilizzo improprio di chiavette USB durante la manutenzione e/o l'esercizio di ESD sia l'accesso dall'esterno via internet a componenti ICS, soprattutto stazioni di controllo, monitor (HMI).

Nella figura 1 è riportato un esempio di sala controllo con strumentazione digitale.

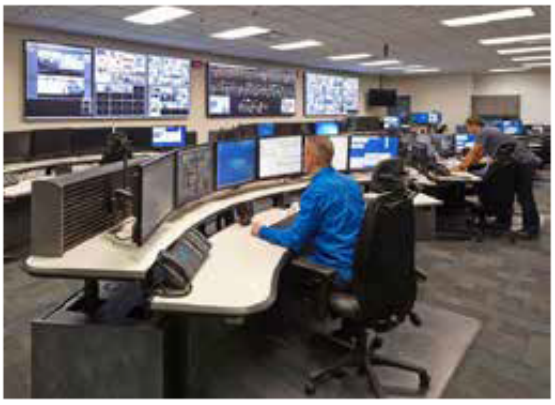
Le conseguenze di tali attacchi cyber ricadono in tre categorie: perdita, negazione, manipolazione come di seguito riportato:

- perdita di vista (loss of view)
- perdita di controllo (loss of control)
- negazione di vista (denial of view)
- negazione di controllo (denial of control)
- negazione della sicurezza (denial of safety)
- manipolazione di vista (manipulation of view)
- manipolazione del controllo (manipulation of control)
- manipolazione dei sensori e degli strumenti (manipulation of sensors and instrtuments)
- manipolazione della sicurezza (manipulation of safety).

Nella figura 2, relativa ai possibili obiettivi di un attaccante(hacker), sono riportate le suddette conseguenze con gravità crescente.

La perdita di vista di un sistema ICS/ESD non consente all'operatore di conoscere lo stato del sistema e comporta il rischio di azioni inappropriate e pericolose. In questi casi molti operatori sono indotti al blocco automatico degli impianti. La perdita di vista è causata dalle interfacce uomo-macchina (HMI) costituita dai

Figura 1 - Sala controllo con strumentazione digitale



monitor, quadri e consolle di controllo infettati dai worms tipo Slimmer e Blaster.
La manipolazione di vista determina decisioni errate da parte dell'operatore, basate su informazioni sbagliate sullo stato del sistema.
La negazione del controllo non consente all'operatore l'accesso ai sistemi critici. La negazione non intenzionale comprende guasti all'hardware, alla rete di interconnessione, errori dell'operatore.
La perdita del controllo non consente all'operatore di attuare azioni prima dell'accadimento di una potenziale situazione catastrofica.

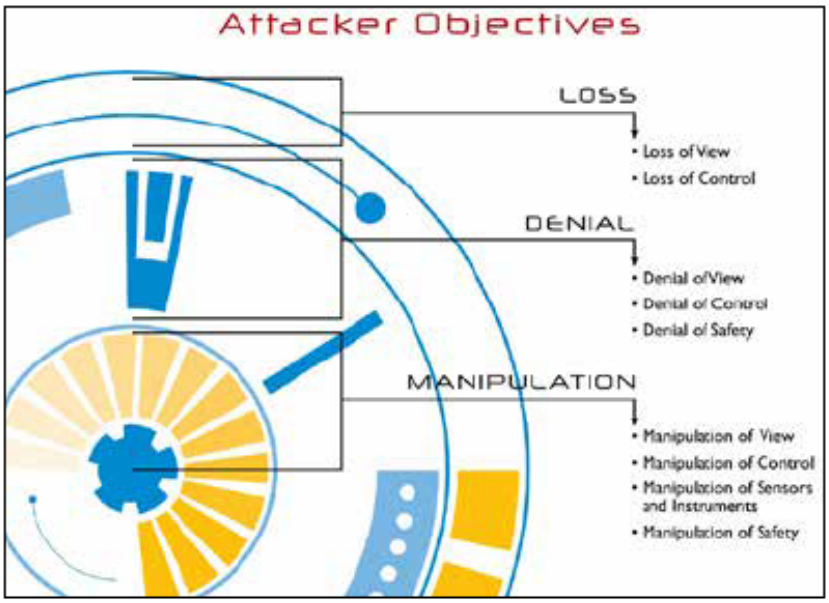


Figura 2 - Possibili obiettivi di un cyber attacco a un sistema ICS e/o ESD

La manipolazione del controllo può avvenire senza alcuna specifica segnalazione all'operatore che spesso può ritenere che si tratti di una anomalia casuale dovuta a guasto.
Malware progettati in modo specifico contro i sistemi ICS e ESD per la manipolazione del controllo sono stati nel tempo i seguenti:
- Stuxnet 2010
- Havex 2014
- Black Energy 2015
- Clashoverride 2016
- Triton 2017.

Gli attacchi non solo non sono aumentati nella relativa frequenza ma anche in severità: dalla distruzione delle centrifughe in Iran da parte di Stuxnet al blocco generale di impianti petroliferi causati dalla messa fuori servizio da parte di Triton dei sistemi di sicurezza di blocco automatico.
La manipolazione del controllo e/o della sicurezza dei sistemi di controllo ICS e di blocco automatico richiede generalmente una sequenza di attacco (Kill Chain) che si sviluppa in 7 fasi:

- Ricognizione (raccolta informazioni ed identificazione obiettivi)
- Preparazione (dell'attacco con messaggio malware)
- Consegna (del malware e lancio dell'operazione)
- Utilizzo (di vulnerabilità per ottenere l'accesso)
- Installazione (di backdoor per consentire l'accesso per un esteso periodo temporale)
- Comando e Controllo (a distanza degli impianti)
- Azioni sugli obiettivi.

Tutte le 7 fasi devono essere attuate con successo per avere un cyberattacco, basta interrompere una fase per impedire l'attacco.

Cyber resilienza dei sistemi ICS e ESD

La cyber resilienza dei sistemi di controllo ICS e blocco automatico ESD è la capacità di resistenza ad un attacco informatico, di recupero e ripristino delle condizioni normali. L'obiettivo principale è quello di continuare ad essere operativi nonostante un attacco e ridurre al minimo i danni.
Le linee guida/ le norme di riferimento più importanti per la cybersicurezza sono quelle elaborate dai seguenti enti/società

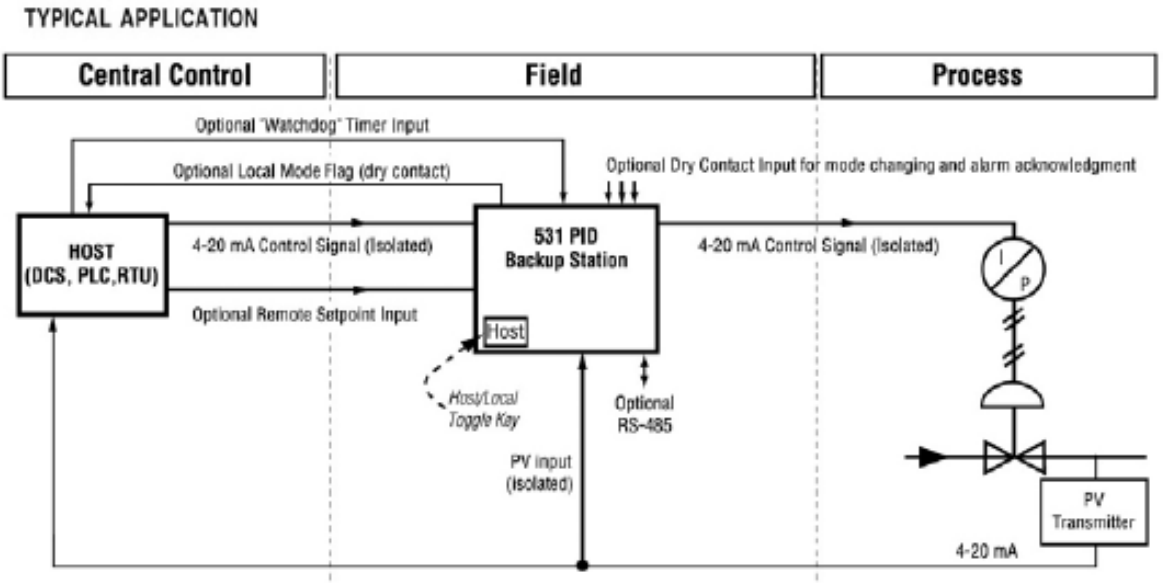


Figura 3 - Stazione di back up di tipo analogico in un sistema ICS

- NIST Linee guida per la security dei sistemi di controllo industriale e per il miglioramento delle infrastrutture critiche
- ISA99/IEC 62443 Norma per la security dei sistemi di controllo ed automazione industriale
- API Std 1164 Norma per la security per i sistemi SCADA.delle pipeline
- LOCKEED MARTIN La metodologia della cyber Kill Chain.

Tali linee guida /norme sono di carattere generale e consentono, con una mirata ed adeguata applicazione un miglioramento della resistenza dei sistemi ICS e ESD agli attacchi informatici senza comunque eliminare la possibilità di futuri eventi.
Si è pertanto sviluppata la cyber resilienza dei suddetti sistemi basata sui seguenti punti fondamentali:

- Ridondanza dei componenti per migliorare l'affidabilità dei sistemi per i guasti di tipo casuale dovuto all'hardware e/o software
- Diversità per i guasti di modo comune dei componenti e del software per i sistemi a microprocessore;
- Indipendenza dei componenti e del software per migliorare l'operatività e l'affidabilità durante l'esercizio.

Considerando il criterio della diversità e dell'indipendenza è possibile aumentare la cyber resilienza dei sistemi ICS e ESD utilizzando componenti di tipo analogico, come di seguito descritto.

- Installazione sui sistemi di regolazione (DCS, PLC, RTU) delle variabili di processo critiche di stazioni di back-up (riserva) di controllo automatico PID di tipo analogico. Tali stazioni ricevono il segnale proveniente dal campo (4÷20 mA) in parallelo alla strumentazione digitale e, in caso di mancanza di quest'ultima, forniscono in tempo reale il segnale di controllo agli attuatori (valvole di regolazione, ecc.) che pertanto non subiscono alcuna perturbazione. L'hardware elettronico analogico di tali stazioni non censente alcuna azione di hackeraggio. Un esempio di back-up di tipo analogico in un sistema ICS è riportato in figura 3.
- Installazione nei sistemi di allarme/blocco ESD critici di soglie di allarme/blocco di back-up (riserva) di tipo analogico hardwired completamente indipendenti dal sistema digitale a microprocessore (PLC) del quale sono una riserva indipendente.

Migliori pratiche di cyber resilienza nelle installazioni critiche

Nell'era del cybercrime la migliore difesa e/o assicurazione può essere l'impiego dell'analogico, come risulta dalla recente esperienza di blocco totale dell'energia elettrica per 80.000 utenti circa per molte ore in Ucraina. Ciò è stato possibile a seguito della interconnessione di ogni cosa dalla centrale termoelettrica al termostato di casa, ad internet. Un attaccante al sistema digitale può mettere fuori servizio tutti i servizi interconnessi in una sola volta. Negli Usa sono state proposte come contromisura l'inserimento di hardware fisico di back up nei punti più vulnerabili delle reti elettriche, installazioni militari ed altre infrastrutture critiche.

L'approccio proposto è che se il sistema principale è di tipo digitale interconnesso, la migliore difesa è un sistema di sicurezza di tipo analogico (non computerizzato e quindi non hackerabile).

Vi è una crescente richiesta da parte degli esperti dello sviluppo sia di nuovi controllori logici di tipo analogico in sostituzione degli attuali PLC sia di regolatori di processo moderno di tipo analogico in sostituzione degli attuali DCS. Con tale approccio è possibile realizzare sia sistemi intrinsecamente cybersicuri sia sistemi aventi una notevole cyber resilienza ad attacchi informatici esterni / interni, voluti / non voluti.

In alcuni settori delle infrastrutture critiche (distribuzione energia elettrica, centrali nucleari, estrazione idrocarburi offshore, ecc) vi è un progressivo ritorno all'impiego di strumentazione moderna di tipo analogico sia per i sistemi di regolazione che di blocco automatico per i punti critici delle installazioni. L'assenza di sistemi computerizzati, e quindi di software, rende tali sistemi intrinsecamente cybersicuri, non avendo alcun accesso a internet né a chiavetta USB e/o altri dispositivi digitali mobili.

I moderni sistemi di sicurezza di tipo analogico hanno le seguenti caratteristiche:

- usano semplici funzioni ed hanno interfacce umane limitate
- non richiedono alcun software
- non hanno problemi di cybersicurezza
- non hanno rapida obsolescenza.

Secondo recenti informazioni alcuni attacchi hacker a raffinerie / petrolchimici hanno avuto conseguenze limitate in quanto i sistemi di controllo ICS e blocco automatico ESD avevano, per le parti critiche, un back up automatico di tipo analogico.

Conclusione

La cyber resilienza dei sistemi di controllo ICS e di blocco automatico ESD può essere migliorata oltre che con l'impiego di quanto previsto dalle norme di cybersicurezza (NIST, ISA/IEC, API) anche con l'impiego di back up (riserva) di tipo analogico.

In alcuni settori delle infrastrutture critiche (distribuzione energia elettrica, centrali nucleari, offshore, ecc.) vi è un progressivo ritorno all'impiego di strumentazione moderna di tipo analogico e di sistemi di sicurezza non computerizzati nei punti critici, che risultano pertanto intrinsecamente cybersicuri.

Acronimi

DCS - Distributed Control System
ESD - Emergency Shutdown System
HMI - Human Machine Interface
ICS - Industrial Control System
PLC - Programmable Logic Controller
SCADA - Supervisor Control and Data Acquisition
USB - Universal Serial Bus

Bibliografia

- NIST - Framework for improving critical infrastructure cybersecurity – 2019
- NIST-SP800-82 - Guide to industrial control system (ICS) security – 2015
- ISA99/IEC62443 - Security for industrial automation and control systems – 2018
- ISA99/IEC62443-4-2 - Technical security requirements for IACS components – 2018
- API-STD 1164 - Pipeline SCADA security – 2016
- LOCKHEED MARTIN - Cyber kill chain methodology – 2015

Domenico Barone
Coordinatore CT 266 "Sicurezza degli impianti a rischio di incidente rilevante"