La Comunicazione - Note, Recensioni e Notizie n. 67
Anno 2023

Cybersecurity delle Operational Technologies (OT): minacce e contromisure

Cybersecurity of Operational Technologies (OT): threats and countermeasures

Roberto Setola♦

♦ Università Campus Bio-Medico di Roma

Sommario

Le Operational Technologies (OT) sono quella parte di sistemi informatici progettate allo scopo di monitorare, controllare e gestire i diversi processi fisici siano essi il semplice sistema di refrigerazione di un frigorifero fino al sistema di controllo della rete elettrica nazionale. I sistemi OT da un lato sono sempre più simili ai sistemi IT condividendone tanto lo hardware che una buona parte dei software, ma dall'altro hanno specifiche peculiarità legate alla tipologia di dati manipolati (pochi byte) e soprattutto agli stringenti tempi di latenza imposti dalla necessità di garantire il rispetto dei vincoli del hard real-time. Tutto questo si traduce in una crescente esposizione di questi sistemi alle minacce cyber e nella difficoltà/complessità di mettere in atto adeguate strategie di cybersecurity. Ciò rende fragili questi sistemi a interferenze cyber che possono paralizzare la funzionalità delle infrastrutture da essi controllati con conseguente impossibilità di erogare servizi anche vitali alla popolazione. Inoltre, vi è anche la possibilità che azioni cyber adeguatamente progettate possano comportare danneggiamenti strutturali a tali infrastrutture trasformando in tal modo un attacco cyber in un evento cinetico con potenziali conseguenze dirette sulla salute delle persone, sull'ambiente e con tempi e costi di ripristino estremamente significativi. In questo articolo dopo una disamina della problematica verranno presentate alcune linee guida utili per la realizzazione di strategia di cyber security per i sistemi OT.

Abstract

Operational Technologies (OT) are that part of IT systems designed for the purpose of monitoring, controlling and managing different physical processes be it the simple refrigerator up to the control system of the national power grid. OT systems are increasingly similar to IT systems by sharing both their hardware and a good part of their software, and they have specific peculiarities related to the type of data manipulated (few bytes) and above all of the stringent latency times imposed by the need to ensure compliance with the constraints of hard real-time. All this translates, on the one hand, to an increasing exposure of these systems to cyber threats and, on the other, to the difficulty/complexity of implementing adequate cybersecurity strategies. This makes these systems fragile to cyber interference that can cripple the functionality of the infrastructure they control resulting in the inability to deliver even vital services to the population. In addition, there is also the possibility that properly designed cyber actions can result in structural damage to such infrastructures thereby transforming a cyber attack into a kinetic event with potential direct consequences on people's health, the environment, and with extremely significant recovery time and costs. This article after an examination of the issue will present some useful guidelines for the implementation of cyber security strategy for OT systems.

Keyword

Industrial control system, SCADA, PLC, DCS; APT, cyber attack, cyber risk.

1 - Introduzione

In praticamente tutti i sistemi di uso quotidiano come gli elettrodomestici, le autovetture, ecc. ma ancora di più quando ci riferiamo alle infrastrutture che erogano servizi “essenziali” alla popolazione come la corrente elettrica, l’acqua, i trasporti ecc. abbiamo che il loro corretto funzionamento è governato da sistemi informatici il cui scopo è quello di monitorarne l’andamento al fine di determinare quando ed in che modo intervenire per garantire che il comportamento del processo sia in linea con le aspettative.

Questi sistemi sono genericamente indicati quali controllori e rappresentano il *core* del sistema di automazione. In estrema sintesi, come schematicamente illustrato nella Figura 1, l'attività del sistema di controllo è quella di leggere costantemente lo "stato" del processo mediante l'impiego di specifici sensori, confrontare il valore misurato da questi sensori opportunamente integrati e manipolati con quelle che sono le grandezze di riferimento desiderate (ad esempio la temperatura all'interno del frigorifero) e in funzione dell'eventuale scostamento fra misura effettiva e grandezza di riferimento comandare specifici attuatori. Gli attuatori sono elementi comandabili dal sistema di controllo ed in grado di modificare il modo in cui il processo si sta sviluppando (ad esempio aumentando la portata di gas o acqua in un tubo, riducendo la velocità di un veicolo, ecc.). L'aspetto caratteristico dei sistemi di controllo è che essi operano quasi sempre in modalità a ciclo chiuso (in inglese *closed loop*) questo significa che le azioni degli attuatori sono tali da indurre modifiche nel processo che a loro volta comportano una alterazione delle grandezze misurate dai sensori.

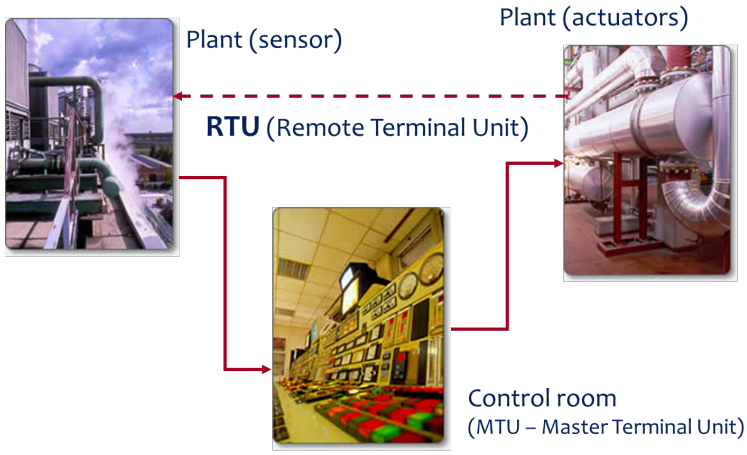

Figura 1 – *Principio di funzionamento di un sistema di controllo automatico a ciclo chiuso*

Ciò implica che il modo di operare del sistema di controllo deve essere compatibile in termini di velocità di esecuzione con quelle che sono le dinamiche proprie del processo controllato.

In altri termini la velocità con la quale il sistema di controllo acquisisce le misure dal campo le elabora e definisce le attuazioni è determinato dal processo fisico sottostante e ciò implica nella stragrande maggioranza dei casi la necessità di avere specifici vincoli sui tempi di esecuzioni indicati come requisiti di ***hard-real time***.

Tale locuzione sta ad indicare che i tempi di ciclo, ovvero il tempo intercorrente fra l'acquisizione di una misurazione e l'esecuzione della corrispondente attuazione, devono garantire in modo assoluto il rispetto di specifici vincoli temporali (che possono variare in funzione del processo da qualche secondo a qualche millesimo di secondo) e non come accade per i normali sistemi IT in modo probabilistico con approcci best-effort che caratterizzano il tempo di risposta in termini di valori medi. Nel caso di sistemi OT è fondamentale garantire che anche nel wrost-case (cioè nel peggiore degli scenari) il tempo massimo (e non quello medio) sia inferiore al vincolo temporale.

Inoltre, i requisiti peculiari dei sistemi di automazione non riguardano solo i tempi di esecuzione ma anche la necessità di garantire determinismo nella risposta, life-time dell'ordine delle decine di anni e necessità di operare 24 ore su 24 per 11 o 12 mesi l'anno in continuazione. Ciò ha comportato alcune differenze fra i sistemi utilizzati nell'automazione di processo e i normali sistemi IT sintetizzate nella tabella 1.

Tabella 1. Principali differenze fra i sistemi IT e i sistemi impiegati nell'ambito dei sistemi di automazione.

Aspetto	Corporate IT	Controllo di Processo
Anti virus	Ampiamente utilizzato	In molte situazioni, impossibile da implementare
Life-time	3 - 5 anni	5 – 20 anni
Patching	Frequentemente (anche su base giornaliera)	Dilazionata nel tempo (richiesta certificazione del fornitore e interruzione processo produttivo)
Vincoli temporali	Ritardi accettabili	Hard real time
Disponibilità	Accettabili blocchi operatività in determinati momenti (di notte e durante i festivi)	Operano in molti casi 24/7/365

Aspetto	Corporate IT	Controllo di Processo
Determinismo	Accettabile che in alcune situazioni il sistema possa rispondere in modo non prevedibile	Fondamentale che la risposta a determinati ingressi sia sempre la medesima
Tipologia dati scambiati	File strutturati	Messaggi di pochi byte
Numero di dispositivi connessi	Pochi	Molti

Queste peculiarità hanno comportato che nel corso del tempo i sistemi dedicati all'automazione abbiano seguito una evoluzione in parte diversa dai normali sistemi IT con lo sviluppo di hardware e software peculiare.

Nel maggio del 2021 i cittadini americani hanno avuto una prova concreta di quelle che potrebbero essere le conseguenze di un'azione cyber contro un sistema OT, allorquando un malware creò la paralisi del più importante oleodotto che trasporta i carburanti dalle raffinerie del Golfo del Messico a tutte le città della costa orientale, Washington e New York incluse [1]. Il blocco di questo oleodotto di proprietà della Colonial Pipeline si è protratto per 6 giorni comportando problemi agli approvvigionamenti di benzina (con oltre il 75% delle pompe rimaste senza carburanti), impennata dei prezzi dei carburanti, panico e disorientamento nella popolazione.

2 – Operational Technologies

I sistemi informatici utilizzati per l'automazione sono indicati con la sigla ***OT – Operational Technologieis*** per distinguerli dai normali sistemi IT. In realtà nel corso degli anni tali sistemi hanno avuto diverse denominazioni a partire dalla generica locuzione **Process Control** a quella più estensiva di **Industrial Control System (ICS)**. In molti contesti l'intero sistema di controllo è indicato usando il termine **SCADA** (che, come vedremo, è in realtà una sua componete). Attualmente oltre all'acronimo OT si sta diffondendo anche l'utilizzo del termine ***CPS – Cyber-***

Physical System che meglio enfatizza la stretta interazione che c'è in questi sistemi fra la dimensione cyber e quella fisica.

Quando si parla di sistemi di automazione in realtà ci si riferisce ad un insieme di tecnologie che possono essere rappresentate in modo gerarchico tramite il così detto *modello di Purdue* [2]. Tale modello prevede una organizzazione a 6 livelli da zero a cinque che divide quelle che sono le componenti tipiche di un sistema di automazione (livello 0 – 3) da quelli che sono i sistemi propri della corporate IT (livello 4 e 5). Sebbene come tutte le classificazioni è arbitraria, l'utilizzo del modello di Purdue aiuta a comprendere meglio la complessità e quelli che sono gli elementi più significativi di una architettura OT. Il modello di Purdue è illustrato schematicamente nella Figura2.

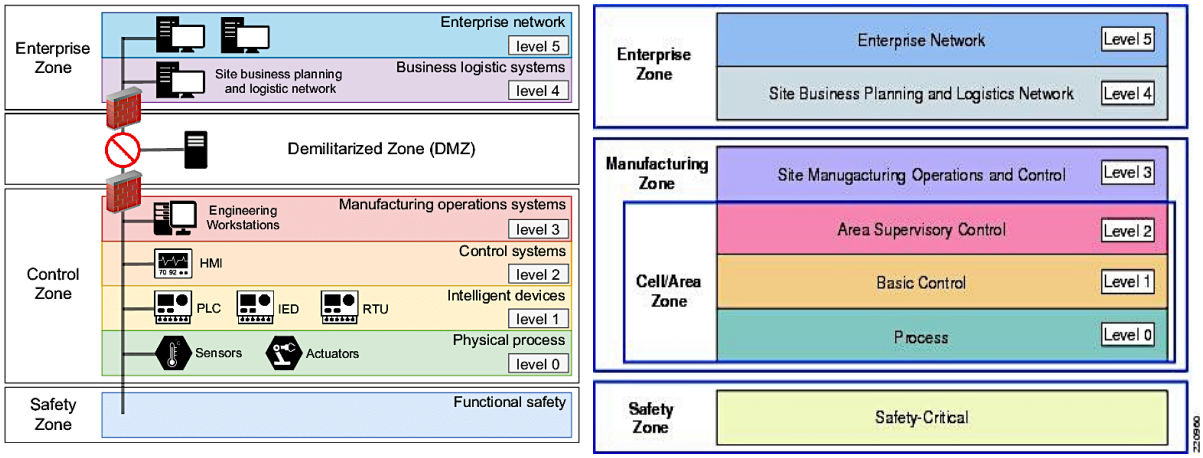

Figura 2 –*Purdue model per la gerarchizzazione dei sistemi OT.*

2.1 – Livello 0: Livello di Campo (Field Level)

Come illustrato nella Figura 2, il livello 0 è costituito dagli elementi del sistema di automazione direttamente connessi con il processo, ovvero dai sensori e dagli attuatori. Sebbene originariamente questi elementi non fossero dotati di una propria capacità elaborativa autonoma, oggigiorno essi sono dotati di micro-processori in grado di effettuare attività di diagnostica sulle misure acquisite oltre che sul dispositivo stesso.

Per quel che riguarda gli attuatori a questo livello troviamo i controlli di asse, ovvero il controllo per ciò che riguarda il funzionamento basilare del dispositivo (ad esempio l'inseguimento di un profilo di velocità da parte di un motore).
Questo cambiamento ha fatto sì che ai collegamenti in analogico (generalmente su circuiti a ±5V o a 4-20mA) si siano sostituiti comunicazioni che utilizzano protocolli di fieldbus (il più diffuso dei quali è sicuramente il modbus).

2.2 – Livello 1: Controllori di Cella (Intelligent Devices)

A livello 1 troviamo gli elementi che hanno il compito di chiudere i loop a livello di cella (ovvero di un insieme di apparecchiature che devono cooperare per l'esecuzione di uno specifico task). Sono sistemi che ricevono dai livelli superiori i set-point e determinano i comandi da impartire agli attuatori sulla base delle attuali misure provenienti dai sensori. Sono sistemi che operano a ciclo continuo svolgendo un loop di controllo che prevede le attività di misura-controllo-attuazione. Essi sono caratterizzati per operare con stringenti vincoli temporali. Nella maggior parte dei casi tale attività è svolta dai ***PLC (Programmable Logic Controller)*** che sono sistemi hardware specificatamente progettati per le esigenze del controllo industriale. I PLC sono ampiamente diffusi grazie alle loro caratteristiche di modularità e robustezza che li rendono particolarmente adatti ad operare all'interno di contesti industriali. Essi in genere non prevedono una interfaccia per l'operatore, se si esclude la presenza di led che segnalano lo stato degli ingressi/uscite binarie, ed utilizzano linguaggi di programmazione dedicati il cui più diffuso è il ***Ladder***.

2.3 – Livello 2: Controllori di Area (Control System)

Il livello 2 rappresenta un livello intermedio fra il controllo di cella ed il controllo di impianto ed il suo scopo è il coordinamento fra le attività di più celle. Tale livello è presente in genere soprattutto in impianti dispersi sul territorio ovvero in quei casi in cui uno stabilimento è organizzato in isole che gerarchicamente integrano più cella.

In genere essi hanno anche delle interfacce operatore HMI (Human Machine Interface) mediante le quali sono in grado di illustrare lo stato di funzionamento dei diversi sistemi e ricevere specifici comandi.
Da un punto di visto architetturale a questo livello possiamo trovare sia dei PLC che degli SCADA (illustrati nel paragrafo sezione sottostante).

2.4 – Livello 3: Controllo di Impianto (SCADA/DCS)

In questo livello troviamo i sistemi che servono per la supervisione e il controllo di un impianto. Qui troviamo in particolare quelli che sono i DB dedicati alla raccolta e memorizzazione degli eventi e delle misure (detti in genere *Historian*), l'interfaccia con gli operatori (*HMI Human Machine Interface*), i moduli per la gestione degli allarmi, dei trend, delle ricette e di tutto ciò che è connesso con le esigenze di analytics. Questo è il dominio dei sistemi ***SCADA (Supervisor Control and Data Acquisition)*** che integrano tutte queste funzioni in un ambiente unico che consente il monitoraggio dell'impianto, ne offre una rappresentazione tramite sinottico agli operatori, consente di gestire allarmi con diversi livelli di priorità, di attuare la produzione mediante ricette dove sono specificati gli input e le tipologie di lavorazione da svolgere per ogni specifica lavorazione, gli strumenti per l'analisi dei trend, dei consumi, dei guasti e quant'altro necessario per la corretta gestione dell'impianto [3]. A questo livello negli impianti di processo possiamo trovare anche i ***DCS (Distributed Control System)*** che hanno funzioni analoghe agli SCADA sebbene siano storicamente dedicati al controllo di processo.

3 – Cambio di scenario

Fino alla fine degli anni '80 i sistemi OT erano relegati all'interno degli impianti industriali con sostanzialmente nessuna interazione con gli altri sistemi IT aziendali. Questo era dovuto ad un insieme di cause legate ad un modello di produzione rigida ma soprattutto al fatto che questi sistemi hanno avuto una evoluzione autonoma rispetto ai normali sistemi IT con la conseguenza che tali sistemi utilizzavano hardware, protocolli di comunicazione e software specifico. Tale aspetto risulta particolarmente evidente andando a considerare quelli che sono

i linguaggi di programmazione per i PLC codificati nella norma IEC 61131 [4]. In particolare il linguaggio Ladder che è ancor oggi il più diffuso per la programmazione di questi dispositivi evidenzia in modo chiaro i legami storici con quelli che erano gli schemi elettrici impiegati per la progettazione degli impianti a relè (si veda Figura 3).

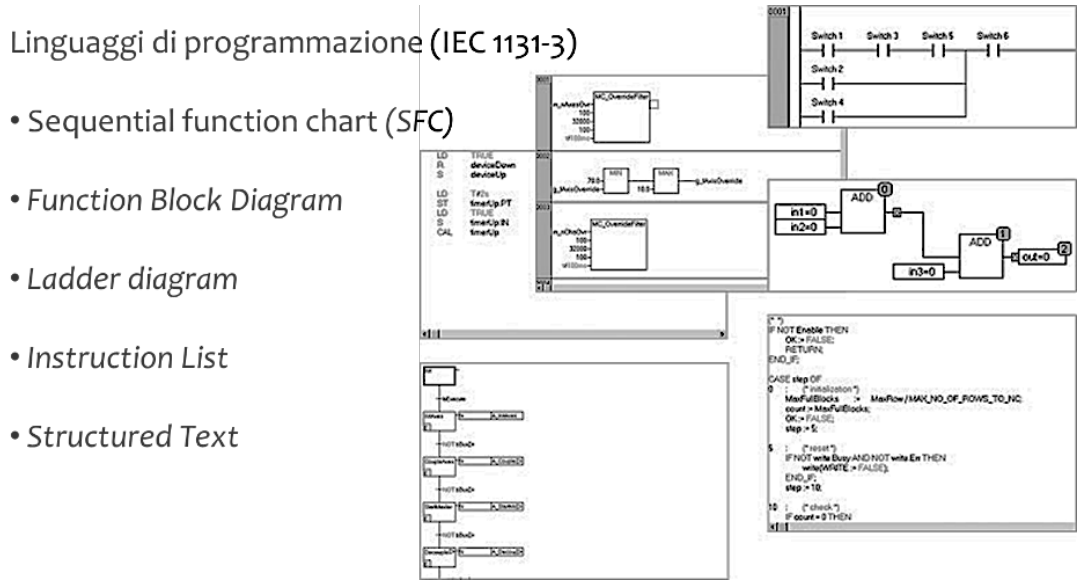

Figura 3 *–Linguaggi di programmazione per PLC come codificati dalla IEC 61131-3.*

Questa sostanziale autonomia dei sistemi OT ha fatto sì che essi si sviluppassero tenendo in conto in modo quasi esclusivo gli aspetti di safety tralasciando le problematiche di security alla luce delle peculiarità dei sistemi OT e del loro sostanziale isolamento.

A ridosso del passaggio del millennio lo scenario cambia in modo significativo sulla spinta della necessità del business di avere una maggiore integrazione fra sistemi IT e OT per attuare forme di produzione e gestione maggiormente dinamiche atte a supportare una produzione maggiormente flessibile e a piccoli lotti e ad adottare paradigmi quali il just in time.

A ciò si aggiunge anche il mutato scenario che ha visto l'abolizione dei grandi monopoli nazionali a favore di soluzioni di mercato dove diversi operatori si sono trovati a dover gestire, con strategie di cooperazione/concorrenza, porzioni di infrastrutture sostanzialmente unitarie dal punto di visto del processo fisico.

A queste motivazioni si sono aggiunte alcune di carattere più prettamente tecnologico connesse con la necessità di sostituire rapidamente i sistemi legacy per poter gestire il millenium bug (ovvero il problema della data codificata con 6 cifre e le possibili incoerenze che si potevano generare con il passaggio di millennio).

Tutto questo ha comportato una rapida adozione di protocolli e hardware off-the-shelf propri del mondo IT all'interno dei sistemi OT. Tale introduzione, oltre a innegabili vantaggi in termini di abbattimento dei costi, introduzione di nuove funzionalità, ecc., ha esposto questi sistemi ai rischi cyber.

Occorre rilevare che sebbene le minacce cyber siano sostanzialmente le stesse di quelle presenti nei sistemi IT, non tutte le modalità di difesa possono essere replicate anche in questo dominio [5]. Ciò è dovuto in primo luogo al fatto che per i sistemi OT il requisito di disponibilità è quello definitamente più rilevante con conseguenza che tutte quelle soluzioni, come gli antivirus, che implicano la presenza di tempi di latenza non definibili a priori risultano inapplicabili.

Per altro, come illustrato nella Tabella 1; il life time di questi sistemi è decisamente più lungo di un normale sistema IT essendo in genere abbinato al tempo di attività del processo di cui funge da controllare. Da qui la necessaria presa di coscienza che in alcune situazioni il processo di patching risulta impossibile in quanto il prodotto è abbandonato per obsolescenza dal fornitore (ancora oggi esistono processi industriali i cui sistemi OT si basano su sistemi operativi obsleti come Windows NT). Ma anche quando non siamo in presenza di situazioni così estreme, il già citato requisito di disponibilità unito al fatto che molti processi industriali operano a ciclo continuo h 24 impone la necessità per evitare fermi di produzione di differire l'istallazione delle patch nel periodo di fermo impianti (che in genere avviene una volta l'anno).

Per altro le significative implicazioni legate al potenziale non corretto funzionamento di un sistema OT impongono di richiedere che tali sistemi siano certificati e, più in generale, prima di una loro adozione in linea è necessario eseguire tutta una serie di verifiche. Ciò si traduce in una significativa dilatazione dei tempi di patching.

Mentre in un normale sistema IT l'utilizzo di crittografia e tecniche di firma digitale rappresentano soluzioni adeguate per garantire l'integrità dei dati e l'autenticazione della fonte, il loro utilizzo in ambito OT si scontra con il fatto che soprattutto ai livelli 0-1 le comunicazioni sono attuate mediante pacchetti di pochi byte per i quali l'utilizzo di tecniche di firma digitale comporterebbe un significativo aumento di occupazione di banda con conseguente violazione dei requisiti di latenza. Per altro i dispositivi in campo (livello 0) hanno in genere limitate capacità computazionali per cui l'implementazione di schemi di firma digitali risulta in alcuni casi impossibili ed in altri impattanti in modo significativo sulla latenza del tempo di ciclo.

4 – La minaccia Cyber

Oltre alle differenze per ciò che riguarda le strategie di difesa, occorre evidenziare che un'azione cyber avverso un sistema OT può avere conseguenze decisamente diverse e, per molti aspetti più drammatici che un "normale" evento IT. Come evidenziato in modo puntuale nella relazione dell'Intelligence al parlamento del 2016 un'eventuale azione cyber contro un sistema OT può indurre "*potenziali impatti di ordine non solo economico ma anche cinetico*" [6]. Ovvero che un evento cyber può modificare il processo fisico controllato dal sistema OT al punto che esso può creare conseguenze negative dirette per la salute delle persone, potenziali impatti sull'ambiente (sversamento di inquinanti) se non addirittura la distruzione fisica di componenti e apparecchiature. Aspetto quest'ultimo che ha immediate implicazioni sui tempi di ripristino dell'operatività che si dilatano su orizzonti dell'arco delle settimane se non dei mesi.

Una idea di cosa vuol dire fare un attacco cyber ad un sistema OT è dato dal progetto Aurora del governo americano che ha dimostrato nel 2009, con tanto di video reperibile in rete, come una azione cyber sia in grado di indure la distruzione fisica di un gruppo elettrogeno da 17 tonnellate. Ancora più emblematico è stato il malware Stuxnet che nel 2010 è stato in grado di portare alla distruzione oltre 900 centrifughe per l'arricchimento dell'uranio nel sito atomico di Natan in Iran [7].

Questi due episodi sono considerati dagli studiosi come i due capisaldi che hanno dato contezza dell'effettivo pericolo che i sistemi OT corrono rispetto alla minaccia cyber. Il progetto Aurora evidenzia, infatti, che vi è da parte di una pluralità di entità governative un concreto interesse, oltre che una effettiva capacità di manipolazione, verso strumenti e metodologie per utilizzare quali target di cyber-weapon i sistemi OT. D'altro canto, Stuxnet ha dimostrato che l'idea di usare cyber-weapon non è solo teorica, ma effettiva, pratica, concreta ed al tempo stesso si caratterizza per la estrema difficiltà di attribuzione dell'azione ai suoi esecutori. Stuxnet viene considerato la prima cyber-weapon nella storia dell'umanità.

Dopo Stuxnet ci sono stati tutta una serie di episodi [8], molti dei quali a contorno di situazioni geopolitiche complesse, fra le quali possiamo ricordare:

- Nel dicembre del 2015 e del 2016 dei malware, nello specifico BlackEnergy3 (2015) e Crashoverride (2016), sono stati in grado di generare un blackout elettrico di alcune ore in un'ampia regione dell'Ucraina. Evento che va letto nell'ambito delle tensioni esistenti all'epoca fra Russia e Ucraina per il controllo della Crimea;
- Nel 2017 il malware Triton agendo direttamente sul sistema ***SIS (Safety Instrumental System)***, ovvero quella porzione di sistema OT – generalmente isolata dal resto della rete – destinata a prevenire il verificarsi di eventi catastrofici in uno stabilimento (è lo strato rappresentato nella Figura 2 al di sotto del livello 0), ha indotto lo shut-down della più importante raffineria in Arabia Saudita. Evento che va ad inserirsi nelle azioni a contorno della guerra civile in Yemen.
- Nel 2020 in pieno Covid e durante un periodo di siccità vi è stato un cyber attacco al sistema di controllo della rete idrica nella valle del Giordano il cui obiettivo era quello

di manipolare le letture dei livelli di cloro per indurre le autorità a dichiarare non potabile l'acqua. Azione attribuita dagli Israeliani ad attività condotte da soggetti contigui con il regime iraniano.

In realtà, nonostante le conseguenze sono state sostanzialmente simili a quanto occorso al sistema di Colonial Pipeline di cui si è accennato nel primo paragrafo, questi attacchi differiscono in modo significativo dal caso americano, sia perché la matrice non è criminale estorsiva, ma anche per le modalità di attuazione.

Conviene per meglio chiarire questo concetto evidenziare che il sabotaggio ad un sistema OT può essere conseguenza di due diverse strategie.

La prima possiamo definirla come ***sabotaggio "accidentale***", ed è il caso di Colonial Pipeline. Si ha questo scenario quanto una azione cyber perpetrata contro il sistema IT si propaga, potremmo dire accidentalmente, fino a interferire con il sistema OT. Quest'ultimo riscontrando anomalie ed essendo progettato con il principio del "safety first" mette in atto in modo automatico misure di protezione, come lo shut-down, per prevenire un maggior danno alle persone, all'ambiente e agli impianti. È in qualche modo un effetto secondario, il più delle volte non previsto e non voluto dagli attaccanti ed è diretta conseguenza di una eccessiva contiguità fra rete IT e rete OT.

La seconda classe, che diremo di ***sabotaggio "intenzionale"***, mira invece a colpire in modo esplicito i sistemi OT. Anche in questo caso in genere l'azione parte dalla rete IT per poi guadagnare l'accesso alla rete OT. Qui l'obiettivo può essere sia la paralisi dell'impianto, ma anche alternarne il funzionamento se non addirittura portare lo stesso ad operare in condizioni estreme fino a indurre un danneggiamento strutturale. Ovvero trasformare un evento cyber in un vero e proprio evento cinetico. Per fare ciò il malware utilizza vulnerabilità IT per penetrare nella rete della vittima e acquisire le credenziali per poter operare, ma poi, ed è questo l'aspetto che fortemente caratterizzante questa tipologia di azioni, la vera azione è attuata **utilizzando comandi legittimi**. In altri termini il malware utilizza le vulnerabilità IT per penetrare nella rete mentre per attuare la strategia di attacco utilizzando comandi sintatticamente corretti attuati in una sequenza tale da portare il processo in una condizione

critica. Per riuscire in questo intento il malware deve avere una adeguata conoscenza del processo e della sua architettura di controllo che può essere acquisita ricorrendo ad Insider, ad azioni di spionaggio o attraverso un monitoraggio "intelligente" della rete stessa con tecniche di APT (Advance Persist THreat) che però richiedono una lunga permanenza "dormiente" all'interno della rete del target.

5 – Contromisure

Come per i sistemi IT, non esite la soluzione perfetta per garantire la sicurezza di un sistema OT. Questo sia perché il rischio zero non esiste, perché le minacce evolvono nel tempo ma soprattutto perché l'architettura del sistema OT è fortemente legata a quello che è il sottostante processo da controllare e quindi ogni soluzione deve essere adattata e specificata per la singola realtà.

Come per ogni strategia di cyber security, anche per i sistemi OT la strategia deve essere organizzata in termini di **persone**, **procedure** e **tecnologie**. Dove l'ordine non è causale ma vuole sottolineare che l'elemento di maggior vulnerabilità è e rimane il fattore umano che è alla base di quasi il 90% di tutti gli eventi cyber. Le persone, adeguatamente formate e rese edotte delle minacce e di quelle che sono le contromisure da adottare, possono operare seguendo procedure che devo conciliare le esigenze operative con quelle di sicurezza. Mi piace sottolineare che a mio avviso le procedure di security non devono essere "**esimenti" -based**. Ovvero non serve un manuale voluminoso di procedure scritto in linguaggio legalmente esatto creato cercando di normare ogni singolo aspetto con l'obiettivo, il più delle volte implicito, di de-responsabilizzare l'estensore delle procedure a danno dell'esecutore. Ma è preferibile avere un documento che sia un canovaccio di principi ispiratori lasciando al personale, ribadisco adeguatamente formato, di implementare la soluzione adeguata sulla scorta della situazione effettiva. In altri termini usando un approccio **KISS *Keep It Simple and Shorter*** che non solo responsabilizza e valorizza il ruolo del singolo operatore, ma permette una migliore

conoscenza delle procedure e una loro adozione in modo flessibile, intelligente e adattativa alla situazione in contrapposizione all'idea di avere procedure esatte, rigide e "passive".

Nell'ambito delle procedure rivestono specifica importanza quelle legata al processo di gestione dei prodotti OT che includono:

- la fase di acquisizione in cui la componente di cyber-security deve essere introdotta all'interno dei bandi di gara [9];
- il processo di patching sia in termini di obblighi in capo al fornitore, sia dal punto di vista di come il processo è attuato alla luce delle tempistiche, peculiarità e segregazioni della rete OT;
- gli aspetti di maintenance sia con riferimento agli accessi in situ di personale esterno all'azienda, ma soprattutto per tutto quello che riguarda le modalità di manutenzione e aggiornamento dei sistemi da remoto;
- il decommissioning in quanto eventuali informazioni inavvertitamente lasciate memorizzate all'interno di apparecchiature dismesse potrebbero essere utilizzate da soggetti terzi per acquisire quelle informazioni utili per realizzare azioni mirate (sabotaggio intenzionale).

Volendoci soffermare sulla dimensione più prettamente tecnica la realizzazione di una adeguata strategia di cyber security deve basarsi sui due principi basilare dello **Zero-Trust** e del **Defense in Depth** [10].

L'approccio Zero-Trust sintetizza il proverbio "*fidarsi è bene, ma non fidarsi è meglio*" che evidenzia come seppure in alcuni contesti dare per scontate alcune ipotesi possa far aumentare l'efficienza di un processo, il più delle volte tali assunti impliciti possono esporre il sistema a rischi significativi.

Come sottolineato sia dalla SP-800-82 [11] che dalla ISA99/IEC62443 (le due principali linee guida per la cyber security nel settore OT) il primo aspetto da curare è la segregazione fra la rete IT e la rete OT alla luce della maggiore criticità e vulnerabilità di quest'ultima.

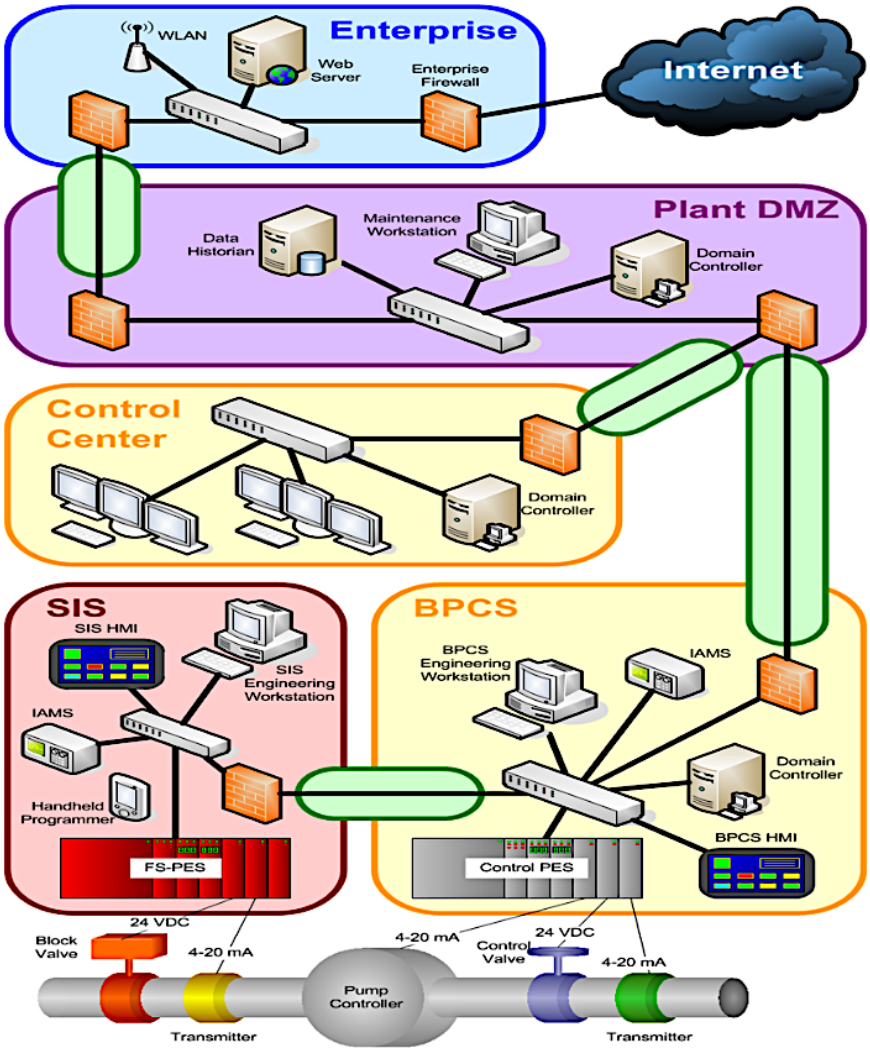

Figura 4 –Segregazione rete OT (fonte www.isa.org/isa99/).

Come evidenziato nella Figura 4 tale segregazione andrebbe attuata creando una DMZ fra la rete aziendale e quella OT. Tale DMZ dovrebbe essere protetta da una coppia di firewall, eventualmente ridondati per garantire continuità operativa, ma soprattutto differenti fra loro per aumentare la robustezza complessiva del sistema (seppur a scapito di maggiori costi di gestione). Lo standard ISA va anche oltre suggerendo di realizzare segregazioni anche a livello della rete OT in relazione al diverso grado di criticità del singolo segmento.

Andando, cioè, a creare delle zone caratterizzate dal medesimo livello di sicurezza (trust) che comunicano fra di loro mediante single-point-of-contact (nello standard denominati *conduit*) adeguatamente monitorati da dispositivi di controllo. Lo stesso standard suggerisce, inoltre, che il flusso informativo fluisca esclusivamente dal livello a sicurezza maggiore verso quello a sicurezza inferiore e mai il viceversa. Purtroppo, non sempre è possibile segmentare la rete OT a causa della necessità di flussi informativi fra i diversi dispositivi, ma soprattutto sebbene la stragrande maggioranza delle informazioni abbia una direzione preferenziale (dal campo verso la rete IT) esistono tutta una serie di situazioni, dalla necessità di riconfigurare la produzione, la gestione delle patch, la manutenzione, ecc. che rendono necessaria la presenza di flussi bi-direzionali. Di conseguenza è fondamentale avere efficaci strumenti di ***Perimeter Security***. Tali sistemi dovranno avere basse latenze e capacità di monitorare anche i protocolli OT quali, ad esempio il modubs, il profibus, il cambus, etc.

Il mondo OT è maggiormente stabile rispetto al IT e questo consente di attuare con maggiore facilità politiche di **Least-Privilege** e di **Deny-by-Default**, ovvero di identificare come corretti solo quei protocolli di comunicazione effettivamente utilizzati, ed autorizzare solo i flussi fra specifici indirizzi/porte nonché l'utilizzo di solo alcuni applicativi (**whitelisting**). Per l'implementazione di queste strategie risulta indispensabile avere sistemi di **asset inventory** in grado di mantenere costantemente aggiornata la lista dei dispositivi e gli applicativi presenti nel sistema.

Un aspetto da curare con attenzione è quello dell'autenticazione; aspetto questo complesso in una ambiente dove coesistono anche migliaia di dispositivi, molti dei quali dispersi in ambienti facilmente accessibili anche da soggetti terzi. Ciò implica la necessità di prestare molta attenzione a quelli che sono gli aspetti di **sicurezza fisica** che è da considerare la prima barriera (ed in alcuni casi anche l'unica) di sicurezza perimetrale dal basso, ovvero per minacce che risalgano dai livelli 0 o 1 verso i sistemi SCADA.

Questo anche perché molti di questi dispositivi, per ragioni di costo, sono dotati di limitate capacità computazionali rendendo di fatto estremante problematico l'utilizzo di tecniche robuste di autenticazione.

Queste considerazioni, unitamente alla costatazione che a differenza di quanto suggerito dagli standard ci sono situazioni in cui non è possibile per problemi di latenza far passare tutti i flussi attraverso i firewall, suggeriscono l'utilità di attuare anche un adeguato livello di **network security** istallando sistemi di **IDS** e di ***anomaly detection***. Questi sistemi, se opportunamente addestrati e configurati, sono in grado di riconoscere situazioni potenzialmente pericolose operando senza introdurre latenze nel sistema di controllo. Occorre però evidenziare che i sistemi IDS rule-based e signature-based soffrono dell'incapacità di individuare attacchi 0-day (oltre che della necessità di un loro costante aggiornamento con conseguente necessità di adeguate procedure per accedere dalla rete OT ai repository con le informazioni di aggiornamento). D'altro canto i sistemi di anomaly-based soffrono di un elevato rate di false-positive. In questo contesto l'utilizzo di applicazioni di intelligenza artificiale e soprattutto lo sviluppo di soluzioni anomaly detection che considerano la natura cyber-physical del sistema potranno portare interessanti risultati [12].

6 – Conclusioni

Gli ambienti utilizzati per il monitoraggio ed il controllo dei processi "fisici", le così dette Operational Technologies (OT), hanno avuto fino alla fine degli anni '80 uno sviluppo parallelo ed autonomo rispetto a quello dei sistemi IT. L'impiego di tecnologie, protocolli e sistemi proprietari, oltre alla quasi totale segregazione fisica di questi sistemi rispetto ai sistemi IT aveva reso poco rilevante per i sistemi OT le problematiche legate alla cyber-security.

Le spinte legate al cambio di paradigma nel mondo produttivo con l'adozione di strategie basate, ad esempio, sul just-in-time, unitamente alla globalizzazione dei mercati da un lato ed alla urgenza di sostituire i sistemi legacy affetti in larga parte dal millenium bug, hanno profondamente modificato questo assunto. I sistemi OT oggi risultano connessi con i sistemi IT aziendali ed utilizzano in larga parte componenti off-the-shelf e software sviluppati per il mondo IT. Questo espone di fatto i sistemi OT ai "classici" rischi di cyber security sebbene alcune loro peculiarità rendano molto più complessa l'adozione delle misure di protezione e mitigazione.

L'aspetto di maggiore criticità risiede, però nelle potenziali conseguenze che possono generarsi da un attacco cyber ad un sistema OT. Infatti, la contiguità dei sistemi OT con macchinari e processi produttivi può trasformare l'evento cyber in un evento cinetico con conseguenze, anche significative, sulla salute delle persone, la sicurezza dell'ambiente e l'integrità strutturale degli impianti.

Diversi episodi, a partire dall'esperimento condotto negli Stati Uniti con il programma Aurora (2009) e il malware Stuxnet (2010), hanno evidenziato l'effettiva possibilità di realizzare questi attacchi. La cui peculiarità riesce nel fatto che essi sfruttano vulnerabilità software per penetrare nella rete IT (quasi sempre con la involontaria complicità di operatori umani non adeguatamente formati) ma utilizzano poi comandi legittimi per condurre deliberatamente il sistema fisico a operare in modo difforme se non addirittura a porlo in condizioni critiche fino ad indurne la rottura meccanica. Questa modalità di attacco implica, fortunatamente per noi, la necessità da parte dell'attaccante di avere molte informazioni sul funzionamento del processo fisico e del relativo sistema OT che devono essere acquisite tramite insider oppure, come occorso con gli attacchi eseguiti in Ucraina nel 2015 e 2016, mediante sistemi "dormienti" che hanno analizzato su un significativo arco temporale le modalità operative del sistema OT per individuare i legittimi comandi da attuare. Questo limita l'interesse per queste azioni solo a soggetti state-sponsored che hanno capacità, mezzi e tempi per pianificare con ampio anticipo azioni tramite vere e proprie cyber-weapon.

Abbiamo però assistito all'intensificarsi di altre tipologie di azioni cyber contro i sistemi OT, che potremmo definire di sabotaggio accidentale, come il caso del blocco dell'oleodotto americano Colonial Pipeline (2021). In questo caso, come in un crescente numero di casi similari, una non corretta segregazione fra sistemi IT e sistemi OT ha consentito a un ransomware di infettare la rete OT inducendo l'intervento dei sistemi di protezione degli impianti con conseguente blocco degli stessi. Questi episodi evidenziano che non vi è ancora una adeguata percezione del rischio cyber per i sistemi OT ed è pertanto fondamentale operare a tutti i livelli per far crescere sia la awareness che le competenze per contrastare la minaccia cyber. Aspetto questo che si scontra, oltre che con la ben nota carenza di competenze in cyber security, anche con il fatto che per la gestione della cyber security nei sistemi OT occorrono non solo competenze di informatica ma anche quelle di automazione industriale e sono davvero pochi i percorsi formativi rivolti a queste figure professionali.

Se poi osserviamo il crescente numero di attacchi attribuibili a soggetti state-sponsored, che probabilmente permarranno, se non aumenteranno, anche dopo la conclusione conflitto Russo-Ucraino, appare urgente l'adozione di azioni mirate a migliorare la sicurezza di questi sistemi. In questo quadro il perimetro nazionale di sicurezza cibernetica rappresenta sicuramente un elemento rilevante, così come la NIS. Tali norme vanno nella direzione di imporre obblighi alle diverse società a partire da quelle di maggiore rilevanza alla luce delle potenziali conseguenze che un evento cyber condotto avverso i loro sistemi OT potrebbe avere per il Paese. Occorre però affiancare a queste azioni iniziative rivolte verso la PMI che sulla spinta di cogliere i benefici legati alla Trasformazione Digitale rischiano di estendere la loro superficie di esposizione ad attacchi cyber senza avere la contezza dei rischi né le conoscenze e gli strumenti per contrastare tali minacce.

9 - Bibliografia

[1] Bing C., & Kelly S., "Cyber attack shuts down US fuel pipeline", Biden briefed. Reuters, 2021

[2] Williams T.J. "The Purdue enterprise reference architecture". Computers in industry (24.2-3: 141-158), 1994.

[3] Yadav G., & Paul K., "Architecture and security of SCADA systems: A review". International Journal of Critical Infrastructure Protection, (34, 100433), 2021.

[4] Tiegelkamp M., & John K.H., "IEC 61131-3: Programming industrial automation systems" (Vol. 166). Berlin/Heidelberg, Germany: Springer, 2010.

[5] Knowles W., Prince D., Hutchison D., Disso J.F.P., & Jones K., "A survey of cyber security management in industrial control systems". International journal of critical infrastructure protection, (9, 52-80), 2015.

[6] Relazione sulla politica dell'informzione per la sicurezza, (https://www.sicurezzanazionale.gov.it/sisr.nsf/relazione-annuale/relazione-al-parlamento-2016.html), 2016

[7] Kushner D., "The real story of Stuxnet", IEEE Spectrum, (50(3), 48-53), 2013.

[8] Setola R., Faramondi L., Salzano E., & Cozzani, V., " An overview of cyber attack to industrial control system". Chemical Engineering Transactions, (77, 907-912), 2019.

[9] Setola R. et al., "Analisi dei requisiti presenti nei capitolati di gara in tema di cyber security", Unindustria (https://www.unicampus.it/storage/647f602e/Rapporto-Analisi_dei_requisiti_presenti_nei_capitolati_di_gara_in_tema_di_Cybersecurity.pdf), 2023

[10] Setola R., Morelli F., "Cyber Security Strategies for the Protection of Electrical Substations". ITASEC 2022 (195-206), 2022

[11] Stouffer K., Falco J., & Scarfone K., "Guide to industrial control systems (ICS) security". NIST special publication (800(82), 16-16), 2011.

[12] Faramondi L., Flammini F., Guarino S., & Setola R., "Evaluating machine learning approaches for cyber and physical anomalies in SCADA systems", Proceeding IEEE CSR Conference (pp. 82–89), 2023